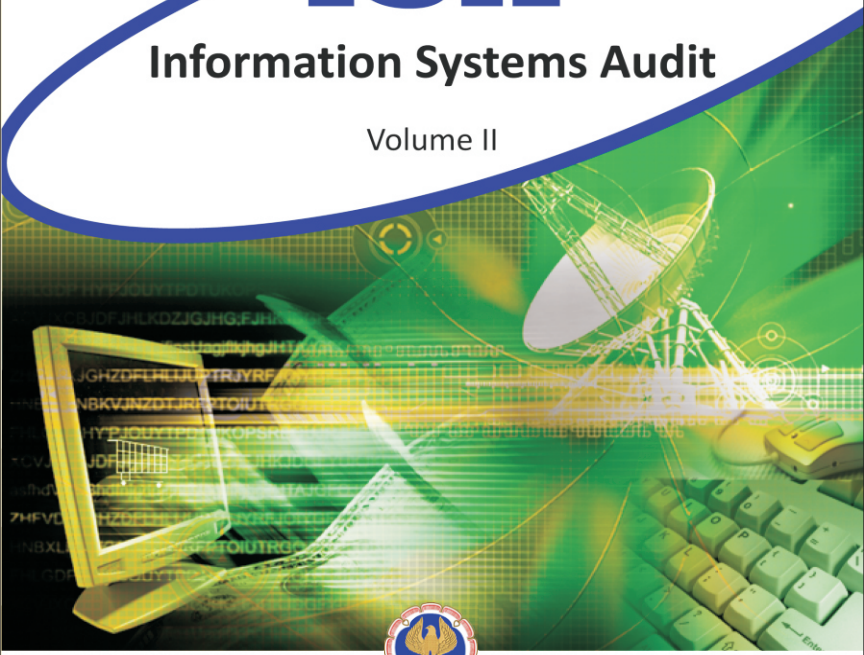
Background Material

ISA

Information Systems Audit

Volume II



Committee on Information Technology
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Background Material

On

Information Systems Audit

Volume II

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Revised Edition: February, 2010

Committee/ Department : Committee on Information Technology

E-mail : cit@icai.org

Website : www.icai.org, http://www.cit.icai.org

Price : Rs. 500/- (For Vol-I and Vol-II, Including CD)

ISBN : 978-81-8841-336-6

Published by : The Publication Department on behalf of the Institute of Chartered Accountants of India, ICAI Bhawan, Post Box No. 7100, Indraprastha Marg, New Delhi - 110 002.

Printed by : Sahitya Bhawan Publications, Hospital Road, Agra 282 003.
February / 2010 / 1,000 Copies (Revised)

Foreword

Information Technology is revolutionizing the way businesses operate and offer goods and services. Business Process Outsourcing (BPO) is fast becoming the order of the day and is now migrating into Knowledge Process off shoring; Internet has expanded our horizons with the free flow of vast amount of information. Networks are increasingly connecting offices and diverse businesses. The world is truly transforming into a Global Village. All these developments are Information Technology driven.

The increasing use of Information Technology is not without the attached risks and threats. Hacking is the order of the day. Viruses/ Worms are commonplace. Denial of service attacks have happened. The ever increasing globalization is shrinking barriers amongst nations across the world. Developments in outsourcing and off shoring are based on sophisticated and complex Information System Infrastructures. All these have resulted in a growing need for assurance services on Information Systems in India.

The Committee on Information Technology (CIT) of the Institute has been established to identify the emerging professional opportunities in the Information Technology sector for members and prepare them to face the threats and challenges ahead. Since its inception, the Committee has proactively considered the modern day requirements and initiated steps to suitably equip the members in terms of knowledge and skills to face the challenges ahead.

Post Qualification Course on Information Systems Audit is the first initiatives of the Committee to enable members to offer value added services of IS Audit, which are in increasing demand.

It gives me immense pleasure to so see this revised ISA Background Material for the Post Qualification Course on IS Audit, to enable members to develop understanding of the intricacies of Information Systems Audit in a simple and lucid manner.

I appreciate the efforts put in by CA. K. Raghu, Chairman, IT Committee and other members of the Committee and also the faculty members for bringing out the revised background material.

I am sure that this course will equip you to practice in this emerging field and enhance the range of services that can be provided by you. I wish you all the very best in pursuing the ISA Course.

January 11th, 2010
New Delhi

CA. Uttam Prakash Agarwal
President

Preface

Today there is seamless integration of business processes, internal controls, accounting systems and Information Technology. Our members need to provide increased assurance and other value added services to clients in this scenario.

The Committee on Information Technology (CIT) of ICAI established in the year 2000 to identify the emerging professional opportunities in the Information Technology sector for members and prepare them to face the challenges ahead had started the course on Information Systems Audit (ISA) to suitably equip members to provide assurance related services in the field of Systems & Process Assurance and a course on Computer Accounting & Auditing Techniques (CAAT) to provide hands-on training on use of computers, CAAT Resources CD to provide exposure to use of General Audit Software/ Computer Assisted Audit Techniques. Additionally, the Committee has published the Technical Guide on Information Systems Audit to provide a guide to conduct of IS Audit and also organizes practical workshops/ Conferences/ Seminars to provide technical updates to members, apart from other developments.

The Committee on Information Technology is pleased to present this thoroughly revised, upgraded and enhanced Background Materials for the ISA Course keeping in view the required revisions to the course and modules in tune with developments in the field.

I am very thankful to CA. Uttam Prakash Agarwal, President and CA. Amarjit Chopra, Vice President, for the guidance and support in coming out with this revised material. I would like to record my deep appreciation for the guidance and support of the Members of the Committee on Information Technology in coming out with the revised materials. I am also very thankful to all the team members involved in conceptualizing the revision, content/ material development, content review and content editing/consolidation for this commendable job. I also acknowledge the significant contribution made by the Ms. Indu Arora, Additional Director of Studies.

I am confident that the revised Background Materials for the ISA Course will be of significant assistance to the members providing Information Assurance Services that is currently in increasing demand.

January 11th, 2010
New Delhi

CA K. Raghu
Chairman
Committee on Information Technology

ISA SYLLABUS

Module 1: Information Technology Infrastructure and Communication/ Networking Technologies

Chapter 1: Introduction to Computer Hardware and Software

Types of computers - Hardware architecture of the computer - Various Input/Output (I/O) devices - ASCII and EBCDIC codes - Hardware monitoring procedures - Data and capacity management - Hardware acquisition plan - Definition of systems and application software - Various systems software and its brief description -Operating systems and its functions

Introduction to Database Management Systems - Introduction - Database and Database Management Systems (DBMS) - DBMS architecture - DBMS models - Database Languages - SQL - Roles and duties of a Database Administrator (DBA) and Data Administrator (DA)

Chapter 2 : Introduction to Computer Networks

Basics of communication - Simplex, Half-Duplex, and Full-Duplex Communications, Asynchronous & Synchronous Communication, Multiplexing, Switching techniques

Modem, Network Categories- LAN, WAN & MAN, Network Topology, Media used in communication, Factors that influence the use of media, Factors that degrade a signal.

Chapter 3: Introduction to OSI model

Various layers of OSI model - Application layer, Presentation layer, Session, Transport, Network layer, Datalink layer, Physical layer. Networking devices- Introduction to network management -IEEE LAN standards

Chapter 4: TCP/IP and Internet

A brief history of Internet & TCP/IP - Internet Administration - Generic Top-Level Domains (gTLDs)- TCP/IP Protocol Architecture -The architecture of TCP/IP suite -IP Addressing Scheme - The Domain Name System – Ports -Comparison between OSI model and TCP/IP protocol suite - Internet Services -Client/Server (C/S) Software Architectures--An Overview - Intrusion Detection Systems (IDS)

Chapter 5: Introduction to Firewalls

Characteristics of a Firewall -Types of Firewalls - Common implementation structures of a firewall - Limitations of Firewalls - Costs involved with Firewalls - General Controls associated with Firewalls - Phases in firewall lifecycle

Chapter 6: Cryptography

What is Cryptography? - Brief History of Cryptography - Why Cryptography? - The goals of cryptographic systems - Symmetric Key and Asymmetric Key Algorithms - How public key encryption method works - RSA : An Example for Public-Key Encryption - Digital Signatures - Comparison between Symmetric and Asymmetric Key Encryption Algorithms - Digital Envelopes - Digital Certificates - Cryptanalysis and their ways

Module 2: Protection of Information Assets

Chapter 1: Securing Physical Access

Introduction, IS Assets: Objects of Physical Access Controls, Physical Access, Threats and Exposures, Sources of Physical Access Threats, Physical Access Control Techniques, Administrative Controls, Technical Controls, Auditing Physical Access, Environmental Access Controls, Introduction, IS Assets: Objects of Environmental Controls, Environmental Threats and Exposures, Techniques of Environmental Control, Administrative Controls, Technical Controls, Integration and Fine Tuning of Environmental Controls, Audit and Evaluation of Environmental Controls, Audit of technical controls, Documentation of findings

Chapter 2: Logical Access Controls

Introduction, Objectives of Logical Access Controls, Paths of Logical Access, Logical Access Exposures, Technical Exposures, Malicious Code, Logical Access Controls Identification and Authentication, Authentication Techniques, Biometric Security, Access Controls in Operating Systems, Database Controls, Database Roles and Permissions, Views , Stored Procedures, Triggers, Database Restrictions, Audit Trail, Audit of Access Controls, Audit Procedures - Special Considerations, Identification of logical access paths, Audit Test Procedures, Systems Configuration, Logical Access mechanisms, User account management and password management, Privileged logons and special user accounts, Access to file directories and application logic and system instruction sets, Bypass Security Procedures, Appendix: Access Controls Checklist

Chapter 3: Network Security Controls

Introduction, Network Characteristics, Threats and Vulnerabilities, Information Gathering, Communication Subsystem Vulnerabilities, Protocol Flaws, Impersonation, Message Confidentiality Threats, Message Integrity Threats, Web Site Defacement, Denial of Service, Distributed Denial of Service, Threats from Cookies, Scripts and Active or Mobile Code, Network Security Controls, Architecture, Cryptography/ Encryption, Content Integrity, Strong Authentication, Remote Access Security, Firewalls, Intrusion Detection Systems, Auditing Network Security, Penetration Testing, Penetration Testing Scope, Penetration Testing Strategies, Types of Penetration Testing, Risks associated with Penetration Testing, Network Infrastructure Auditing Checklist, Network Server, Router, Firewalls, Network Administration and Security Auditing Checklist, Process, Authentication, Public Key Infrastructure (PKI), Access Control, Cryptography, Network Information Security, Information Security Administration, Microcomputer/PC Security, Audit Trails

Chapter 4: Application Controls

Introduction, Components of Application Controls, Application Boundary Controls, Input Controls, Source Document Design, Data entry screen design, Data code controls, Batch Controls, Data Input Validation Controls, Input Authentication Controls, Edit Controls , Data Input Error Handling and Reporting, Instruction Input Controls, Instruction input methods, Reporting Instruction Input Errors , Processing Controls, Data processing controls , Data file Controls, Output Controls, Existence Controls in Application Systems, Audit of Application Controls, Review of application controls

Chapter 5: Information Assets & Their Protection

Introduction, Information Classification, Classification of Information Assets, Data Privacy and Data Protection, Classification of Users, Naming Conventions, Access Control Models, Information Security Policy, Tools to Implement Policy: Standards, Guidelines, and Procedures, Components of a security policy, Program Policy, Components of Program Policy, Issue-Specific Policy, Components of Issue-Specific Policy, Areas Appropriate for Issue-specific Policies, Examples of Issue-Specific Policies, Network Policies, Data Privacy Policies, Data Integrity Policies, System Administration Policies, Usage Policies, Physical Security Policies, System-Specific Policy, Policy Implementation, Policy Documentation, Policy Visibility , System-Specify Policy Implementation, Interdependencies, Awareness, Training and Education, Cost Considerations, Audit of IS Security Policy

Module 3: Systems development life cycle & Application Systems

Chapter 1: Business Application Development Framework

Business Application Development Framework, Characteristics of System, Business, Application Development involves, Project Initiation, Need for Structured Systems Development Methodology, Risks associated with SDLC, Advantages for IS Audit of Structured Methodology, Overview of Phases in Structured Methodology of SDLC, Phase-Feasibility Study, Identification of problem, Identification of objective, Delineation of scope, Feasibility Study, Phase – Requirements Analysis, Understanding Requirements, Study of history, structure and culture, Study of Information flows, Eliciting user requirements, Structured Analysis, Context and Data Flow Diagrams (DFD), Entity-Relationship diagram, Data dictionaries, Decision Table / Decision Tree /Structured English, Decision Tree, Structured English (Psuedocode), State Transition diagram, System charts / program flow charts, Interface in form of data entry screens and dialogue boxes, Report layouts, Software Acquisition, Roles involved in SDLC, Steering committee, Project manager, Systems analyst, Module leader/Team leader, Programmers, Database Administrator (DBA), Quality assurance, Testers, Domain specialist, Technology specialist, Documentation specialist, IS auditor

Chapter 2: Phases in Software Development

Learning Goals, System Design Phase, Systems Design, Architectural design, Design of data / Information flow, Design of database, Design of user interface, Physical Design, Development Phase: Programming Methods, Techniques And Languages, Programming Methods & Techniques, Programming Language, Windows Platform, Unix / Linux based Platform, Coding style, Software Testing Phase, Objectives of testing, Levels of testing, Types of unit tests, Static analysis tests, Dynamic analysis tests, Integration / Interface testing: Final Acceptance Testing, Implementation of Software, Direct implementation / Abrupt change-over, Parallel implementation, Phased implementation, Pilot implementation, Activities during Implementation Stage, Post Implementation Review, Corrective maintenance, Adaptive maintenance, Perfective maintenance, Preventive maintenance, Umbrella Activities

Chapter 3: Alternative Methodologies of Software Development

Waterfall Model, Spiral Model, Data Oriented Systems Development, Process Oriented Approach, Object Oriented Systems Development, Prototyping, Rapid Application Development - RAD, Reengineering, Software reengineering consists of six activities, Inventory analysis, Document restructuring, Reverse engineering, Structured Analysis, Web-based Application Development, Informational, Download, Customization, Interaction, User Input, Transaction oriented, Service Oriented, Portal, Database Access, Data Warehousing, Risks associated with Web Based Applications, Agile Development, Information Systems Maintenance Practices, Change control, Continuous update of systems documentation, Program migration process, Testing program changes, Library control software, Executable and source code integrity, Program code comparison, Source code comparison, Object code comparison, Emergency changes, Configuration Management.

Chapter 4: Project Management Tools and Techniques

Budgets an Schedules, Software size estimation, Gantt Charts, Schedule, Gantt Chart for above schedule, Program Evaluation Review Technique (PERT), PERT terminology, Activity, Event, Predecessor activity, Successor activity, Slack, Maximum Total duration of this project = days, Dummy, Time estimate, Critical Path Method (CPM), System Development Tools and Productivity Aids, Code generators, Computer Aided Software Engineering (CASE), Classification of CASE tools, Upper CASE, Middle CASE, Lower CASE, Integrated CASE environments, CASE database (Repository), Advantages and limitations in using CASE, Benefits of using CASE, Disadvantages of CASE

Chapter 5: Specialised Systems

Artificial Intelligence (AI), AI applications, Cognitive Science, Expert Systems, Learning Systems, Fuzzy logic, Neural networks, Intelligent agents, Robotics, Virtual reality, Auditor's Role, Expert Systems, Components of expert systems, User interface, Interface engine, Knowledge base, Advantages of expert systems, Limitations of expert systems, Applications of expert systems, Applications of expert systems in IS Audit, Risk Analysis, Evaluation of Internal Control, Audit Program planning, Technical Advice, Data Warehouse, Features of Data Warehouse, Preparation of Data Warehouse, Consolidation, Drill-down, Slicing and dicing, Auditor's Role, Data Mining, Decision Support Systems (DSS), DSS frameworks, Design and Development, Implementation and use, Assessment and evaluation, DSS trends, Point of Sale Systems (POS), Automatic Teller Machines (ATM), Auditor's

Role, EDI, E-Commerce, ERP Systems, Electronic Data Interchange (EDI Systems), How does the EDI system function, Communication Software, Translation Software, EDI standard, Communication handler, EDI Interface, EDI Translator, Applications Interface, Application System, EDI standards, Features of ANSI ASCX, Features of UN/ EDIFACT, UN/XML, Web Based EDI, EDI Risks and Controls, Auditor's Role in Auditing EDI, Electronic Commerce (E-Commerce), The Advantages of the E Commerce, Types of E Commerce Models, Enterprise Resource Planning Systems (ERP Systems), Auditor's Role

Chapter 6: Auditing the System Development Process

IS Auditor's Role in Systems Development, Acquisition and Maintenance, IS Auditor's Role in Reviewing Developmental Phases of SDLC, Feasibility study, Requirement definition, Software acquisition process, Detailed design and programming phases, Testing phase, Implementation phase, Post-implementation review, System change procedures and program migration process, IS Auditor's Role in Project Management, Systems Development Project - Audit Checklist, Corporate Policies and Practices, User Requirements, Feasibility Analysis, Systems Design, Systems Specifications, Systems Development, Implementation, Post-Implementation

Module 4: Business Continuity Planning

Chapter 1: Business Continuity & Disaster Recovery Plan

Disasters and other disruptive events

Chapter 2: Documenting a Business Continuity Plan

Pre requisites in developing a Business Continuity Plan, Steps in developing a Business Continuity Plan (Phase I – Project Management and Initiation, Phase II – Business Impact Analysis / Risk Assessment, Phase III – Recovery strategies, Data communications, Voice communications, Fault tolerant, implementation strategies, Phase IV - Plan design and development, Phase V –Testing, maintenance, awareness and training)

Chapter 3: The Business Continuity Plan Audit

Priorities, Strategies, Responsibilities and Tasks, Plan Maintenance, Review of insurance coverage

Module 5 : Information Systems Organisation & Management

Chapter 1 – Governance

Enterprise Governance Definition - The enterprise governance framework - Best Practices in Enterprise Governance - Strategic Oversight -Enterprise risk management -The acquisition process - Board performance - Corporate Governance Definitions - Information Technology Governance - The Changing Role of the IT Department - Definition of IT Governance - Purpose of IT Governance - Some benefits of good IT governance - Who needs IT governance? – Best Practices in IT Governance - IT / IS Assurance Systems - IT Strategy Committee - The Balanced Score Card - Information Security Governance - Enterprise Architecture - Risk Management - E-Governance Definition- Users – Models – Benefits – Questions – Answers - Glossary of Terms

Chapter 2 - The Information System Management Process

The objectives of an organisation - The importance of management - The importance of managing the information systems department (ISD) - The process of The Deming Cycle - The Planning Function - The IS Steering Committee - The Master Plan of the Organisation - Long Range Plans - Short Range Plans – Policies – Standards – Guidelines – Procedures - The importance of leadership - The Acquisition of resources and Implementation of processes - Sequencing of policies, systems, processes, procedures and work instructions - The acquisition of IS resources - The Implementation of processes - Benchmarking processes - Financial Management processes -

IS Budgets and Variances - User Pays Scheme and Transfer Prices - User satisfaction survey processes - Capacity Management & Growth Planning processes - Goal Accomplishment processes / Indicators - Performance Measurement processes / Indicators - Quality Management processes Definition - ISO 9000:2000 Series - ISO 9126 Software Quality Model - The Software Capability Maturity Model (CMM) - Sourcing processes - HR processes - Documentation processes - Management Organisation Structures - Project and Line Management - The risks and controls of the various roles performed by personnel in the IS Department - Separation of Duties – Check – Act – Questions – Answers - Glossary of Terms

Chapter 3 – Auditing Information Systems Organisation & Management

Checklists / Audit Programmes - Suggestive Audit Checklist for auditing information systems organisation and management

Module 6: IS Audit Process

Chapter 1: IS Audit Process

Information Systems Audit Strategy, Fundamentals for Establishing an IS Audit Function, Audit Mission, Audit Charter, Structure and Reporting of the IS audit function, Staffing the IS Audit function, Internal and External Audit Control Framework, Quality Assessment and Peer Reviews, Engagement Letter, Skills and Competence Requirements of an IS Auditor, Phases in Information Systems Audit, Audit Planning, Preliminary Review , Knowledge of the Business, Understanding the Technology, Understanding Internal Control Systems, Legal Considerations and Audit Standards, Risk and Materiality, IS Audit Program, IS Audit Methodology, Examining and Evaluating Information, Communicating the Audit Results i.e. Reporting, Follow Up, Documentation Requirements, Use of Sampling in Information Systems Audits

Chapter 2: Information Risk Management

Information Risk Management: the Process (Step 1: Identification of Information Assets, Conceptual / Intangible Assets, Physical / Tangible Assets, Step 2: Valuation of Information Assets, Step 3: Identifying the potential threats, Step 4: Information Risk Assessment, Vulnerability Assessment, Probability or likelihood assessment, Impact analysis, Step 5: Developing Strategies for Information Risk Management),

Understanding the Relationships Between IS Risks and Controls, Acceptable / Residual Risk, Controls Assessment, IT Control Objectives, Category of Controls, Information Systems Control Framework, Information Systems, Risks & Controls – implications for Financial Auditor.

Chapter: 3 –IS Audit Techniques & Computer Assisted Audit Techniques

IT Environment Impact on audit methodology- Auditing in a computerized information system environment-Audit of IT controls and security-IS Audit approach-Computer Assisted Audit techniques-Type of CAATs-Other computer assisted audit techniques-Continuous auditing approach

Chapter 4: Overview of Information Systems Audit Regulations and Standards

Audit Standards, The Auditing and Assurance Standards issued by ICAI, Professional ethics and Code of Conduct prescribed by ICAI, IS Audit Guidelines by ISACA, COBIT – IT Governance Model, Other Global Standards on IS Assurance and Audit (A: The information security standards BS7799 & ISO 27001, B : SAS 70 - Statement

on Auditing Standards (SAS) No. 70, Service Organizations (AICPA), C:SysTrust, D: IT Infrastructure Library (ITIL), ISO 20000)

Overview of Regulatory Developments Impacting Controls in a Computerized Environment (A: Information Technology Act, 2000 of Government of India, B. The UNCITRAL Code, C: Sarbanes - Oxley Act 2002 Internal Control & COSO Criminal Penalties and Protection SOX and IT Controls Amendments to Clause 49 of the SEBI Listing Agreement, D: Basel II Framework for Risk Management).

Table of Contents

Volume – I

MODULE 1: Information Technology Infrastructure and Communication/ Networking Technologies

MODULE 2: Protection of Information Assets

MODULE 3: System Development Life Cycle & Application Systems

Table of Contents

Volume – II

MODULE 4: Business Continuity Planning

MODULE 5: Information Systems Organisation & Management

MODULE 6: IS Audit Process

Module – IV

Business Continuity Planning

1 Business Continuity and Disaster Recovery Plan

Learning Objectives

- To understand the need for business continuity plan and disaster recovery plan.
- To understand various types of disasters and their impacts.

Introduction

Business and enterprises of today depend heavily on Information and Communication Technology (ICT) to conduct business. The ICT plays a central role in the operation of the business activities. For example, the stock market is virtually paperless. Banks and financial institutions have become online, where the customers rarely need to set foot in the branch premises. This dependence on the systems means that all enterprises should have contingency plans for resuming operations from disruption. The disruption of business operation can be due to unforeseen man-made or natural disaster that may result into revenue loss, productivity loss and loss of market share among many other impacts. Thus enterprises have to take necessary steps to ensure the continuity of operation in the event of disruptions.

Objectives of a Business Continuity Plan

The objective of a Business Continuity Plan (BCP) is to enable an organisation to continue to operate through an extended loss of any of its business premises or functions. The fundamental aim of BCP is to:

- Manage the risks which could lead to disastrous events.
- Reduce the time taken to recover when an incident occurs and
- Minimize the risks involved in the recovery process.

Organisations worldwide are more and more being dependent on computers, in assisting and carrying out the decision making processes and in recording business transactions. An organisation is extremely dependent on several resources like intellectual property, employees, computers and communication links. If any of these resources are not available, the organisation will not be able to function at its full strength. The longer one or more of these resources are unavailable, the longer it

might take the organisation to get back to its original state. Sometimes, organisations can never get back to its original state. As a result, it becomes important to have a tested plan for the disaster recovery, more importantly, in the information processing area to ensure business continuity. The organisations that think ahead have always a better chance of survival.

Definition of a Business Continuity Plan

A Business Continuity Plan is a documented description of the actions to be taken, the resources to be used and the procedures to be followed before, during and after an event which renders part or all of an organisation's business functions unavailable. Business continuity plans are devised to ensure that those functions which are vital to continue the business operations are recovered and made operational in an acceptable time frame. There is no standard Business Continuity Plan, each plan must be based on the realistic business requirements of the organisation for which it is being developed. However, a distinction may be drawn between business continuity planning and disaster recovery planning.

A Business Continuity Plan (BCP) aims to sustain mission critical business process during an unplanned interruption event. Whereas a Disaster Recovery Plan (DRP) is a comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss, DRP is usually focused on an information technology (IT) or other operational facility. The key differences between the two plans lie in their scope. BCP includes DRP, more commonly, a BCP includes several DRPs.

A Business Continuity Plan does not address the recovery from day-to-day operational problems such as a hardware failure or a hard disk crash. Recoveries from problems of this nature are supposed to be addressed in the operation documentation. However, should an operational problem extend beyond a predetermined critical period, the Business Continuity Plan may be invoked. Business Continuity Plans are not casual agreements for support with little expectation, they are formal plans, approved and owned by senior management having an impact on the organisation in entirety.

To put it simply, a Business Continuity Plan is developed to prevent and / or minimize interruptions / disruptions to normal business activities and its effect on business. Disruptions are events that may be intentional or unintentional, natural or man-made and may hamper normal business operations. A Business Continuity Plan, generally, looks into the recovery of all critical information processing areas of the company, including but not limited to:

i. Information processing recovery: Information processing recovery deals with the alternatives available for the recovery of a facility following a major disruption.
ii. Telecommunications recovery: Telecommunications recovery deals with various options available to recover lost data and voice communication.
iii. Other recovery options.

Features of Business Continuity Planning

Business Continuity Planning has three complementary features:

i. **Risk reduction:** Risk reduction is the management of risks to prevent a disaster. This is done by identifying and assessing the risks faced by a department at their premises which could result in a disaster;
ii. **Emergency Plan:** Emergency plan deals with crisis management of the incident when it occurs (Incident Control) to prevent it from developing into a disaster, and to lessen its impact. The priority is to evacuate staff and others when this is necessary, but essential or valuable information and objects can often be rescued without risk to personal safety;
iii. **Business Continuity Plan:** BCP is a plan for the fast, efficient resumption of essential business operations by directing the recovery actions of specified recovery teams. The three elements to consider in the plan are the continuity of:

- office services - premises, furniture, stationery etc;
- information technology - communications and computing services; and
- human and other resources - ensuring that staff:
  - are aware of the alternative arrangements;
  - have the resources they need; and
  - are productively employed.

The key tasks in Business Continuity Planning are to:

Identify which operations and supporting activities need to be restarted after a disaster, the maximum acceptable time limits by which they must restart, and the resources needed to restart them;

- identify contingencies for the required resources;
- select a cost-effective strategy for restarting operations;
- develop the BCP to guide and direct the restart of operations;
- test the BCP, train staff in how to use it, and keep it up to date.

If a BCP is to be correctly constructed and operate successfully, it must involve all levels of management, and must cover the:

- action to be taken following a disaster;

- staff responsible for specific tasks;
- essential operations and systems;
- actions required to restart operations;
- emergency data processing arrangements;
- off-site backup requirements;
- supplies requirements; and
- Means of keeping staff and others informed of arrangements and developments.

Disasters and other disruptive events

A disaster can be defined as an unplanned interruption of normal business process. More comprehensively, a disaster can be defined as a disruption of business operations that stops an organisation from providing its critical services caused by the absence of critical resources. The critical resources could be:

- People and skill sets
- Facilities
- Communications
- Power
- Data/Information
- Information systems

The disruption could be several hours to several days, depending upon the extent of damage to the information resource. Most importantly, disasters require action to recover the operational status. However, all events are not disasters. A good business continuity plan will take into consideration all types of events impacting business operations. For extreme cases, both short term and long term fall back strategies are required. For the short term, an alternate processing facility may be required to restore the operations to reduce losses.

Types of disasters

There are many possible causes of disaster or disruptive event. These can be classified as Natural or Technical (man-made):

i. ***Natural disasters***

Natural disasters are caused by natural events and include fire, earthquake, tsunami, typhoon, floods, tornado, lightning, blizzards, freezing temperatures, heavy snowfall, pandemic, severe hail storms, volcano, etc.

ii. ***Man-made / Technical disasters***

Man-made disasters are caused by actions of human beings, such as terrorist attack, Bomb Threat, Chemical Spills, Civil Disturbance, Electrical Failure, Fire, HVAC

Failure, Water Leaks, Work Stoppage / Strikes hacker attacks, viruses, Human Error, Loss of Telecommunications, Data Center Outage, Lost / Corrupted Data, Loss of Network, Services, Power Failure, Prolonged Equipment Outage, UPS / Generator Loss and anything that diminishes or destroys normal data processing capabilities.

Impact of disasters

The impact of a disaster may be one or more of the following:

i. **Loss of human life**: The extent of loss depends on the type and severity of the disaster. Protection of human life is of utmost importance and, the overriding principle behind continuity plans.
ii. **Loss of productivity**: When a system failure occurs, employees may be handicapped in performing their functions. This could result in productivity loss for the organisation.
iii. **Loss of Revenue:** For many organisations like banks, airlines, railways, stock brokers, effect of even a relatively short breakdown may lead to huge revenue losses.
iv. **Loss of Market share:** In a competitive market, inability to provide services in time may cause loss of market share. For example, a prolonged non-availability of services from services providers, such as Telecom Company or Internet Service Providers, will cause customers to change to different service providers.
v. **Loss of goodwill and customer services:** In case of a prolonged or frequent service disruption, customers may lose confidence resulting in loss of faith and goodwill.
vi. **Litigation:** Laws, regulations, contractual obligation in form of service level agreement govern the business operations. Failure in such compliance may lead the company to legal litigations and lawsuits.

When considering the impact of a disaster, it should be remembered that it will never happen at a convenient time; and is always unpredictable. There is no way of knowing:

- when it will happen;
- what form it will take;
- how much damage it will cause; or
- how big the impact will be.

The impact of a disaster can vary. A disaster could involve:

- **total destruction** of the premises and its contents, for example as a result of a terrorist attack;

- **partial damage**, preventing use of the premises, for example through flooding; or
- **No actual physical damage** to the premises but restricted access for a limited period, such as enforced evacuation due to the discovery nearby of an unexploded bomb.

Phases of Disaster

A typical disaster will consist of some or all of the following phases:

1. Crisis Phase;
2. Emergency Response Phase;
3. Recovery Phase; and
4. Restoration Phase.

1. **Crisis Phase:** The Crisis Phase is under the overall responsibility of the Incident Control Team (ICT). It comprises the first few hours after a disruptive event starts or the threat of such an event is first identified; and is caused by, for example:

   - Ongoing physical damage to premises which may be life threatening, such as a fire; or
   - Restricted access to premises, such as a police cordon after a bomb incident or discovery of asbestos in the premises.

   During the crisis phase, the fire and other emergency evacuation procedures (including Bomb Threat and Valuable Object Removal Procedures) will apply; and the emergency services should be summoned as appropriate.

2. **Emergency Response Phase:** The Emergency Response Phase may last from a few minutes to a few hours after the disaster. It will start near the end of, or after, the Crisis Phase if there has been one, or when a potentially threatening situation is identified. During the Emergency Response Phase, the Business Continuity Team (BCT) will assess the situation; and decide if and when to activate the BCP.
3. **Recovery Phase:** The Recovery Phase may last from a few days to several months after a disaster and ends when normal operations can restart in the affected premises or replacement premises, if appropriate. During the recovery phase, essential operations will be restarted (this could be at temporary premises) by one or more recovery teams using the BCP; and the essential operations will continue in their recovery format until normal conditions are resumed.
4. **Restoration Phase:** This phase restores conditions to normal. It will start with a damage assessment, usually within a day or so of the disaster, and may identify

any need for refurbishment or even replacement of the premises. This phase will not occur if physical damage did not happen. When the cause for evacuation or stopping of operations has ended, normal working will be restarted. During the Restoration Phase, any damage to the premises and facilities will be repaired. Because each disaster is different:

- it is not possible to predict which phases a disaster will involve; and the response to an incident will vary according to the individual circumstances.

Some examples of disasters and the phases they may involve are:

S.No	Examples of disaster	Phases
1.	serious fire during working hours	all the phases in full;
2.	serious fire outside working hours	all the phases but no staff and public evacuation;
3.	very minor fire during working hours	Crisis Phase only, staff and public evacuation but perhaps no removal of valuable objects, Fire Service summoned to deal with the fire;
4.	gas main leak in street outside working hours, repaired after some hours	Only Emergency Response Phase appropriate.

Summary

When critical services and operation cannot be conducted, consequences to the business can be severe. All the organisations are at risk and face potential disaster if unprepared. A Business Continuity Plan is a tool that helps to moderate the risk and enable continuity of business despite disruption.

Questions:

Q1. The fundamental aim of the BCP is to:
   a. Manage the risks which could lead to disastrous events.
   b. Reduce the time taken to recover when an incident occurs and
   c. Minimize the risks involved in the recovery process.
   d. All of the Above.

Q2. Disaster recovery plan and Insurance are:
   a. Controls of first resort.
   b. Unreliable controls.
   c. Preventive controls.
   d. Controls of last resort.

Module – IV

Q3. The overriding principle behind most continuity plans is
   a. The protection of profits.
   b. The protection of assets.
   c. The protection of human life.
   d. The protection of customers.

Q4. A comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss is called a:
   a. Business continuity plan (BCP)
   b. Disaster recovery plan (DRP)
   c. Disaster continuity plan (DCP)
   d. Business recovery plan (BRP)

Q5. The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability is called a/an:
   a. Threat
   b. Risk
   c. Exposure
   d. Hazard

Q6. Any force or phenomenon that could degrade the availability, integrity or confidentiality of an Information Systems resource, system or network is called a:
   a. Threat
   b. Risk
   c. Vulnerability
   d. Threat-source

Q7. A disruption of business operations that stops an organisation from providing its critical services caused by the absence of critical re-sources is called a:
   a. Disaster
   b. Vulnerability
   c. Catastrophe
   d. Calamity

Q8. The goal of recovery and restoration phase includes:
   a. Re-deploying personnel
   b. Re-establishing normal operations
   c. Resuming operations at pre-disruption level
   d. All of the Above.

Answers:

1 D	2 D	3 C	4 B	5 A	6 D	7 A	8 D

2 Documenting a Business Continuity Plan

Learning Objectives

- Develop a Business Continuity Plan.

Introduction

There is no mandatory requirement for a BCP in our country and legal framework is still evolving. Therefore, the onus lies on the management of all organisations to ensure that all critical business processes are identified; risks associated with the processes are determined, adequate measures of redundancy are built in and around the processes, to minimize the effect of loss, should there be a disaster.

Though the foreign laws are not applicable in our country, it is worthwhile to know about them, as sooner or later a law will be enacted in our country on the same line. Some of them are Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II), Sarbanes-Oxley, HSPD-12, BASEL II, Gramm-Leach-Bliley. It is also worth mentioning that certain commonly accepted International standards also emphasize the BCP, for example COBIT and ISO 27001.

Pre requisites in developing a Business Continuity Plan

A BCP cannot be completed within a week or a month. In fact, it can never be completed; the plan must be tested and updated at least once a year, if not more frequently. Moreover, critical business functions may evolve. A plan that does not keep pace with the changes in the organisation is not of any use. Therefore, one may have a working plan today, but the project needs to be a continuous affair to ensure success, if the plan is ever needed.

The primary objectives of a BCP are to guide an organisation in the event of a disaster and to effectively re-establish critical business operations within the shortest possible period of time with minimal loss of data. The goals of the planning project are to assess current and anticipated vulnerabilities, define the requirements of the business and IT, design and implement risk mitigation procedures, and provide the organisation with a plan that will enable it to react quickly and efficiently at the time of a disaster.

It must be noted that a BCP is not limited to the IT environment. It is predominantly a business issue; the plan must address the operational needs of the business environment. The key members of the business processes should be involved in the planning to ensure that the needs are clearly understood and documented. IT personnel should not make assumptions as to what systems are critical to the business community. The following points must be considered while developing a business continuity plan. These are:

- The top management must fully support and agree to the BCP requirements.
- The BCP project team should consist of members from all functional groups including the Information Technology (IT) group.
- The business and ICT recovery requirements must be defined and agreed upon. Furthermore, they should be posted somewhere accessible to everyone in the organisation, through company Intranet, news-letter, etc. This type of visibility helps to ensure that people realize the importance in the effort, and their role in its success.
- A process needs to be developed to keep the plan up-to-date, with review and updating of plan at regular interval or as need arises. The plan should represent the true business and computing requirements at all times.

Steps in developing a Business Continuity Plan

Just as every organisation is unique, so too is the business continuity planning project. As such each plan should be tailored to the individual organisation, what works for an organisation may not necessarily work for another. There are five phases in developing a BCP (see Fig. 2.1). The first phase is Project Management and Initiation, followed by a Risk Assessment, choosing a Recovery Strategy, Plan design, development and Implementation, and lastly testing, Maintenance, Awareness and training.

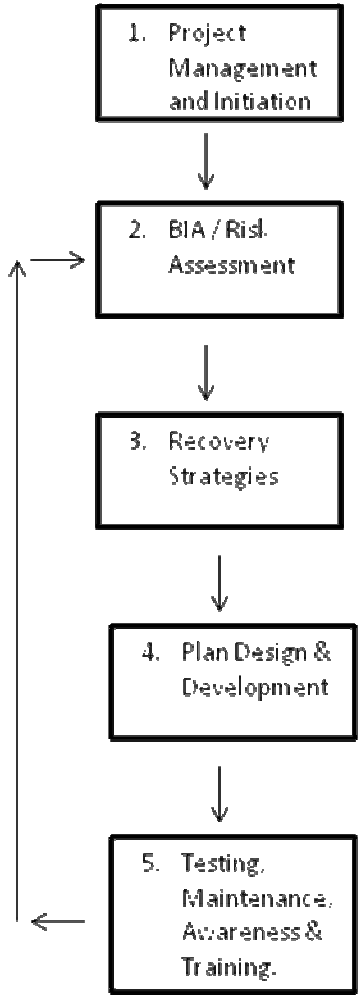


Fig. 2.1: Five Phases in developing a BCP

Phase I - Project Management and Initiation

The objectives of this phase is to gain an understanding of the existing and planned future IT environment of the organisation, define the scope of the project, develop the project schedule, and identify risks to the project. In addition, a Project Sponsor / Champion and Steering Committee should be established during this phase. The Project Sponsor / Champion should be a member of the senior management team with required authority to push the project to completion. The Steering Committee should be responsible for guiding the project team. The Committee should have members from both functional and IT departments. Also a Project Manager and / or a

Disaster Recovery Coordinator should be appointed. Following key tasks should also be conducted:

- A thorough risk assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance; database security; data and voice communications security; systems and access control software security; insurance; security planning and administration and application controls should be carried out. A risk assessment is carried out to determine the extent of the potential threat and the risk associated with system. The output of this process helps to identify appropriate controls for reducing or eliminating the risk during risk mitigation process.

The risk assessment will enable the project team to improve any existing emergency plans and disaster prevention measures and to implement required emergency plans and disaster prevention measures where none exist.

Present findings and recommendations resulting from the activities of the risk assessment to the Steering Committee so that corrective actions can be initiated in a timely manner.

Define the scope of the planning effort.

- Develop a plan framework.
- Assemble a project team and conduct awareness sessions.

Phase II – Business Impact Analysis / Risk Assessment

Risk Assessment seeks to identify which business processes and related resources are critical to the business, what threats or exposures exist to cause an unplanned interruption of business processes, and what costs accrue due to an interruption.

There are various analytical procedures that are used to determine the various risks, threats, and exposures faced by an organisation. These are known by various names, such as Business Impact Analysis (BIA), Application Impact Analysis, Threat and Exposure Analysis, Risk Impact Analysis and so on. While many authors and practitioners maintain subtle differences between these terms, this discussion subsumes all these activities under Risk Assessment.

Risk is an exposure to unwanted loss. In terms of Business Continuity, it is the risk of an incident happening which may result in unwanted loss of an asset or delay in operations.

Risk Assessment is the systematic identification of all risks, their investigation and grading relevant to each other and to the department, so that the management can be given a clear and full understanding of the risks it faces.

Objectives of Risk Assessment

Risk Assessment is an important phase in the development of a Business Continuity Plan (BCP). The aims of Risk Assessment are to:

- identify the risks that departments face;
- identify essential operations that must be restarted as quickly as possible after a disaster has taken place;
- identify cost-effective measures that could be introduced to prevent risks or lessen their impact and;
- provide an input for Risk Management.

All disaster events may not be anticipated or considered. For example, very few organisations considered Tsunami as a major risk in South Asia, before it actually struck.

The threats, exposure, probability of happening and the loss are documented as part of the Risk Assessment. An analysis of all the business processes that are supported by IT will be carried out to identify the systems / processes that critical / core to very survival of the business and also to determine the length of time that such processes can survive without IT by not incurring heavy loss. The information should be gathered through standard survey tools or questionnaires and should be documented in a clear and understandable format to be presented to the management.

Risk Assessment & Recovery

The objectives of risk assessment include:

1. **Criticality prioritization:** Identifying business functions or processes and their associated resource requirements. Prioritizing business processes according to their time-sensitivity and criticality.
2. **Estimating the critical recovery time period:** (also called “Recovery Time Objectives" or "Maximum Tolerable Downtime") of the business process. The critical recovery time period is the maximum amount of time allowed for the recovery of the of the business function. This is the amount of downtime of the business process that the business can tolerate and still remain viable. If this time is exceeded, then severe damage to the organisation will result.

From the IT point of view, recovery usually means restoring support for the processing and communication functions that are considered to be critical to the

business and then restoring support for other non critical / ancillary systems. From the business perspective, recovery means being able to execute the business functions that are at the key to the survival of the business and then being able to execute the -non-critical/ ancillary functions. Another key factor to consider when defining recovery is the timeframe. Recovery of the function and the system is evaluated considering several Time based factors such as:

i. **Recovery Time Objective (RTO):** RTO is the measure of the user's tolerance to downtime. For example: Critical monitoring system must have very low RTO or zero RTO. RTO may be measured in minutes or less.
ii. **Service Delivery Objective (SDO):**SDO refers to the amount of time that can elapse from the failure to the time when the system or services are available for use. For example: a company's order processing system may have a SDO of 24 hours, while its intranet facility has a SDO of 1 week. RTO is a measure of the users' tolerance to down time. A large RTO means that users can tolerate extensive down time. Similarly, the organisation needs to understand how much data it can afford to lose during a disruption. This is referred to as Recovery Point Objective (RPO).
iii. **Recovery Point Objective (RPO):** RPO is a measure of how much data loss due to a node failure is acceptable to the business. A large RPO means that the business can tolerate a great deal of lost data. Depending on the environment, the loss of data could have a significant impact. A rule of thumb is that the lower the RPO, higher the overall cost of maintaining the environment for recovery.

An RPO of 5 minutes can lose data up to 5 minutes of data, whereas 0 RPO will have no loss of data. Like RTO / SDO, RPO may vary with services and system. However, it is important to understand the dependencies between the systems and taken into consideration while determining the critical systems. These two objectives are not closely related – they may both be almost zero, they may both be large, or one may be small but the other large. Examples of need of various systems are shown below:

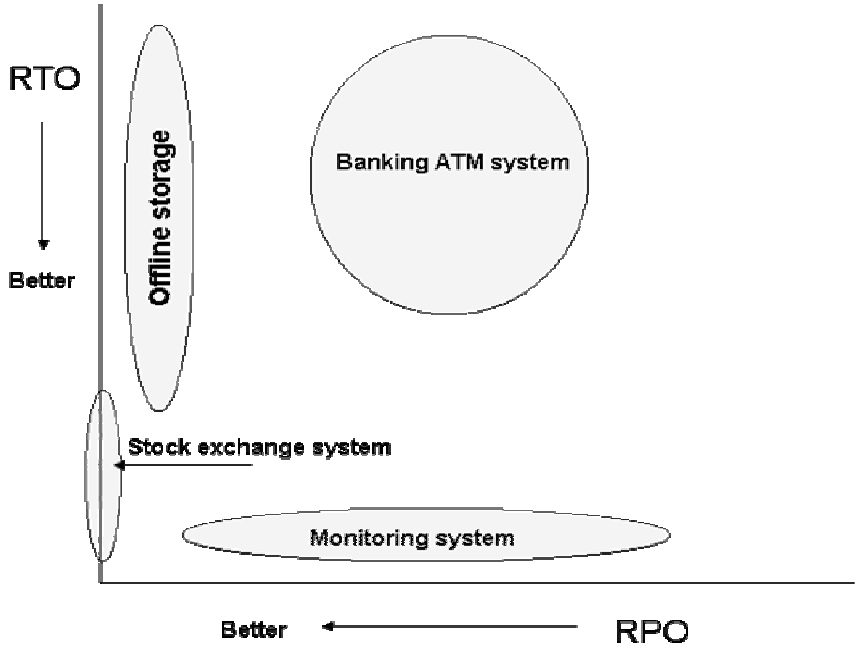


Fig. 2.2: Illustrates relations between RTO/RPO

Examples from the above Figure:

i. A stock exchange trading system must be restored very quickly and cannot afford to lose any data. Since the price of the next trade depends upon the previous trade, the loss of a trade will make all subsequent transactions wrong. In this case, the RTO may be measured as a few minutes or less, but the RPO must be zero.

ii. A critical monitoring system such as those used by power grids, nuclear facilities, or hospitals for monitoring patients must have a very small RTO, but the RPO may be large. In these systems, monitoring must be as continuous as possible; but the data collected becomes stale very quickly. Thus, if data is lost during an outage (large RPO), this perhaps impacts historical trends; but no critical functions are lost. However, an outage must end as quickly as possible so that critical monitoring can continue. Therefore, a very small RTO is required.

iii. A Web-based online ordering system must have an RPO close to zero (the company does not wish to lose any sales or, even worse, acknowledge a sale to a customer and then not deliver the product). However, if shipping and billing are delayed by even a day, there is often no serious consequence, thus relaxing the RTO for this part of the application.

iv. A bank's ATM system is even less critical. If an ATM is down, the customer, although aggravated, will find another one. If an ATM transaction is lost, a customer's account may be inaccurate until the next day when the ATM logs are used to verify and adjust customer accounts. Thus, neither RPO nor RTO need to be small.

Once a company decides what RPO and RTO are applicable to an application, the method for backup and recovery of that application becomes much more evident.

Threats and its type

A threat is anything with a potential for adverse effect on an asset, for example fire, unauthorized access to premises. Threats should be assessed to determine:

- How vulnerable the Department's assets are to the threats;
- What preventative measures could be taken to lessen the impact of the threats.

The different types of threat a Department's assets may be at risk from are illustrated in Fig. 2.3.

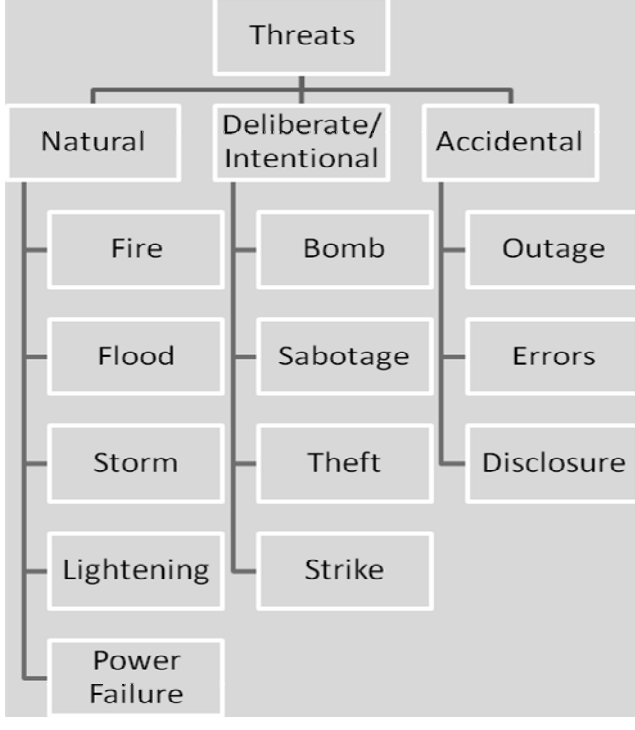


Fig. 2.3: Types of Threats.

Departments should also consider threats arising from various issues as illustrated in Fig. 2.4.

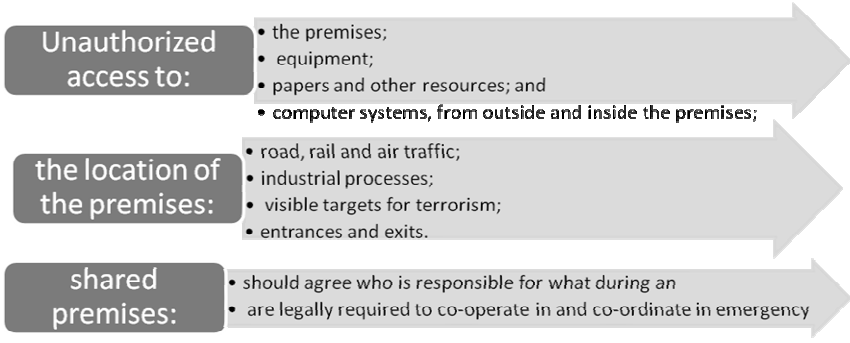


Fig. 2.4: Threats.

Areas for Investigation	Status (Y/N) / Comment
Existence of fire and other emergency evacuation procedures	
Existence of bomb threat procedures	
Reliance on telephone, fax, IT equipment	
List of reliable contractors for emergency repairs	
Dependency on specific goods and Services	
Dependency on specific equipment	
Computer data backed up and stored off site	
Compliance with legislation on public health, health and safety, fire precautions	
Compliance with listed building constraints	
Leakages, burst pipes, internal flooding water, oil, gas	
Power isolation devices on electrical systems	

Fig. 2.5: Checklist for Risk Assessment.

Risk Assessment Methods

If the Risk Management is to be effective, a systematic approach to Risk Assessment should be taken. This means that Risk Assessment should be conducted formally,

rather than casually. The following methods will enable a systematic and reliable Risk Assessment to be carried out:

1. Risk Ranking
2. Value ranges
3. Formulae for comparing risks
4. Computer software if suitable -

1. Risk Ranking: The ability of a company to cope with interruption of a business process determines the TOLERANCE of the business process. This tolerance depends on the length of the disruption and may also be linked to the time of the day or month the interruption occurs. In practice, tolerance is usually expressed as a monetary amount – the cost to the company if business process is interrupted for a given unit of time. This cost of interruption is inversely related to the tolerance. The various business processes may be classified on their critical recovery time period.

i. **Critical:** These are functions that cannot be done manually under any circumstances. Unless a company located identical capabilities to replace the damaged capabilities, these functions cannot be performed. These functions have zero or very low tolerance to interruption and consequently, the cost of interruption is high.
ii. **Vital:** These functions can be performed manually but only for a brief period of time. There is relatively higher tolerance to interruption as compared to critical functions and consequently somewhat lower cost of interruption. The function classified as vital can withstand a brief suspension of operations but cannot withstand an extended period of downtime.
iii. **Sensitive:** These processes can be carried out by manual means for an extended period, though with some difficulty. They may require additional staff to perform and when restored, may require considerable amount of time to restore the data to current or usable form.
iv. **Non-Critical:** These processes have a high tolerance to interruption and can be interrupted for an extended period of time with little or no adverse consequences. Very little time is required to restore the data to a current or usable form.

2. Value ranges: To assist in comparison, a range of values should be set for each of the following:

- asset cost;
- likelihood of threat happening;
- vulnerability; and
- assessment of the risk.

The following ranges can be used:

- a scale of one to five; or
- Very Low, Low, Moderate, High and Very High.

A scale of one to five will produce a more accurate Risk Assessment than a scale of one to three. Ranges greater than five are usually unnecessary and should only be used if a particularly accurate Risk Assessment is required, or a greater distinction between different risks needs to be made.

3. Formulae for Comparing Risks: To produce more precise results from a Risk Assessment, a formula can be used in conjunction with the value ranges in mentioned above to compare and priorities risks. For example:

$$\text{Risk} = \frac{\text{Asset Cost} + \text{Likelihood} + \text{Vulnerability}}{3}$$

Divide the sum of asset cost, likelihood and vulnerability by three to find the average value. For convenience, the resulting score can then be translated into words to describe the risk, such as:

- 1 -Very Low;
- 2 - Low;
- 3 - Moderate;
- 4 - High;
- 5 -Very High.

Example: The risk of flooding to a premise has been assessed and the following values awarded:

- asset cost = 5 (the property is highly valued);
- likelihood = 3 (flood is considered to be a moderate threat because the property is located in the midland); and
- Vulnerability = 2 (because the property is constructed well above the ground level/ Sea level).

Using the formula given above, the score for this particular risk is:

$$\frac{5 + 3 + 2}{3} = 3.3$$

This translates into words as `Moderate' risk.

The example above and the formula used are simple and should be adequate for uncomplicated Risk Assessments.

4. Computer software: Computer software packages for Risk Assessment are available. It must be remembered that software is only a tool and cannot carry out Risk Assessment on its own. The user must:

- know how to operate the software properly;
- input the correct information; and
- interpret the data generated by the software correctly.

Phase III – Recovery Strategies

Recovery strategy defines the best way to recover from disruption. The selection of recovery strategy also depends on the type of system, whether centralized, networked or distributed etc among other consideration like cost, time, criticality of business process and security.

Strategies for Centralized Systems

The traditional focus of BCP/DRP was the recovery of the corporate computer system, which was almost always a mainframe or large minicomputer. Mainframe-centric disaster recovery plans often concentrated on replacing an inaccessible or non-functional mainframe with compatible hardware. The following are some of the widely adopted strategies for centralized system recovery.

i. **Mirror Site/ Active Recovery Site:** The single most reliable system backup strategy is to have fully redundant systems called an active recovery or mirror site. While most companies cannot afford to build and equip two identical data centres, those companies that can afford to do so have the ability to recover from almost any disaster. This is the most reliable and also the most expensive method of systems recovery.

ii. **Hot Sites:** A dedicated contingency centre, or 'hot site' is a fully equipped computer facility with electrical power, heating, ventilation and air conditioning (HVAC) available for use in the event of a subscriber's computer outage. These facilities are available to a large number of subscribers on a membership basis and use of site is on a 'first come, first served' basis. In addition to the computer facility, these facilities offer an area of general office space and computer ready floor space on which the users can build their own long term recovery configuration. Test time is available throughout the year together with software and telecommunications support, library space, and a tested secure environment. While these are the most expensive of the services, they offer the user a great deal comfort for faster recovery. This type of site is likely to be used where the organisation is dependent upon online systems, which must be recovered within a matter of hours or days. It should be noted, however that time

available for use in a disaster is usually limited, which is why the computer ready space is also available for long term requirements.

The fee for a dedicated contingency centre normally includes an initiation fee, an annual membership fee, a notification fee, if the member requires its use in a disaster situation, and a usage fee. The ability to meet telecommunication requirements must be carefully reviewed.

Some vendors offer only one site. The larger vendors have multiple sites in different geographical regions, and offer subscribers the ability to recover in another site should their primary recovery site not be available when disaster is declared. Some of the vendors also offer remote operations facilities for use in tests or emergency. Where the recovery centre is in a city other than the subscriber's home location, this can be used to reduce the need to transport staff and resources.

iii. **Warm Sites:** A warm site is a cross between a hot site and a cold site. Like a hot site, a warm site will be available with electrical power, HVAC and computers, but the applications may not be installed or configured. The site is partially prepared for systems restoration but does not contain all of the components necessary to do an immediate restore of all business functions. In the event of an emergency, the hardware and software additions needed to get the system operational may cause a delay. A warm site can be used as a data processing centre until it is needed for business continuity.

iv. **Cold Sites:** The cold site or empty shell facility is fully designed to house a computer centre, but it contains no hardware. It includes pre-installed flooring, electric power, air-conditioning, water, and telecommunication equipments. It is basically a shell ready to receive computer equipment during an emergency. This is a viable solution, if the subscriber or owner can survive without computer facilities until the shell is equipped and operating. While estimates of the time needed to accomplish this will vary, it is possible that several weeks may pass before the affected organisation is capable of resuming operations at such a site. Cold sites are also available on a membership basis, a limited number of members being taken from a given site is on a 'first come, first served' basis. The fees for an empty shell facility will be lower than a fully-equipped site, but reflect a similar type of structure (annual membership, notification charge and usage charge). As with a hot site, the ability of the shell to meet the client organisations telecommunications requirements should closely be examined.

While testing is possible for a cold site solution, it is not easy to obtain the same level of comfort as is possible with a hot site. Communications capabilities

remain a key question in assessing the viability of such sites as an appropriate solution.

v. **Commercial Service Bureaux:** Over the last several years, commercial service bureau have become increasingly involved in providing contingency processing services. This has been, for many, a natural progression for their base of service, and they are uniquely equipped for expansion. In order to support their traditional market they have significant equipment inventories, sophisticated operating environments, extensive telecommunications capabilities, adequate support facilities and better-than-average security. It is important to realize, however, that contingency services are not their primary source of revenue. In order for a service bureau to turn over all or part of its facilities to an affected subscriber, it may have to dislocate some current customers. For this reason, the majority of service bureau offering contingency services have elected to offer them only in a shared environment. Among this group, some have also restricted their offering to current customers. While the shared environment complicates matters somewhat, it does not rule out the service bureau as a viable alternative.

   In evaluating a "shared" service bureau, the planner is cautioned to carefully investigate how much capacity will be made available, and the operating system used. Where non-removable disk drives are not to be used, the planner must be sure to include the necessary dump/restore timings in the usage estimates. Other areas to be researched in this "shared" environment include:

   - office space availability
   - software compatibility
   - security
   - telecommunications availability and bandwidth: and
   - processor throughput considerations and the duration of service availability.

   When looking at a "shared" service bureau, the planner should consider which applications might best fit that environment, rather than looking for a blanket solution for all applications. For example, a Payroll bureau may be a suitable alternative for a critical payroll application. In other cases, the services bureau could provide an effective short term bridge for on-line systems until a more permanent long-term solution can be put into place.

vi. **Intercompany reciprocal agreements:** Many reciprocal agreements or mutual support pacts have not been formalized other than by a handshake. Regardless of their formality, reciprocal agreements have been around for a long time and are workable. They are also, however, very fragile and suitable only for a select

few. In order for a reciprocal agreement to be practicable, the following conditions are necessary:

- Each party must have business continuity plan;
- Each must be prepared to invoke its own plan in order to support the injured party, which is often difficult to enforce;
- The critical resource requirements of both must be supportable with the hardware and software of either; and
- Normal installation growth plans must parallel each other.

While there are other requirements for success, these four are critical. No site can expect to support another without impacting its own operation. Until the requirements of each of the potential participants have been defined, the viability of this arrangement is questionable. Until the willingness of each participant is assured, reliance cannot be placed on this alternative.

In addition, reciprocal agreements are often between competitors who have similar configurations based on de facto industry standards. This can be of concern in itself if the information being processed is confidential in nature. Similarly, if the sites are both in the same geographical region, e.g. two banks in the core of a city, such arrangements may not provide coverage for geographical disasters.

This approach can have distinct cost advantages, but will be unlikely to provide for recovery within hours. Availability during regular office hours may also remain a problem if the agreement calls for after hours processing only. Finally, any such agreement should be subject to formal contract and legally binding if it is to be effective.

vii. **Company controlled multiple sites:** It may be appropriate to consider the establishment of a second, company-controlled data processing site in those situations where the critical data processing work load is:

- growing very rapidly;
- able to be subdivided without loss of function or continuity;
- regionally segregable.

Such a site has the added advantage of offering a reasonably quick cut cover, a staff familiar with the processing work load, and security and control environment designed to the company's own standards. The establishment of a second site, however, does not exempt the company from detailed planning necessary to ensure its adequacy or ultimate success. Each site must still be configured to support the combined critical processing load, and both must cooperate in a

controlled site growth program (hardware and software). In addition, the company must be prepared to accept some degree of staff, hardware, and telecommunications redundancy for effective support. While this is clearly an expensive backup option, it can be justifiable.

Where there are a number of wholly-owned or tightly controlled companies within a group, it is possible that a multiple site option could be adopted between member companies, providing there is centralized control and direction of the business continuity planning process. In the case of a large organisation it may be possible to justify a group owned empty shell or hot recovery site, the cost of which will be borne in part by each of the individual operating subsidiaries which make use of it.

The most expensive form multiple site would be the construction of a company specific recovery site. This solution is unlikely to prove cost beneficial for most organisations. It can, however, provide for the fastest recovery, making use of existing communications networks and staff knowledge. Such a site could be used for non-critical functions such as development on an on-going basis.

viii. **Mobile Solutions:** There has been a growth in the number of mobile recovery solutions over the last five years. These trailer based alternatives can be delivered to a client's site within hours or days of a disaster, depending on location.

Most mobile solutions are empty shell facilities providing a computer ready room for installation of replacement equipment. Their major advantage over commercial cold sites is their ability to be located at existing client premises, and, therefore, the possibility of not having to relocate staff if a disaster occurs.

This approach may provide a low cost solution to a decentralized organisation's business continuity needs. The major disadvantage of the mobile or portable solutions is that there may be no suitable place to locate the trailer after a major disaster, and no guarantee that local services will still be available.

ix. **Telecommunications Recovery Options:** The recovery of telecommunications facilities/capabilities is a major issue in today's business continuity plans. Any selected recovery approach must cover two potential disasters, as opposed to the one disaster anticipated by the information systems recovery options. Firstly, the approach must be capable of addressing recovery options. Secondly, the approach must be capable of handling the loss of carrier service, such as through a disaster at the carrier's central office. Disasters of the second nature have received increased coverage in recent years.

In reviewing the options available, each of these important aspects will be considered. In selecting from the alternatives presented, consideration should be given to:

- the use of simple, proven technologies;
- approaches which can be tested;
- approaches which are consistent with normal operating procedures, where possible;
- the minimization of idle charges, for the times when the recovery mode is not in use; and the speed in which the alternative can be activated.

Strategies for Networked Systems

LANs can be implemented in two main architectures:

- Peer-to-Peer — each node has equivalent capabilities and responsibilities. For example, five PCs can be networked through a hub to share data.
- Client/Server — each node on the network is either a client or a server. A client can be a PC or a printer where a client relies on a server for resources.

A LAN's topology, protocol, architecture, and nodes will vary depending on the organisation. Thus, contingency solutions for each organisation will be different. Listed below are some of the strategies for recovery of LANs.

1. **Eliminating Single Points of Failure :** When developing the LAN contingency plan, the organisation should identify single points of failure that affect critical systems or processes outlined in the Risk Assessment. These single points of failures are to be eliminated by providing alternative or redundant equipment.
2. **Redundant Cabling and Devices:** Contingency planning should also cover threats to the cabling system, such as cable cuts, electromagnetic and radio frequency interference, and damage resulting from fire, water, and other hazards. As a solution, redundant cables may be installed when appropriate. For example, it might not be cost-effective to install duplicate cables to every desktop. However, it might be cost-effective to install a redundant cable between floors so that hosts on both floors could be reconnected if the primary cable were cut. Contingency planning also should consider network connecting devices such as hubs, switches, bridges, and routers.
3. **Remote Access:** Remote access is a service provided by servers and devices on the LAN. Remote access provides a convenience for users working off-site or allows for a means for servers and devices to communicate between sites. Remote access can be conducted through various methods, including dialup access and virtual private network (VPN). Remote access may serve as an

important contingency capability. Recovery teams or users from a distant location can access the corporate data even when they are not in a position to reach the physical premises due to some calamity. If remote access is established as a contingency strategy, data bandwidth requirements should be identified and used to scale the remote access solution. Additionally, security controls such as one-time passwords and data encryption should be implemented, if the communication traffic contains sensitive information.

Wireless LANs

Wireless local area networks can serve as an effective contingency solution to restore network services following a wired LAN disruption. Wireless networks do not require the cabling infrastructure of conventional LANs; therefore, they may be installed quickly as an interim or permanent solution. However, wireless networks broadcast the data over a radio signal, enabling the data to be intercepted. When implementing a wireless network, security controls, such as data encryption, should be implemented, if the sensitive information is to be communicated.

Strategies for Distributed Systems

A distributed system is an interconnected set of multiple autonomous processing elements, configured to exchange and process data to complete a single business function. To the user, a distributed system appears to be a single source. Distributed systems use the client-server model to make the application more accessible to users in different locations.

Distributed systems are implemented in environments in which clients and users are widely dispersed. These systems rely on LAN and WAN resources to facilitate user access and the elements comprising the distributed system require synchronization and coordination to prevent disruptions and processing errors. A common form of distributed systems is a large database management system (DBMS) that supports organisation wide business functions in multiple geographic locations. In this type of application, data is replicated among servers at each location, and users access the system from their local server.

The contingency strategies for distributed system reflect the system's reliance on LAN and WAN availability. Based on this fact, when developing a distributed system contingency strategy, the following methods applicable to system backups should be considered for decentralized systems.

viii. Data backups.
ix. Electronic vaulting and remote journaling.
x. Redundant array of inexpensive disks (RAID).

xi. Ensuring redundancy of cables and critical system components.
xii. Storage Virtualization, Network attached Storage (NAS) or Storage Area Network (SAN).
xiii. Remote access.
xiv. Wireless networks.

In addition, a distributed system should consider WAN communication link redundancy and possibility of using Service Bureaus and Application Service Providers (ASPs).

Strategies for Data communications

i. **Dial-up:** Using Dial-up as a backup to normal leased or broadband communications lines remains the most popular means of backing up wide-area network communications in an emergency. This approach requires compatible modems at each remote site and at the recovery location. Ideally, the modems should be full duplex modems which will permit transmission and receipt down the same line. The half-duplex option will require two telephone lines for each data line lost.

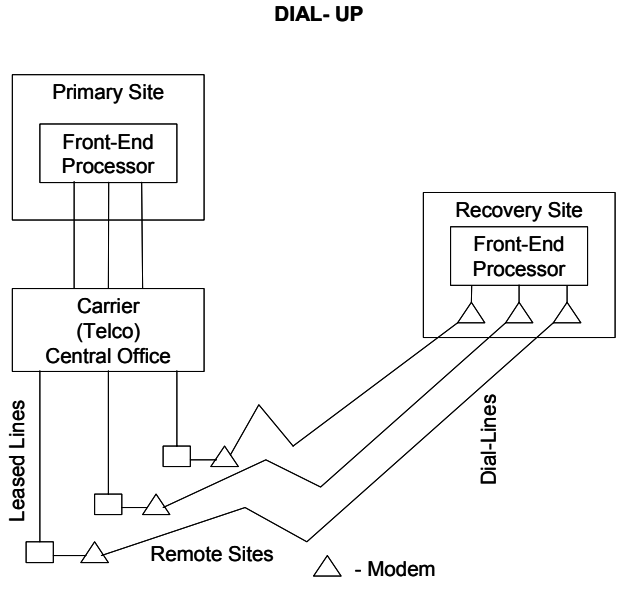


Fig. 2.6: Illustrates dial-up recovery option

Most commercial hot site vendors promote the use of dial backup, particularly for smaller networks. To assist subscribers, most offer a modem pool which can be shipped on notification of disaster to the client's remote sites.

Advantages of Dialup	Disadvantages of Dialup
(a) Low idle state cost	(a) High usage cost
	(b) High error rates
	(c) Inability to handle carrier outage

ii. **Circuit Extension:** Circuit extension techniques are usually applied to high bandwidth communications services, such as high speed leased lines. This technique builds redundancy into the client's network, by including the recovery site as a defined and serviced node. This is illustrated in Fig. 2.7, where the communications from the remote sites can be directed to the primary site or the recovery site from the carrier's central office. This is effective duplication of equipment and facilities, but with some potential for sharing the costs of the equipment at the recovery site.

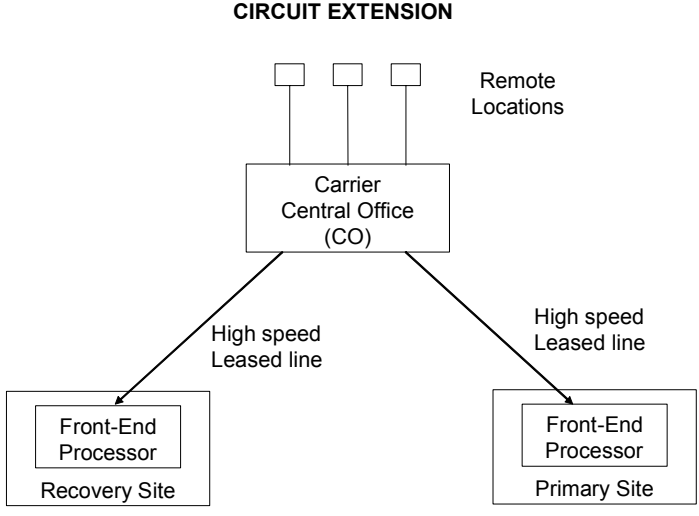


Fig. 2.7: Circuit Extension

Establishing such links on a permanent basis can provide for speedy recovery in a transparent manner. This is also a reliable approach using client's preferred and regular communications method. It will not, however, be effective if the disaster occurs at the central office. This method is also a very expensive approach, since the lines to the recovery site have to be paid for on a regular basis.

iii. **On-demand service from the carriers:** Many carriers now offer on-demand services which provide the mechanisms to switch communications to the

recovery site from the primary site on client notification. This service is provided from the central office. Commonly used method of carrier re-routing is illustrated in Fig. 2.8.

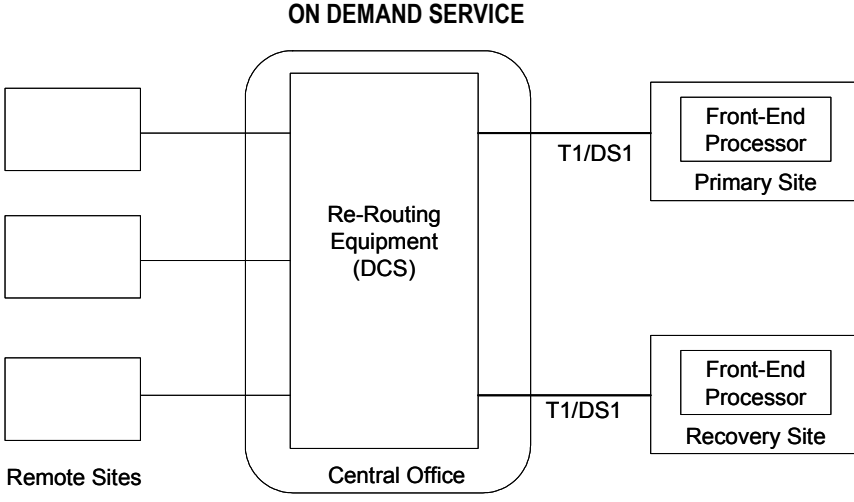


Fig. 2.8: On demand Recovering Strategies

Switched 56 kbps Service: This is used for organizations which do not require full T1/DS1 service. Similar re-routing occurs within the central office but using different re-routing equipment. The major advantage which this approach has over circuit extension is cost. The client does not pay for the lines to the recovery site until they are used. However, this service will not address outages at the carrier's central office.

iv. **Diversification of services:** The use of diverse services provides the best solutions to the loss of a carrier central office. Diversity can be achieved in a number of manners, including: Use of more than one carrier on a regular basis. If the organization uses two or more carriers, it will likely pay above the odds for its regular service and require investment in some additional equipment. For this approach to communications recovery to work, there must also be some redundancy accommodated following any carrier outage.

v. **Microwave communications:** The regular communications can be backed up by the use of microwave communications. This could be used to: backup communications from the central office to the primary site, in case of breakage in the land lines; backup communications from the central office to the recovery centre; or a backup link from a company controlled communications centre direct to the recovery centre. This is illustrated in Fig. 2.9.

MICROWAVE COMMUNICATIONS

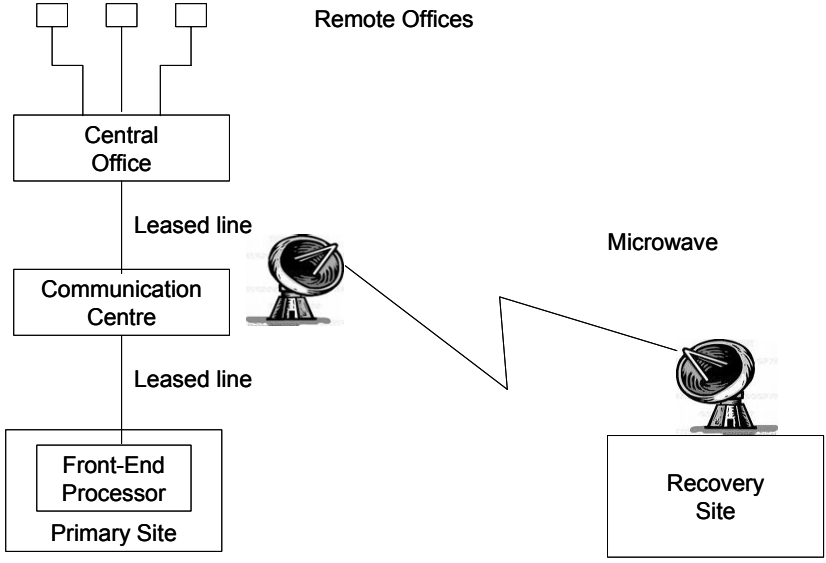


Fig. 2.9: Microwave Communications based Recovering Strategies

Microwave can also be used to link the primary site to a digital switching centre where it can be picked up by another carrier. Generally, this approach will provide good quality communications, but it can itself be impacted by geographic disasters such as earthquakes. The communication charges should not be excessive, but there is a requirement for investment in the microwave towers. Another option, which may be viable, is the renting of mobile equipment in a disaster or investment in a mobile unit to support multiple company locations.

vi. **VSAT (Very Small Aperture Terminal) based satellite communications:** Companies are increasingly looking to VSAT communications as a cost effective means of communicating large volumes of information. This technique could similarly be used to backup the primary carrier service. The use of this technology requires VSAT terminals to be installed at each remote location and at the recovery centre if it does not currently provide such a service. Fig. 2.10 shows an example of how VSAT technologies can be used as a backup technique.

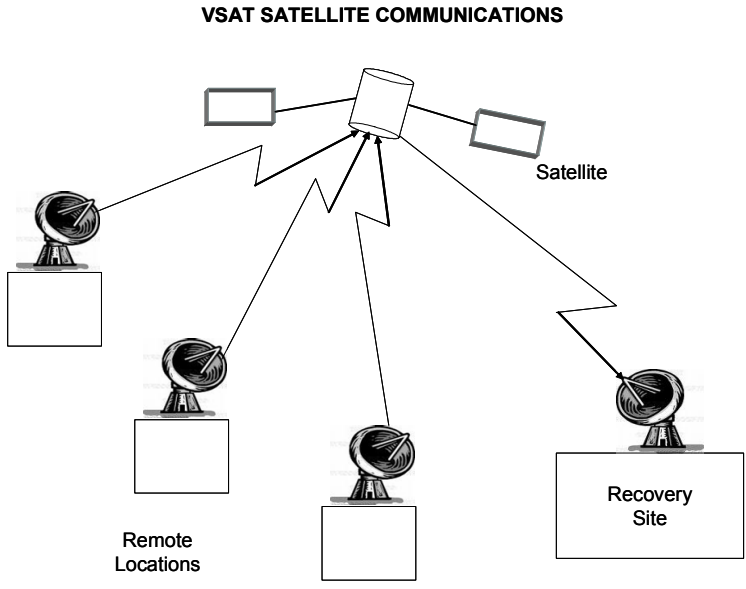


Fig. 2.10: VSAT Satellite Communications

VSAT is an effective means of communicating data up to T1/DS1service levels with low error rates, but is not a viable option for voice. It can be relatively economical, being based on metered usage, but does require an investment in the equipment, unless portable options are available for rent by the client. Where such options are in use and the equipment in place on a regular basis, the client can also perform load balancing on the normal communications traffic to minimize costs and the potential for serious disruption.

Strategies for Voice Communications

Many of the techniques and concerns above relate to voice communications as well as data, and this will continue with the expansion of ISDN services for integrated voice and data communications. Other techniques available for voice recovery include:

i. **Cellular phone backup:** If the regular voice system is inoperative, key employees can be provided with cellular phones as a backup. Given that cellular phones are not run by the major carriers from the same central offices, this also provides coverage for the loss of the central office. Such phones could also be used on an on-going basis and could be used to balance the load on the main PBX switch. Cellular services can also be extended to data and facsimile transmission.

ii. **Carrier call rerouting systems:** Most of the major carriers now provide customers with call rerouting services such that all calls to a given number can be rerouted to another number temporarily. While this will not be possible in the case of a carrier outage, it can be used for the rerouting of critical business communications following a disaster at a client's offices. Calls can be rerouted to a call management service, for example, to support the client in the interim.
iii. **Backup PBX systems:** Although the PBX vendors have improved inter-connectivity, reliance on the use of another vendor's equipment will not be a straight forward solution. In addition, most vendors are not maintaining large inventories of switches or spare parts in their warehouses. As a result, quick delivery of replacement equipment cannot be relied upon. Some PBX suppliers have now started to offer specific disaster recovery services, involving transportable systems capable of linking to local and long distance carriers. These are not available from all vendors or in all areas of the world.

Strategies for Fault Tolerant Implementation

Fault-tolerance is the property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components.

The basic characteristics of fault tolerance require:

xv. No single point of failure.
xvi. No single point of repair.
xvii. Fault isolation to the failing component.
xviii. Fault containment to prevent propagation of the failure.
xix. Availability of reversion modes.

In addition, fault tolerant systems are characterized in terms of both planned service outages and unplanned service outages. These are usually measured at the application level and not just at a hardware level. The figure of merit is called availability and is expressed as a percentage. A five nines system would therefore statistically provide 99.999% availability.

A spare component addresses the first fundamental characteristic of fault-tolerance in three ways:

i. **Replication:** Providing multiple identical instances of the same system or subsystem, directing tasks or requests to all of them in parallel, and choosing the correct result on the basis of a quorum;
ii. **Redundancy:** Providing multiple identical instances of the same system and switching to one of the remaining instances in case of a failure (failover);

iii. **Diversity:** Providing multiple *different* implementations of the same specification, and using them like replicated systems to cope with errors in a specific implementation.

All implementations of RAID, redundant array of independent disks, except RAID 0 are examples of a fault-tolerant storage device that uses data redundancy.

Redundant array of inexpensive disks (RAID) – RAID provides fault tolerance and performance improvement via hardware and software solutions. It breaks up the data to write it in multiple disks to improve performance and / or save large files. There are many methods of RAID which are categorized into several levels. There are various combinations of these approaches giving different trade -offs of protection against data loss, capacity, and speed. RAID levels 0, 1, and 5 are the most commonly found, and cover most requirements.

i. RAID 0 (striped disks) distributes data across several disks in a way which gives improved speed and full capacity, but all data on all disks will be lost if any one disk fails.

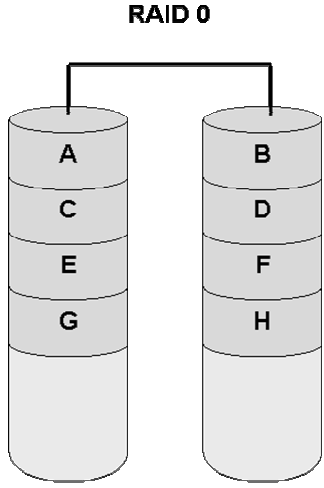


Fig. 2.11: RAID 0

ii. RAID 1 (mirrored disks) could be described as a backup solution, using two (possibly more) disks that each store the same data so that the data is not lost as long as one disk survives. Total capacity of the array is just the capacity of a single disk. The failure of one drive, in the event of a hardware or software malfunction, does not increase the chance of a failure nor decrease the reliability of the remaining drives (second, third, etc).

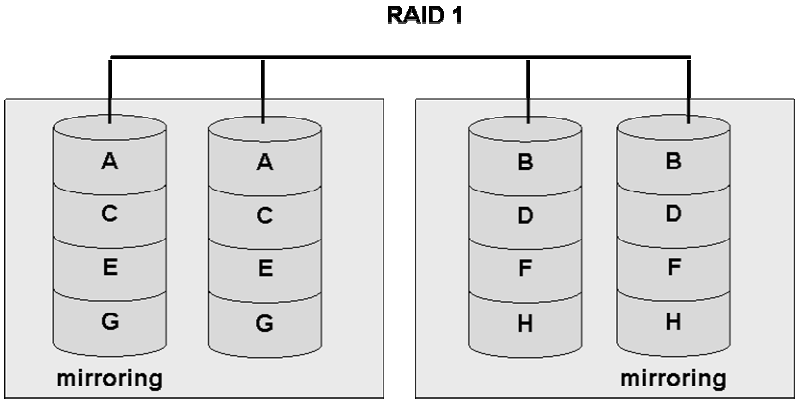


Fig. 2.12: RAID 1

iii. RAID 5 (striped disks with parity) combines three or more disks in a way that protects data against loss of any one disk; the storage capacity of the array is reduced by one disk.

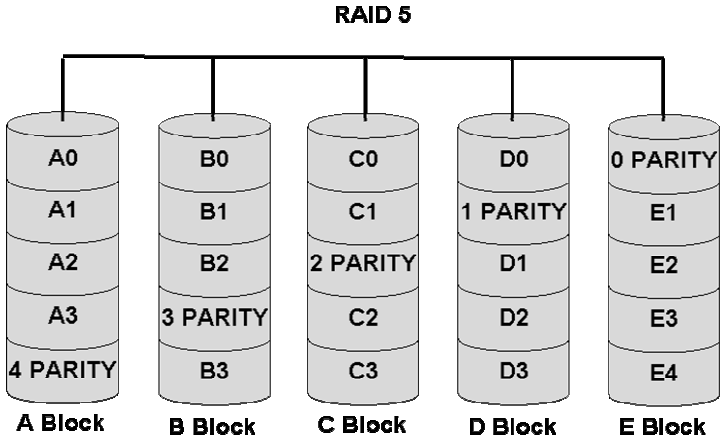


Fig. 2.13: RAID 5

iv. RAID 6 (less common) can recover from the loss of two disks. RAID-6, Independent Data Disks with Double Parity. RAID-6 is essentially an extension of RAID level 5 which allows for additional fault tolerance by using a second independent distributed parity scheme (two- dimensional parity). Data is striped on a block level across a set of drives, just like in RAID 5, and a second set of parity is calculated and written across all the drives; RAID 6 provides for an extremely high data fault tolerance and can sustain multiple simultaneous drive failures.

v. RAID 7 is a very expensive and proprietary (trademark of Storage Computer Corporation). RAID system adds caching to Levels 3 or 4.
vi. RAID 10 combines a very high reliability combined with high performance. It involves creating multiple RAID 1 mirrors and a RAID 0 stripe is created over these disks. RAID 10 has the same fault tolerance as RAID level 1. It is often referred as RAID 1+0, and requires a minimum of 4 drives to implement.

Generally, most organisations use RAID-1 to RAID-5 for data redundancy.

Electronic vaulting – Electronic vaulting is a backup type where the data is backed up to an offsite location. The data is backed up, generally, through batch process and transferred through communication lines to a server at an alternate location.

Remote journaling – Remote journaling is a parallel processing of transactions to an alternate site, as opposed to batch dump process like electronic vaulting. The alternate site is fully operational at all times and introduces a very high level of fault tolerance.

Database shadowing – Database shadowing is the live processing of remote journaling, but creates even more redundancy by duplicating the database sites to multiple servers.

Back up strategies

Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Various backup strategies are:

- **Dual recording of data:** Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
- **Periodic dumping of data:** This strategy involves taking a periodic dump of all or part of the database. The database is saved at a point in time by copying it onto some backup storage medium – magnetic tape, removable disk, Optical disk. The dump may be scheduled.
- **Logging input transactions:** This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump. In case of complete database failure, the last dump is loaded and reprocessing of the transactions are carried out which were logged since the last dump.
- **Logging changes to the data:** This involves copying a record each time it is changed by an update action. The changed record can be logged immediately before the update action changes the record, immediately after, or both.

Apart from database backup strategies as mentioned above, it is important to implement email and personal files backup policies. The policy can be like burning CDs with the folders and documents of importance periodically to more detailed and automated functions. The choice depends and varies with the size, nature and complexity of the situation. For example, individuals are responsible for taking backups of personal files and folders. However, a policy may be there whereby individual users may transfer personal files and folders from the PC to an allocated server space. The data so transferred in the server will be backed up by the IT department as a part of their routine backup. Email backups should necessarily include the address book backup. However, the most important and critical part of the backup strategy is to include a restoration policy. Restoration of the data from the backup media and devices will ensure that the data can be restored in time of emergency; else a failed backup is a double disaster. The restoration should be done for all backups at least twice a year.

Phase IV – Plan Design and Development

Based on the inputs received from Business Impact Analysis (BIA) team, a detailed plan is then developed. It should ideally address all issues involved in a disruption to business processes and recovery from a disaster. The plan should be documented and written in a simple language, so that everyone in the organization and related to the organization including, if necessary, third-party vendors etc. understands it. It should be a part of the plan to develop some important teams with clear cut roles and responsibilities. Some of such important teams are:

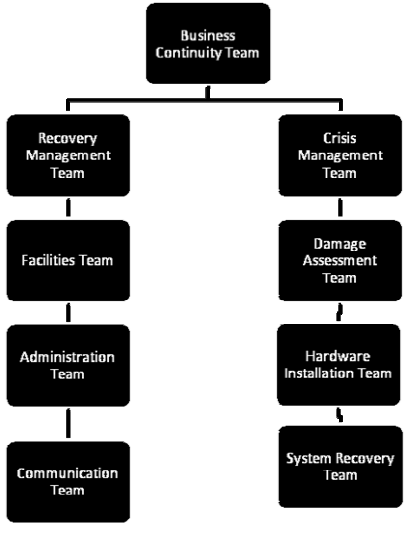


Fig. 2.14: Business Continuity Team

i. **Recovery Management Team:** The recovery management team will oversee and manage any recovery exercise. Leaders of all other teams should form a part of the management team, to ensure that complete and up-to-date information is presented at all status meetings. The business continuity planning coordinator or administrator will be a part of team. Any decisions on revising the recovery process or reacting to changed circumstances will be made by this team. The manager of this team will also report to senior corporate management who are not intimately involved in the process. Even where multiple sites are covered by the plan, the membership of this team will be relatively constant. Only the leaders from the site specific recovery team will vary.

ii. **Crisis Management/Public Relations Team:** Dealing with external agencies or interest groups is an inevitable part of any post-disaster activity. The work performed by this team may extend beyond the provision of details on what has happened, and what is being done to keep the business in operation. For example, this team may also have to handle:

xx. notification of death or injury to next of kin;
xxi. dealing with the media;
xxii. liaison with government or regulatory bodies; and
xxiii. handling public concerns if the disaster has health or environmental implications.

To be effective, this team must have all of the necessary information at their disposal and include appropriate senior corporate officials who are comfortable in dealing with the media and relaxed in front of cameras. Mishandling public relations can severely damage an organization's reputation and cause more harm than the disaster itself.

Dealing with the media is a skill which must be developed, and there are consulting firms which specialize in this service. In addition to being comfortable in the handling of the media, this team must have a predefined plan for issuing statements, an agreed location for making those statements and an understanding of the level of information to be issued. Experience has shown that saying nothing or "no comment" can be more costly to the organization than providing full and open disclosure. If the media cannot get the information from official sources, it is very good at finding other, not necessarily reliable, information from other sources.

The crisis management team or public relations team must be thoroughly prepared to handle the media and all other external communications. Appropriate spokespersons should be identified and trained.

i. **Hardware Installation Team:** In today's business environment, it is likely that a recovery operation will require the installation of some computer equipment. This

may include the ordering and installation of a replacement data centre, the installation of the specific terminals and printers required by the impacted business unit, or even the replacement of microcomputers.

ii. **System recovery Team:** Once the hardware team has completed its job, the system recovery team will be responsible for installing the necessary software, recovering data backup and ensuring that the recovered systems are capable of supporting the critical business functions.

iii. **Communications Team:** The communications team is responsible for handling the re-routing or re-connection of the essential voice and data communications. Because of the specialized nature of the communications functions, many large and decentralized organizations still maintain a centralized communications group.

iv. **Facilities Team:** Ensuring a smooth transition to temporary premises, and the restoration or replacement of the primary premises is among the responsibilities of the facilities team. This team may also be responsible for equipping the premises with furniture, office supplies and other facilities.

v. **Administration Team:** The various recovery teams will each require administrative support. This will be one of the functions of the administration team. Administration team staff may also be responsible for such matters as staff travel arrangements, catering, petty cash control, telephone services, mail services, and some personnel functions.

vi. **Damage Assessment Team:** Damage assessment will be one of the first activities performed after a disaster occurs. Depending on the nature of the operations at the site impacted, the performance of such an assessment may require a number of different skill sets.

vii. Other teams which may be established include:

- **Application recovery teams** – to recover specific critical application systems.
- **Logistics team** – to assist in team coordination, if staffs are located at geographically separate sites for recovery purpose. This team can handle the distribution of mail and reports, movement of input documents and media, etc.
- **Staff coordination team**- responsible for keeping staff informed of the situation and providing interim financial assistance to families, where required. Employees can be great representatives in times of stress, but can also cause problems if they feel mistreated.
- **An insurance team**- responsible for turning the damage assessment information into timely insurance claims.

- **User liaison team** – responsible for communications between a data centre recovery site and the remote users of that site.

Once the teams have been established and their responsibilities agreed upon, details of the teams should be entered into the plan. This does not require step by step procedures, but an overview of each team's responsibilities and understanding of the interaction required between the teams.

Elements of a Business Continuity Plan Manual

The BCP plan will contain the following elements:

i. **Purpose of the plan:** This section should contain a summary description of the purpose of the manual. It should be made clear that the manual does not address recovery from day to day operational problems. Similarly, it must be stressed that the manual does not attempt to foresee all possible disasters, but rather provides a framework within which the management can do base recovery from any given disaster.

ii. **Organisation of the manual:** A brief description of the organization of the manual, and the contents of each of the major sections, will provide the reader with the direction to the relevant section of the manual in an emergency situation. Any information which is external to the manual but will be required in an emergency should be identified in this section.

iii. **Disaster definitions:** It may assist the user of the manual if a definition of disaster classification is provided, together with an identification of the relevance of the plan to that situation. Four types of classification can generally be used:

   i. Problem – Problem/Incident: Event or disruptions that cause no significant damage.
   ii. Minor disaster – Event or disruption that causes limited financial impact.
   iii. Major disaster – Event or disruptions that cause significant impact and may have an effect on outside clients.
   iv. Catastrophic disaster – Event or disruptions that have significant impact and adversely affect the organization's "going concern" status.

The BCP manual of each organisation is expected to classify disasters, after taking into account the size and nature of its business.

The time and cost associated to each kind of disaster should be defined as per the requirement of the individual organization. It should be noted, however, that development of a plan based on each classification is not recommended. The need to invoke the plan should be determined by the length and associated cost of the

expected outage and not the classification of the disaster, although there is a direct correlation. These definitions will be most useful for communication with senior management.

1. **Objectives of the plan:** The objectives of the manual should be clearly stated in the introductory section. Typically, such objectives include:

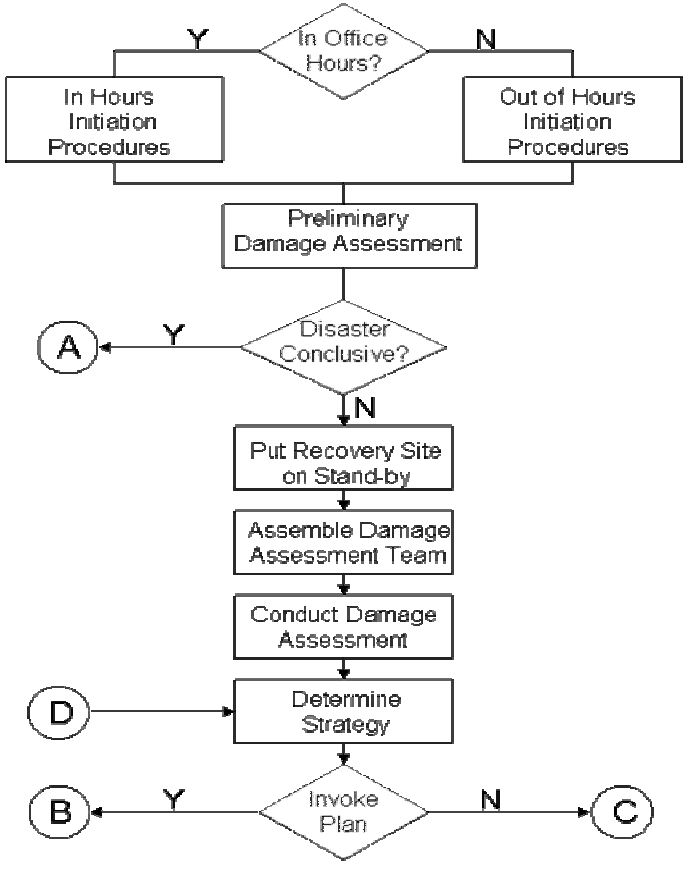
   xxiv. Safety/security of all personnel. The paramount objective of a BCP is to ensure the safety and security of people (both employees and others who may be affected in the event of a disaster). The safeguarding of assets/data is always a secondary objective.
   xxv. The reduction of confusion in an emergency.
   xxvi. The identification of critical application systems and / or business functions.
   xxvii. The identification of all resources, including personnel, required to recover the critical business functions.
   xxviii. The identification of alternative means to ensure that the critical business functions are performed and
   xxix. The establishment of a workable plan to recover the critical business functions, and subsequently resume normal operations, as quickly as possible after a disaster.

   The list should be expanded as necessary to meet the requirements of any given plan.
2. **Scope of the plan:** In order that there is no confusion as the situations in which the plan will apply, the scope of the plan must be clearly identified. Any limitations must be explained.
3. **Plan approach / recovery strategy:** A step by step summary of the approach adopted by the plan should be presented. For ease of reference, it may be good to provide this overview by means of a schematic diagram. In particular, it may be useful to set up the recovery process as a project plan in this section.
4. **Plan administration:** The introductory section should also identify the person or persons, responsible for the business continuity plan manual, and the expected plan review cycles. These persons will be responsible for issuing revisions which will ensure that the plan remains current. Because the manual will include staff assignments, it is also advisable that the personnel or human resource function accept responsibility for notifying the plan administrators of all personnel changes which must be reflected in the plan.
5. **Plan management:** Following a disaster, the normal reporting channels and lines of management are unlikely to be strictly adhered to. During a disaster, reporting by exception may be the only feasible way to operate. This does not,

however, negate the requirement for formalized management. The management responsibilities and reporting channels to be observed, during disaster recovery should be clearly established in advance.

6. **Disaster notification and plan activation procedures:** The procedures represent the first steps to be followed when any disaster occurs. It is recommended that the procedures be written in a task-oriented manner and provide a logical flow to enable ease of management. A sample outline of a set of disaster notification procedures is given below:

DISASTER NOTIFICATION AND PLAN ACTIVATION



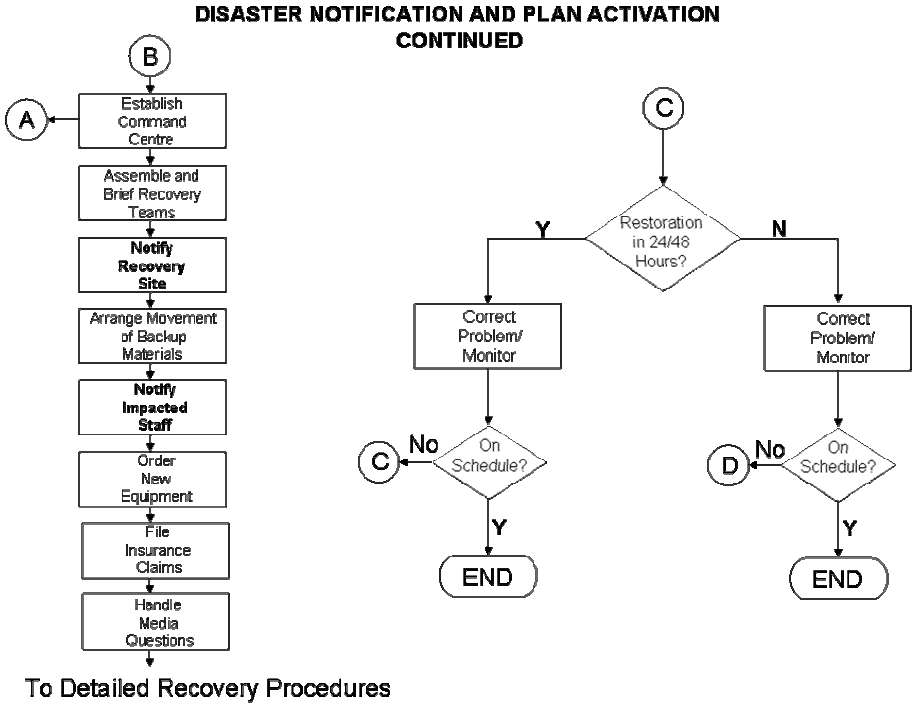


Fig. 2.15: Disaster Notifications and Plan Activation

- **Initiation procedures:** The notification procedures will ensure that the organisation's appropriate officials are contacted on a timely basis when a disaster event occurs. These procedures will involve the contact of key staff.
- **Preliminary damage assessment:** Once management has been notified of the problem, a preliminary damage assessment should be performed. This need not be a detailed assessment, but will provide an initial indication as to whether the plan needs to be activated.
- **Put recovery site on standby:** Where the BCP involves the use of a commercial recovery centre, that site should be put on notice. Most vendors do not charge for being put on notice and appreciate an advance warning.
- **Assemble damage assessment team:** If the preliminary assessment is not conclusive, the full damage assessment team can be assembled. If all staff is on site when disaster strikes, this should be a relatively easy task. However, if the incident occurs after office hours it will be necessary to call the staff at home to notify all team members of the problem.
- **Conduct damage assessment:** The damage assessment process should be conducted as soon as possible following disaster notification. The

assessment of the extent of the damage, possible duration of service disruption, and job processing status will directly impact the subsequent course of recovery action. The assessment process should consider the impact on:

- the facilities
- power and other utilities
- the environment and
- essential equipments.

- **Determining strategy:** The identification of the most appropriate strategy will typically require a decision by the recovery management team, based on the damage assessment report. Once an appropriate strategy has been identified, the adoption of that solution must be approved by the senior management.
- **Establish emergency command centre:** While it may not be necessary to establish command centre for the damage assessment team alone, once the decision has been made to invoke the plan it will be necessary to activate that location. All members of the teams responsible for recovery of the management should assemble at an identified Emergency Command Centre. This centre must be established at a predefined location within easy access of the primary site, but sufficiently far removed, so that it will not be affected by a disaster event. It is from this site that recovery operations will be directed.
- **Assemble and brief recovery teams:** This effects the notification of all team members to report to the command centre. This should include:
  - Giving details of who is calling.
  - Providing a brief synopsis of disaster status.
  - Instruction to call all staff or alternates on the list of the person being called.
  - Instruction on where to report, when and with what materials and
  - A record of all calls made should be retained.
- **Notify recovery site:** The recovery to be used including any commercial sites, should be notified of the decision to use the facility and requested to prepare the site in accordance with the contract.
- **Arrange movement of backup materials:** Once the decision is made to move to the recovery site, all of the necessary materials should be recovered from off-site storage and shipped to that location. The shipment of any required special forms from backup supplies should also be coordinated at this time.

- **Notify impacted staff:** Once the recovery operations are under way, the staff that will be impacted but will not be required for recovery activities should also be notified. It is preferable that they receive the notification from the organisation rather than from the media.
- **File Insurance claims:** It may not be possible to file the claims immediately, as further damage assessment may still be required However, as soon as the necessary information is available, the claims should be prepared.
- **Detail procedures for recovery:** A step by step instructions for recovering systems at recovery site should be written down. Some of instructions are:
    - assemble and check site
    - check off site materials
    - install equipment
    - test operating system
    - recover applications
    - test applications
    - hire temporary staffs
    - update to disaster (if the recovery site is not shadowing all data processed at the primary site, data entry up to the state of disaster will be entered again at the recovery site)
    - process backlog
    - configure networks
    - test network
    - establish external links
    - redirect mail
    - redirect communications
    - correct problem / monitor
    - establish controls.

7. **Primary site procedures:** While the detailed recovery procedures are concentrated on alternate facilities to restore the critical business operations, the primary site should be built up again. Steps remain to be taken in that location following the damage assessment and the decision to invoke the plan.
8. **Return to normal operations:** Once the primary site is refurbished or a new primary site is available, it is necessary to relocate to that site.
9. **Post recovery reviews:** Once the return to normal operations has been completed and approved, the normal job schedules and operating instructions should be reintroduced. In addition, a review of the recovery operations should be performed to identify any areas in which the plan can be improved. This post-mortem should be performed as soon as possible to ensure that the concerns and problems experienced are still clear in staffs' minds.

Phase V – Testing, Maintenance, Awareness and Training

Once the BCP plan is developed, it must be subjected to rigorous testing. The testing process itself must be properly planned and should be carried out in a suitable environment to reproduce authentic conditions in so far as this is feasible. The plan must be tested by those persons who would undertake those activities if the situation being tested occurred in reality. The test procedures should be documented and the results recorded. This is important to ensure that a feedback is obtained for fine tuning the plan. Equally, it is important to audit both the plan itself and the contingency and back up arrangements supporting it. No short cut can be made here.

There are five main types of tests and they are:

1. Checklist test
2. Structured walk through test
3. Simulation test
4. Parallel test
5. Full interruption test

1. **Checklist test:** In this type of test, copies of the plan are distributed to each business unit's management. The plan is then reviewed to ensure that the plan addresses all procedures and critical areas of the organization. In reality, this is considered as a preliminary step to real test and is not a satisfactory test in itself.
2. **Structured walk through test:** In this type of test, business unit management representatives meet to walk through the plan. The goal is to ensure that the plan accurately reflects the organisation's ability to recover successfully, at least on paper. Each step of the plan is walked through in the meeting and marked as performed. Major faults with the plan should be apparent during the walk through.
3. **Simulation test:** In this type of test, all of the operational and support personnel who are expected to perform during an actual emergency meet in a mock practice session. The objective is to test the ability and preparedness of the personnel to respond to a simulated disaster. The simulation may go to the point of relocating to the alternate backup site or enacting recovery procedures, but does not perform any actual recovery process or alternate processing.
4. **Parallel test:** A Parallel test is a full test of the recovery plan, utilizing all personnel. The difference between this and the full interruption test is that the primary production processing of the business does not stop, the test processing runs in parallel to the real processing. The goal of this type of test is to ensure that critical systems will actually run at the alternate processing backup site. Systems are relocated to the alternate site, parallel processing backup site, and

the results of the transactions and other elements are compared. This is the most common type of disaster recovery plan testing.

5. **Full interruption test:** During a full interruption test, a disaster is replicated even to the point of ceasing normal production operations. The plan is implemented as if it were a real disaster, to the point of involving emergency services. This is a very severe test, as it can cause a disaster on its own. It is the absolute best way to test a disaster recovery plan, however, because the plan either works or does not.

Documentation of results: During every phase of the test, a detailed documentation of observations, problems and resolutions should be maintained. This documentation can be of great assistance during an actual disaster. They are also helpful in improving and maintaining the plan as they reveal the strengths and weaknesses of the plan.

No test is ever a failure because, however badly it may seem to have gone lessons can still be learnt from it. However, it should be remembered that if a test is not planned properly, it could actually create a disaster. Live tests especially could create a disaster if not planned properly because they use real people and real resources in real conditions, probably during normal working hours. Live tests should only be considered after the BCP has been tested in full and all Recovery Team members fully trained. The worst way to test a Plan is to turn off the power suddenly, for example, and tell people to exercise their Recovery Plans, the interruption and delay to normal work could well become a disaster in itself.

Results Analysis: The results of each test should be recorded to identify:

xxx. what happened;
xxxi. what was tested successfully; and
xxxii. what needs to be changed?

If a test indicates that the BCP needs to be changed, the change should be made and the test repeated until all aspects are completed satisfactorily. When all the components have been tested satisfactorily, the whole BCP is ready for testing. It should not be assumed that because the components work individually there is no need to test the whole BCP. Putting it all together may reveal problems which did not show up in lower level testing. When preparing for testing, the participants should be given all the information and instruction they need.

Plan Maintenance: The plan must always be kept up to date and applicable to current business circumstances. This means that any changes to the business process or changes to the relative importance of each part of the business process must be properly reflected within the plan. Most commonly network changes or

changes in computing infrastructure may change the location or configuration of hardware, software and other components. Someone in the senior management must be assigned the responsibility for ensuring that the plan is maintained and updated regularly and should, therefore, ensure that the information concerning changes to the business processes is properly communicated. Any changes or amendments made to the plan must be fully tested. Personnel should also be kept abreast of such changes in so far as they affect their duties and responsibilities.

The best way to ensure that a BCP is up to date is to test it, train staff in how to use it, and review it regularly.

Awareness and Training: From the start of the BCP development project, positive action to create awareness of the BCP during the development, testing and training phases should be taken by holding briefings for all staff at an early stage of BCP development to explain the reasons for the BCP and its benefits to everyone and how it will be developed; The organisation should take care that all new staff are briefed about the BCP as a part of their induction to the department.

It should be remembered that every test also trains the participants. If the full Recovery Teams are not used in each test, the participants should be rotated so that they all gain an adequate experience.

At the end of the testing phase, further training and experience requirements should be identified. The Recovery Team leaders should be consulted for their opinions as they should have the best understanding of the present abilities of their Team members. The training methods to be used may include:

xxxiii. walkthrough session;
xxxiv. scenario workshop; or
xxxv. live test simulation; and

Walkthrough Session: For a walkthrough session, the participants sit round a table, each with a copy of the BCP (or appropriate part of the BCP), and `walk' through it by reading and discussing each part in sequence.

Walkthrough sessions should be conducted at a quiet place without interruption because the objective is to identify any weaknesses, errors and omissions by allowing participants' thoughts to flow freely as they go through the plan. The only limit on discussion is that the whole part must be read to the end.

All components of the BCP should first be tested using this method as it is highly likely to identify changes needed. One good walkthrough per component is usually sufficient if the suggested changes are then reviewed and agreed by a few of the testers.

A suitable BCP component for testing using this method would be the complete plan for one Recovery Team. Links with other Teams should be noted and raised during their walkthroughs.

Scenario Workshop: This is similar to a walkthrough except that a scenario is devised before the workshop, and at least the key members of the Recovery Teams must be involved, although it is preferable to include all Teams. Scenarios should be designed:

xxxvi. around the actual conditions of the premises and its operations;
xxxvii. to introduce any possible disaster in a realistic way;
xxxviii. to give a good testing of the plan;
xxxix. to include developments that would usually occur during a disaster, for example, changes in safety conditions delaying return to the premises.

Participants should sit round a table at a quiet place without interruption with their copies of the BCP (or appropriate part of the BCP), but instead of reading through the whole BCP, they should role-play their participation in the scenario. As they do so, they should say aloud what they are thinking and doing. The objective is to identify errors, omissions and weaknesses, and to establish whether the plan performs as intended. For this method to be effective, participants must:

xl. accept the scenario at face value;
xli. become fully involved in the role play; and
xlii. voice all their thoughts and imagined actions. Brief interruptions to a participant's spoken thoughts and actions are permitted if other participants have constructive comments or questions.

As the scenario progresses the lead participant(s) may change as appropriate to the timescale of the plan, particularly if the whole BCP is being tested rather than one Recovery Team's Plan. Participants need to be aware of this possibility so that it happens smoothly in the right places.

Simulation of a Live Test: Simulation of a live Test should:

xliii. be held outside normal working hours so that resources can be used without affecting normal operations;
xliv. involve the use of the planned and contracted contingencies if this is practical;
xlv. relocate some staff to another site if appropriate; and
xlvi. be as near to real life as possible so that all aspects of the BCP, including contingencies, are tested.

Because it is a test, some shortcuts may be taken, such as sending only a token number of people to the contingency site, or doing only token amounts of work to

prove that the operation has been successfully recovered. However, even if shortcuts are used it must still be possible at the end of the test to conclude that all aspects of the BCP are effective. A simulation of a live test, perhaps more than the other methods, needs to be carefully planned to:

xlvii. ensure that the testing is thorough;
xlviii. avoid confusion when things go wrong; and
xlix. prevent any disruption to the real operations.

Reviewing the BCP: The BCP should be reviewed to identify changes, and to ensure that the business unit's recovery requirements are up-to-date. Such reviews should be carried out at specified intervals, usually annually but more often if the rate of change is high. Keep a record of review dates.

Remember that whenever the BCP is amended, the latest version must be distributed to all holders and the old versions destroyed. Successful recovery could be jeopardized if anyone is working according to an older version.

Summary

A BCP is not merely about systems, it is about people. In a crisis, people have to assume responsibilities that are different from their normal day to day tasks. This requires a series of coordinated actions on the part of the personnel involved. The BCP should, therefore, lay down the notification procedure and transportation and other arrangements that will enable effective recovery. A BCP is rarely a standalone document. It is, usually, part of a set of documents. There may be an organisation-wide BCP and facility-wise DRP. There may be a separate plan, the Cyber Incident Response Plan, to take care of threats like computer viruses and network intrusions. An Occupant Emergency Plan (OEP), may be in use for the evacuation of premises during a fire or medical emergencies. Insurance is yet another tool that supplements a BCP. Monetary losses can be minimised by transferring certain risks to an insurance company on the payment of a premium. A BCP that exists on paper without being tested serves no useful purpose. The worst possible way to "test" a BCP is to see whether it works during a real disaster. Ideally, while framing the objectives of the BCP, the organisation spells out the "acceptance criteria", that is, the tests that will validate the BCP. Testing a BCP can be a complex undertaking as many personnel will have to carry out the tests even while continuing with normal operations.

Checklist for a Business Continuity Plan

Process Objectives

I. To seamlessly recover from the disaster situation.
Ii. To reduce the impact of the damage of the assets, in turn reducing the data loss.
Iii. To assure compliance and
Iiii. To sustain operations so that customer service and corporate image can be maintained.

Sr. No.	Checkpoints/ Particulars
Policy and procedure	
1.	Is business continuity plan documented and implemented?
2.	Whether the scope and objectives of a BCP are clearly defined in the policy document? (Scope to cover all critical activities of business. Objectives should clearly spell out outcomes of the BCP).
3.	Are the policy and procedure documents approved by the Top management? (Verify sign off on policy and procedure documents and budget allocations made by the management for a BCP).
4.	Does the business continuity plan ensure the resumption of IS operations during major information system failures? (Verify that the IS disaster recovery plan is in line with strategies, goals and objectives of corporate business continuity plan).
5.	Are users involved in the preparation of business continuity plan? (Managerial, operational, administrative and technical experts should be involved in the preparation of the BCP and DRP).
6.	Does the policy and procedure documents include the following List of critical information assets. List of vendor for service level agreements. Current and future business operations. Identification of potential threats and vulnerabilities. Business impact analysis. Involvement of technical and operational expert in preparation of BCP and

Sr. No.	Checkpoints/ Particulars
	DRP plans. Recovery procedure to minimize losses and interruptions in business operations. Disaster recovery teams. Training and test drills. Compliance with statutory and regulatory requirements.
7.	Are the BCP policy and procedures circulated to all concerned? (Verify availability and circulation of the BCP & DRP to all concerned, including onsite and offsite storage).
8.	Is the business continuity plan updated and reviewed regularly? (Verify minutes of meeting where policy and procedures are reviewed. Verify amendments made to the policy and procedure documents due to the change in business environment).
Risk Assessment	
1	Has the management identified potential threats/vulnerabilities to business operations? (Verify the business environment study report. Risk Assessment Report?)
2	Are the risks evaluated by the Management? (Verify the probability or occurrence of the threat / vulnerability review carried out by the management).
3.	Has the organisation selected the appropriate method for risk evaluation?
4.	Has the organisation carried out the assessment of internal controls? (Verify the internal controls mitigating the risk).
5.	Has the organisation taken an appropriate decision on the risks identified? (Verify the decision-making on the options - accepted, reduced, avoided or transferred – for the risks identified).
6..	Are the risk assessment carried out at regular interval? (Verify the review frequency.)
Business Impact Analysis	
1.	Does the organisation carry out business impact analysis (BIA) for business operations?

Module – IV

Sr. No.	Checkpoints/ Particulars
2.	Has the organisation identified a BIA Team?
3.	Are RTO and RPO defined by the management?
4.	Whether the organisation has measured BIA? (Impact of risks on business operations can be measured in the form of business loss, loss of goodwill etc.).
5.	Is the business impact analysis carried out at regular interval?
Development & Implementation of the BCP & DRP	
1.	Has the organisation prioritised recovery of interrupted business operations? (Prioritization of activities is based on RTO and RPO).
2.	Has the organisation identified the various BCP & DRP Teams? (Verify employees are identified, informed and trained to take an action in the event of disaster).
3.	Are the responsibilities for each team documented? (Verify the roles and responsibilities assigned to employees for actions to be taken in the event of incident / disaster).
4.	Does the BCP document(s) include the following? Scope and objective. Roles and responsibilities of BCP and DRP Teams. Incident declaration. Contact list. Evacuation and stay-in procedure. Activity priorities. Human resource and welfare procedure. Escalation procedures. Procedure for resumption of business activities. Media communication. Legal and statutory requirements. Backup and restore procedures. Offsite operating procedures
5.	Are the copies of up-to-date BCP documents stored offsite?
6.	Does the offsite facility have the adequate security requirements?

Sr. No.	Checkpoints/ Particulars
	(Verify the logical access, physical access and environmental control of the offsite).
7.	Does the BCP include training to employees? (Verify the evidences of training given).
8.	Whether the organisation has an adequate media and document backup and restoration procedures? (Verify the backup and restoration schedules adopted by the organisation)
9.	Are logs for backup and restoration maintained and reviewed? (Verify the logs maintained and review of the same by an independent person).
10.	Whether the media library has an adequate access control? (Verify the physical and logical access controls to the media library).
11.	Are the BCP and DRP communicated to all the concerned? (Verify availability and circulation of BCP & DRP to all concerned, including onsite and offsite storage).
Maintenance of BCP & DRP	
1.	Whether the business continuity plan is tested at regular interval?
2.	Has the organisation reviewed the gap analysis of testing results? (Review process that includes a comparison of test results to the planned results).
3.	Has the organisation got a testing plan? (Verify copy of test plan and updates).
4.	Are test drills conducted at appropriate intervals?
5.	Do organisation documents and analyses have testing results? (Verify the corrective copies of test results and analysis of the report).
6.	Has the organisation prepared action points to rectify the testing results? (Verify the corrective action plan for all problems encountered during the test drill).
7.	Does the organisation carry out retesting activity for action points? (Verify the evidences of retesting activities).
8.	Does the organisation review the BCP and DRP at regular intervals?

Module – IV

Sr. No.	Checkpoints/ Particulars
9.	Whether a review of the BCP includes following? BCP policy and procedure Scope and exclusion of BCP Inventory of IS assets Validating assumption made while risk assessment and preparation of BCP and DRP Risk assessment Business impact analysis Back up of system and data Training to employees Test drills

Questions:

Q1. The correct order of the steps for developing a BCP is:
   a. Initiate Risk assessment, choose a recovery strategy, Testing and validation, Develop and implement.
   b. Initiate, Choose a recovery strategy, Risk assessment, Develop and implement, Testing and validation.
   c. Initiate Risk assessment, Choose a recovery strategy, Develop and implement, Testing and validation.
   d. Risk assessment, Initiate, Choose a recovery strategy, Develop and implement, Testing and validation.

Q2. Enhanced risk awareness and more emphasis on the importance of good risk measurement and management and properly ensured appropriate capital reserve requirements is a requirement of:
   a. Basel Committee's principles for electronic banking
   b. Basel II Capital Accord
   c. COBIT
   d. ISO/IEC 17799:2000.

Q3. Banks must demonstrate that they have an overall data architecture that integrates the various business functions from operations to finance to risk management if they are to achieve compliance with:
   a. ISO/IEC 17799:2000

b. SAS 70
c. Basel Committee's principles for electronic banking
d. Basel II Capital Accord.

Q4. The Generally Accepted System Security Principles (GASSP) is in- tended to provide authoritative point of reference and legal reference for information security principles, practices, and opinions. These principles were modelled after:
a. Basel II Capital Accord
b. SAS 70
c. The Generally Accepted Accounting Principles (GAAP)
d. ISO/IEC 17799:2000.

Q5. The order of steps in the process of risk assessment for the purpose of a BCP is:
a. Asset identification and prioritization, Threat identification, Exposure assessment, Objective formulation.
b. Objective formulation, Threat identification, Exposure assessment, Asset identification and prioritization.
c. Asset identification and prioritization, Exposure assessment, Threat identification, Objective formulation.
d. Objective formulation, Asset identification and prioritization, Threat identification, Exposure assessment.

Q6. The maximum amount of time allowed for the recovery of the of the business function is called the
a. Maximum Recovery Time Period
b. Critical Recovery Time Period
c. Minimum Recovery Time Period
d. Vital Recovery Time Period.

Q7. Business functions that cannot be done manually under any circumstances are classified as:
a. Vital
b. Essential
c. Critical
d. Non-critical.

Q8. Within any complex system, there are usually components or processes that, if not replicated or otherwise backed up by redundant capabilities, represent points of failure for the entire system. These are called

a. Multiple points of failure
b. Cascading points of failure
c. Linear points of failure
d. Single points of failure.

Q9. Business functions that can be performed manually but only for a brief period of time are usually classified as:
a. Vital
b. Essential
c. Desirable
d. Critical.

Q10. Objectives of risk assessment include:
a. Sensitizing business processes
b. Prioritizing business processes
c. Criticising business processes
d. Evaluating business processes.

Q11. Risk assessment consists of:
a. Data collection
b. Data analysis
c. Data collection and data analysis
d. Data collation.

Q12. During an exposure assessment, the effects of a disruption may be tracked:
a. Over time
b. Across related resources and dependent systems
c. On the basis of historical costs
d. Over time and across related resources and dependent systems.

Q13. Elimination of all risks is usually:
a. Impractical or impossible
b. Easy to achieve
c. Vital to the survival of the company
d. Recommended by law.

Q14. Single points of failure are:
a. Recommended
b. To be eliminated
c. Desirable.

d. To be encouraged.

Q15. Data or documentation that must be retained for legal reasons, for use in key business processes, or for restoration of minimum acceptable work levels in the event of a disaster is classified as:
a. Desirable
b. Vital
c. Essential
d. Critical.

Q16. Data that can be reconstructed fairly readily but at some cost is classified as:
a. Critical
b. Essential
c. Sensitive
d. Vital.

Q17. Which of the following media has the least backup capacity?
a. Removable Cartridges
b. Floppy Diskettes
c. Compact Disk
d. Tape Drives.

Q18. When backups of data and system files are taken together, they are often called:
a. Systems backup
b. Data backup
c. Incremental backup
d. Differential backup.

Q19. Backup media should be stored:
a. On-site in a secure, environmentally controlled location
b. Off-site in a insecure, environmentally controlled location
c. On-site in a insecure, environmentally controlled location
d. Off-site in a secure, environmentally controlled location.

Q20. Identify the correct statement:
a. Both differential and incremental backups take the same amount of time
b. Incremental backups take longer to complete than differential backups
c. Differential backups take longer to complete than incremental backups
d. Incremental backups take longer when using tape drives.

Module – IV

Q21. Which of the following is NOT a type of system backup?
   a. Incremental
   b. Sequential
   c. Differential
   d. Full.

Q22. Which of the following technical methods for Backup does not require restoration?
   a. Electronic Vaulting
   b. Networked Disk
   c. Tape Drives
   d. Remote Mirroring.

Q23. A common backup method for portable computers is:
   a. Electronic Vaulting
   b. Tape Drives
   c. Remote Mirroring
   d. Synchronization.

Q24. Which of the following type of system backup would require the maximum storage?
   a. Incremental
   b. Sequential
   c. Full
   d. Differential.

Q25. Which of the following is the MOST reliable strategy for centralized systems?
   a. Cold site
   b. Reciprocal Agreement
   c. Hot Site
   d. Mirror site/Active Recovery Site.

Q26. Which of the following is the LEAST reliable strategy for centralized systems?
   a. Mobile Site
   b. Hot Site
   c. Reciprocal Agreement
   d. Mirror site/Active Recovery Site.

Q27. The process of combining multiple physical storage devices into a logical, virtual storage device that can be centrally managed and is presented to the

network applications, operating systems, and users as a single storage pool is called:

a. RAID
b. Storage virtualization
c. WAN
d. SAN.

Q28. A file-oriented environment that offers a common storage area for multiple servers and which allows any application residing on or any client using virtually any operating system to send data to or receive data is called:

a. Network-Attached Storage (NAS)
b. Remote Access Storage (RAS)
c. Redundant Array of Inexpensive Disks (RAID)
d. Storage Area Network (SAN).

Q29. A high-speed, high-performance network that enables different servers with different operating systems to communicate with one storage device is called:

a. Network-Attached Storage (NAS)
b. Remote Access Storage (RAS)
c. Redundant Array of Inexpensive Disks (RAID)
d. Storage Area Network (SAN).

Q30. Which of the following is NOT data redundancy techniques used by RAID technology?

a. Mirroring
b. Parity
c. Blocking
d. Striping.

Q31. Which of the following RAID levels is NOT recommended as a data recovery solution?

a. RAID-1
b. RAID-0
c. RAID-10
d. RAID-100.

Q32. The technique that allows traffic to be distributed dynamically across groups of servers running a common application so that no one server is overwhelmed is called:

a. Server Load Balancing

b. Alternative Routing
c. Diverse Routing
d. Storage Area Network.

Q33. Among strategies for telecommunications systems, the strategy that involves the use of different networks, circuits or end points when the primary telecommunication facility is unavailable is called:
a. Distributed Routing
b. Associative Routing
c. Diverse Routing
d. Alternative Routing.

Q34. Which of the following techniques used by RAID technology increases performance?
a. Mirroring
b. Parity
c. Striping
d. Hashing.

Q35. A list of persons or organisations to be notified in the event of a disaster and often included in a Business Continuity Plan is a called a:
a. Crisis Communication Directory
b. Crisis Communication Plan
c. Call Directory
d. Notification Directory.

Q36. The plan that addresses the restoration of business processes after an emergency, but which lacks procedures to ensure continuity of critical processes throughout an emergency or disruption is called a:
a. Business Continuity Plan
b. Crisis Communication Plan
c. Business Resumption Plan
d. Continuity of Operations Plan.

Q37. Procedures that are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data, are contained in a:
a. Continuity of Operations Plan
b. Cyber Incident Response Plan

c. Crisis Communication Plan
d. Business Resumption Plan.

Q38. An IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency is called a:
a. Disaster Recovery Plan
b. Business Resumption Plan
c. Continuity of Operations Plan
d. Cyber Incident Response Plan.

Q39. The response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property is contained in a/an:
a. Business Resumption Plan
b. Cyber Incident Response Plan
c. Business Resumption Plan
d. Occupant Emergency Plan.

Q40. With respect to the BCP testing, which of the following type of test will involve considerable expenditure of time, effort and resources?
a. Checklist
b. Structured walk-through
c. Full-interruption
d. Simulation

Q41. With respect to BCP testing, in which type of test is processing done at both the primary and alternate location?
a. Full-interruption
b. Parallel
c. Simulation
d. Structured walk-through.

Q42. With respect to the BCP testing which is the most rigorous way to test a business continuity plan?
a. Full-interruption
b. Parallel
c. Simulation
d. Structured walk-through.

Module – IV

Q43. Insurance cover that reimburses a company for the expenses incurred to avoid or minimize the suspension of business is called:
   a. Business Interruption Insurance
   b. Equipment and Facility Insurance
   c. Data Reconstruction
   d. Extra expense insurance.

Q44. Insurance that protects the company in the case of a claim against the company for negligence, errors, omissions, or wrongful acts in the performance of the company's duties is called:
   a. Business Interruption Insurance
   b. Equipment and Facility Insurance
   c. Professional Liability Insurance
   d. Extra Expense Insurance.

Answers:

1 C	2 B	3 C	4 C	5 A	6 B	7 C	8 D	9 A	10 B
11 C	12 D	13 A	14 B	15 D	16 C	17 B	18 A	19 D	20 C
21 B	22 D	23 D	24 C	25 D	26 C	27 B	28 A	29 D	30 C
31 B	32 A	33 D	34 C	35 D	36 C	37 B	38 A	39 A	40 C
41 B	42 A	43 D	44 C						

3 The Business Continuity Plan Audit

Learning Objectives

- To understand how the IS Auditor performs a BCP audit

Introduction

Business continuity refers to an organisation's ability to recover from a disaster and/or unexpected event and resume or continue operations. Organisations should have a plan in place ("Business Continuity Plan") that outlines how this will be accomplished. The key to a successful disaster recovery is to have a plan (emergency plan, disaster recovery plan, and continuity plan) well before disaster ever strikes. When conducting an audit of a disaster recovery plan, several factors should be considered. To be effective the plan must be written, must be understandable, and must be accessible to those who need it when they need it. Because of the constant changes that occur in the modern business environment, a plan should be updated frequently to deal with new and existing threats as they develop. The auditor needs to determine if procedures stated in the plan to achieve these ends are actually used in practice. This can be accomplished through:

- Direct observation of procedures
- Examination of the disaster recovery plan
- Inquiries of personnel.

An audit of a company Disaster Recovery Plan should primarily look into the probability that operations of the organisation can be sustained at the level that is assumed in the plan, as well as the ability of the entity to actually establish operations at the site. The auditor should examine and test the procedures involved in BCP, determine reasonable standards relating to implementation and conduct third part independent BCP audit at the facility.

Priorities

- Ensure that the plan's priorities support objectives of the organisation, meet regulatory requirements and conform to contractual requirements.

- Verify that the plan ensures the survival of the organisation by supporting the timely resumption of information processing capabilities after a disruption.
- Check for the evidence that the priorities have been reviewed and accepted by the appropriate levels of the management.
- Check to see that all applications have been evaluated as to their tolerance for a disruption. Ensure that all critical applications have been identified.

Strategies

- Verify that the strategies adopted by the company are in line with the priorities.
- Check for the implementation of the various components of the plan.
- Check whether the resources allocated for the plan are adequate and whether they will be available within the timeframes allowed by the plan.
- Evaluate the strategy to ensure its adequacy. This includes evaluating any offsite facility and reviewing its security and environmental controls.
- Determine if the hot-site or other equipment-ready facility has the correct versions of the system software or a compatible version.
- Review the list of suppliers to be contacted in the event of a disaster to ensure its completeness and appropriateness.
- Determine whether the plan clearly indicates how movement to the recovery site is to be effected.
- Examine the adequacy of telecommunications backup.
- Verify that written backup agreements and contracts exist for all facilities, hardware, software, vendors, suppliers, disaster recovery services, and reciprocal agreements. Verify that all agreements are in force and are adequate for the company's needs.
- Evaluate the methods and frequency of data backups and determine their appropriateness.
- Determine the adequacy of offsite data storage.
- Where the company has gone in for a commercial hot or cold site, the IS auditor should obtain a copy of the contract. References provided by the vendor should be verified.
- Evaluate the security of an offsite facility to ensure that it has logical, physical and environmental controls that are commensurate with the risk as assessed during the risk assessment phase. Ideally, these controls should be on par with that provided at the primary facility.
- Determine whether the offsite storage facility has the necessary data files, system software and associated documentation, application software and associated documentation, operations manuals, forms, stationeries, and suppliers and a copy of the current Business Continuity Plan. This may require the auditor to perform an inventory review at the offsite facility.

Responsibilities and Tasks

- Ensure that the responsibilities and tasks assigned to various personnel are in accordance with the priorities and strategies.
- Evaluate the ability of IS personnel and other staff to respond effectively to a disaster. This requires a review of emergency procedures, training and result of drills and exercises.
- Ensure that the staffs have participated in the development of emergency procedures and assignment of responsibilities and tasks.
- Ensure that the current copy of the plan has been distributed.
- Test check contact information (of vendors, employees) to ensure that they are current.
- All key individuals who are critical to the success of the plan should be interviewed. They should demonstrate an understanding of their assigned responsibilities and have an up-to-date documentation of the tasks that are assigned to them.
- Interview a cross section of the employees to ensure that they have understood the responsibilities and tasks assigned to them.
- Ensure there is no excessive dependence on any one person.

Plan Maintenance

- Ensure that a suitable mechanism exists to update the plan.
- The IS auditor should review the result of the Business Continuity Plan test. The IS auditor should check to see that the results of the test were along anticipated lines. If not, discrepancies between expected outcomes and actual outcomes should be analyzed to find shortcomings in the plan. The IS auditor should examine whether the weaknesses and shortcomings that have been identified during testing have been rectified at a later date.

Review of insurance coverage

- The IS Auditor should ensure that insurance coverage is adequate and reflects the actual cost of recovery. It is important that the organisation not only covers the loss of property but also covers the loss of revenue stream arising from that property.

An Auditor may be present during the testing phase as an independent party to identify the shortcomings in the plan, if any and suggest changes that would make the plan effective and efficient.

Summary

In conducting the audit the individual or team should make use of various other procedures and processes to achieve the objectives of audit. These objectives should be clearly stated in the audit plan. Certification of the British Standards Institutions or Business Continuity BS 25999 is available from the BSI.

Questions

Q1. The Auditor should ensure that the BCP's priorities:
   a. Support objectives of the organisation.
   b. Meet regulatory requirements.
   c. Conform to contractual requirements.
   d. All of the above.

Q2. The Auditor should verify that the recovery strategies adopted by the company are:
   a. In line with audit objectives
   b. In line with costs
   c. In line with the priorities
   d. In line with that of major competitors.

Q3. With respect to a BCP, the Auditor should test, check, contact information (of vendors, employees) to ensure:
   a. They will honour their contractual agreements.
   b. That they are current.
   c. They are physically close by.
   d. They are registered with tax authorities.

Q4. The auditor should evaluate the security of an offsite facility to ensure that it has logical, physical and environmental controls. Ideally, these controls should be:
   a. On par with that provided at the primary facility.
   b. Less than that provided at the primary facility.
   c. More than that provided at the primary facility.
   d. Different from that provided at the primary facility.

Answers:

1 D	2 C	3 B	4 A

References:

Ron Weber, Information Systems Control and Audit, Prentice Hall, 1999

James C Barnes, A guide to Business Continuity Planning, John Wiley & Sons, Ltd., 2001

Web Resources

http://www.the bci.org

http://www.drj.com

http://www.journalofaccountancy.com

Module – V

Information Systems Organisation & Management

1 Governance

Learning Goals / Objectives

The key objectives of these chapters are to ensure that the candidate comprehends the following concepts of Governance:

- Enterprise Governance
- Corporate Governance
- IT Governance
- e-Governance

At the end of this chapter, the candidate should be able to:

- Define what is meant by Enterprise Governance
- Comprehend the need for Enterprise Governance
- Distinguish between Corporate and Business Governance
- Identify best practices in Enterprise Governance
- Define Corporate Governance and the related processes
- Understand the changing role of the IT Department
- Define IT Governance and it's purpose
- Identify the benefits of IT Governance
- Identify those organisations which need IT Governance
- Identify the current best practices in IT governance
- Define e-Governance, its users, the models used and the benefits of e-governance
- Test their understanding of the above by attempting the questions at the end of the chapter

Introduction

This chapter introduces the concept of Enterprise governance and defines its components i.e. corporate governance and Business governance. It explains the differences between the two and why corporate governance alone may not guarantee success.It attempts to identify best practices in Enterprise governance namely, Strategic oversight, Enterprise risk management, the acquisition process and Board performance, and elaborates on each of the concepts.

It identifies key concepts and best practices in corporate governance and the need to modify it by identifying the main impediments to corporate governance. IT governance has also been explained along with how the role of the IT department has changed over time and some best practices have been identified and amplified upon.

It further explains what is information security governance and its components.

The concepts of risk management are summarised in order to refresh the reader's knowledge.

Finally e-governance has been explained in order to remove any confusion with the concepts discussed earlier.

Enterprise Governance

"The proper governance of companies will become as crucial to the world economy as the proper governance of countries".

The Board of the International Federation of Accountants (IFAC) explored the concept of Enterprise Governance in 2002 to focus on why corporate governance often fails in companies and what must be done to ensure that governance does not fail.

Enterprise governance is an emerging term which describes a framework which covers both:

- Corporate governance and
- Business governance in an organisation.

It takes a more holistic view to ensure that strategic goals are aligned and that good management is practiced in order to bridge the "oversight gap".

Definition

Enterprise governance is defined as:

"The set of responsibilities and practices exercised by the Board and executive management with the goal of:

- providing strategic direction
- ensuring that objectives are achieved
- ascertaining that risks are managed appropriately and
- verifying that the organisation's resources are used responsibly".

The enterprise governance framework

Fundamentally, enterprise governance is the entire accountability framework of the organisation, with the twin dimensions of **conformance and performance** of

processes, with more emphasis on the latter. It, therefore, encapsulates corporate governance, performance management, internal control and enterprise risk management.

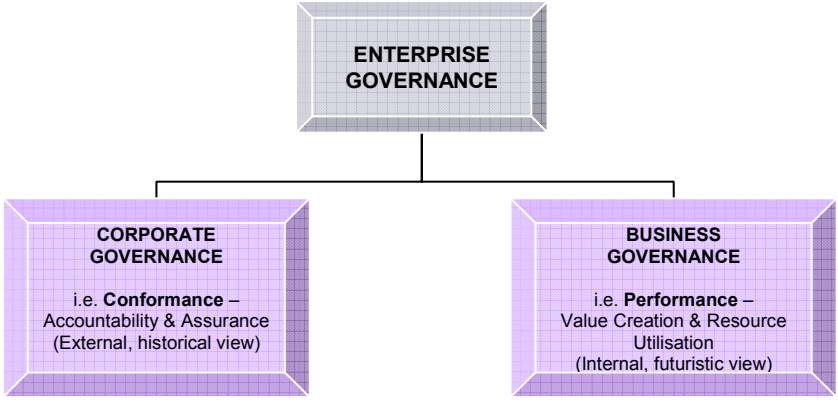


Fig. 1.1 The enterprise governance framework

Conformance deals with external processes like:

- Board committees - audits, remuneration and nominations
- Compliance with regulations
- Roles of the chairman and CEO
- Board of directors – composition, training, non-executive directors etc
- Internal Controls
- Risk Management
- Executive remuneration

Performance focuses on internal processes like strategy and value creation, in order to help the Board to:

- Make strategic decisions
- Understand its appetite for risk , the key drivers of its performance, and
- Identify its key points of decision making

At the heart of enterprise governance is the argument that good corporate governance on its own cannot make a company successful, examples of which are: Aventis, Marks & Spencer, and Nortel Networks. Another study showed that wherever a corporate disaster occurred, bad corporate governance was mainly the key factor. Companies must, therefore, balance conformance with performance.

Four key inter related **corporate governance** issues were identified that determined both success and failure, without any one being dominant. These were:

- Culture, ethics and tone at the top– e.g. Enron, U.S.A., had large scale and serious accounting irregularities.
- The role of the chief executive officer– e.g. WorldCom, U.S.A, had a major accounting fraud.
- The Board of directors– e.g. HIH, Australia, had a dominating CEO which led to an unquestioning culture that allowed poor management to continue unchecked.
- Internal controls, compliance and risk management – e.g. Ahold, Netherlands, had large scale accounting irregularities.

Some of the other corporate failures identified were:

- Vivendi
- Parmalat and
- Xerox
- Satyam

Successes identified were companies that wanted good corporate governance e.g.:

- Tesco
- Bangkok Mass Transit System and
- Southwest Airlines.

But it was also found that good corporate governance did not necessarily guarantee success.

In other words, bad governance can ruin a company, but cannot, on its own, ensure its success.

Enterprise governance, with its focus on both the conformance and performance aspects of business, ensures that companies do not lose sight of this "oversight gap".

Did you know?

After the widely reported collapse of Enron in 2000, and the alleged problems within Arthur Andersen and WorldCom, the duties and responsibilities of the Boards of directors for public and privately held corporations were questioned. As a response to this, and to attempt to prevent similar problems from happening again, the US Sarbanes-Oxley Act was written to stress the importance of business control and auditing. Sarbanes-Oxley and Basel-II in Europe have been catalysts for the development of the discipline of information technology governance since the early 2000s.

Similarly, there were **four key strategic issues** underlying success and failure:

- Choice and clarity of strategy – e.g. Tesco, U.K., used a focused strategy, well executed and supported by a strong management team and learnt from it's acquisition errors.
- Effective strategy execution – e.g. Southwest Airlines, U.S.A., used a strong corporate culture based on customer service and employee satisfaction.
- Ability to respond to abrupt changes and/or fast-moving market conditions – e.g. Li Fung , Hong Kong, transformed itself from a broker between the manufacturers and merchants to a coordinator of sophisticated supply chain networks.
- Ability to undertake successful mergers and acquisitions – e.g. Total, France, implemented a successful post-acquisition integration.

Some other success stories identified were:

- Bank of Nova Scotia
- Proton
- TransCanada Corporation and
- Unicredit Group.

Unsuccessful mergers and acquisitions was the most significant issue in strategy-related failure.

Best Practices in Enterprise Governance

Based on their findings, they identified and considered key best practices in the following areas, in order to make the business and performance aspect of enterprise governance more effective:

a. Strategic Oversight
b. Enterprise risk management
c. The acquisition process
d. Board performance.

Strategic Oversight

1. While a **Strategy Committee** was considered to be important, it was felt that it was a "preparatory committee" and the Board was still responsible for major strategic decisions.
2. The **Balanced Scorecard** conceived by Kaplan and Norton in the early 1990's, was considered and felt to be an invaluable management tool to translate strategy into action and to bring non-financial performance indicators into better focus. But it was considered to be a less successful tool where uncertain and

complex decisions which were required to formulate the strategy during times of transformational change.

3. They proposed a **CIMA Strategic Scorecard** whose objectives are to:

- Assist the Board in the oversight of a strategic process.
- Deal with the strategic choice and transformational change.
- Give a true and fair view of the company's strategic position and progress.
- Track the actions into and out from the strategic process.

The Strategic Scorecard has four basic elements aimed at helping the Board to ensure that all strategic aspects are covered by making the Board aware of what work is being done and when :

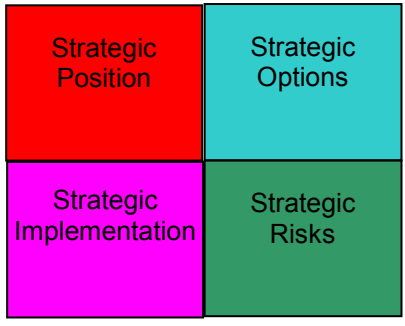


Fig. 1.2 The (Chartered Institute of Management Accountants) CIMA Strategic Scorecard

Strategic Position deals with information on:

- The micro environment e.g. market, competition and customers.
- The macro environment e.g. political, economic and regulatory factors.
- Threats from changes e.g. strategic inflexion points.
- Business position e.g. market share, pricing, quality, service.
- Capabilities e.g. core competencies and SWOT analysis which deals. with Strengths, Weaknesses, Opportunities and Threats.
- Stakeholders e.g. vendors, employees, shareholders.

Strategic Options deals with what options are available with respect to:

- Scope Change e.g. area, product, market sector.
- Direction change e.g. high or low growth, price and quality offers.

Strategic Implementation deals with:

- Project milestones and timelines.

- Pursue or abandon the plan etc.

Strategic Risks deals with what can go wrong and what must go right with respect to:

- Informing the Board on risks and how they are being managed.
- Measurement of risks.
- Internal controls.

Enterprise Risk Management

This reconciles both the:

- Assurance that the business understands its risks and is managing them actively i.e. conformance, and
- Need to better integrate risk management in decision making activities at all levels i.e. performance.

This will give the Board:

- More confidence in the organisation's risk management capability.
- Better empowerment of the Board to question management.
- Improved stakeholders' assurance that the organisation is taking risk management seriously.

The Acquisition Process

In view of the increasing number of mergers and acquisitions, a detailed eight stage process map was created to guide the Board through each stage.

The identified critical success factors are:

- Effective and experienced full time project management.
- Thorough evaluation of synergies and ruthless implementation.
- Effective due diligence.
- Use of experienced specialists in mergers and acquisitions.
- Early identification of risks with appropriate risk reduction actions.

Board Performance

Apart from adhering to the known corporate governance codes, Boards need to give more attention to Board:

- **Performance evaluation and measurement systems** e.g. training, widening the pool of probable candidates, board design, performance metrics.
- **Dynamics** e.g. dominating personalities, quick decision making, restructuring and resignations of key executives, favouring particular interests, interfering with information flows.

- **Design** e.g. the balance between executive and non-executive directors, director independence, the process for appointing directors, and aligning directors' interests with shareholders' interests.

From the above, it can be seen that enterprise governance is the framework that bridges the gulf between corporate governance and business success.

Corporate Governance

Definitions

There are two definitions of corporate governance:

- **Information Systems Audit and Control Association, ISACA** Ethical corporate behaviour by directors or others charged with governance in the creation and presentation of wealth for all stakeholders.
- **Organisation for Economic Cooperation and Development, OECD** The distribution of rights and responsibilities among different participants in the corporation, such as Board, managers, shareholders and other stakeholders, and (it) spells out the rules and procedures for making decisions on corporate affairs. By doing this, it also provides the structure through which the company objectives are set and the means of attaining those objectives and monitoring performance.

From the above and the previous section on Enterprise Governance, it becomes clear that corporate governance also includes a system for:

- Managing and monitoring risks and
- It requires companies to have an internal control system, in order to (a) manage systems and (b) culture.

This is because the interests of the stakeholders of the organisation need to be protected, which cannot be achieved without appropriate risk management and internal controls. These issues are ultimately, the responsibility of the Board of Directors.

Corporate Governance, therefore, means, providing continued value addition to the shareholders and stakeholders, while maintaining ethical corporate behaviour which includes the following:

- Integrity
- Openness

- Transparency and
- Accountability in its corporate conduct (including statutory financial practices, reporting and audit) and business activities.

Its effective implementation is dependent on:

- The right people
- Making the right decisions
- At the right time.

while upholding the objectives of the organisation.

Quality decision making, as stated above, will steer the organisation towards its objectives. These decisions cannot be made without good processes.

The processes which deal with corporate governance have been listed in the previous section on Enterprise Governance and are being repeated here for the sake of clarity:

- Board committees - audits, remuneration and nominations
- Compliance with regulations
- Roles of the chairman and CEO
- Board of directors – composition, training, non-executive directors etc
- Internal Controls
- Risk Management
- Executive remuneration.

The main impediments to good corporate governance have been found to be:

- Corporate governance is not embedded in company law. However, in the U.K. , the Department of Trade & Industry and Deloitte & Touche have suggested in their Company Law Review that corporate governance should be made a part of Company Law.
- Cultural differences which vary from country to country also affect its effective implementation. These differences can influence current strategies and future changes and may need a change in culture.

The importance of culture can be seen from the diagram below.

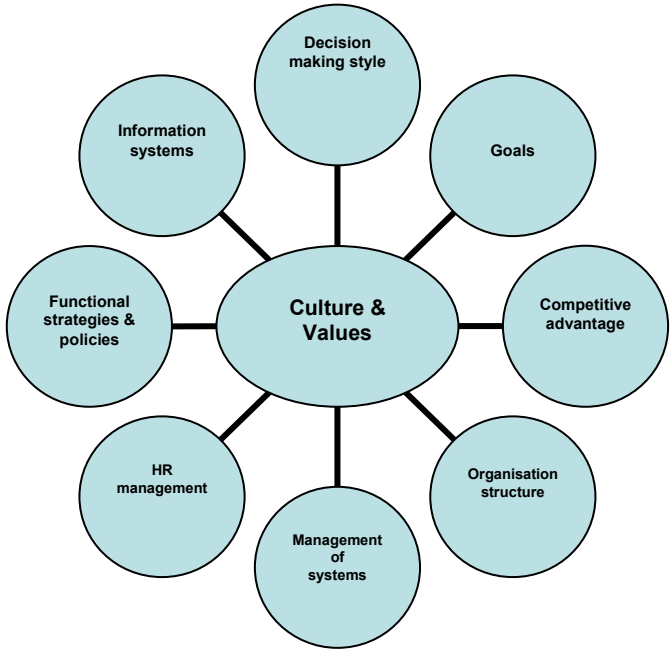


Fig 1.3 The influence of culture and values on an organisation.

Did you know?

The difficulties in achieving a balance between financial transparency and cost-effective data capture in IT financial management is a continual topic of discussion in the professional literature and can be seen as a practical limitation to IT governance

Information Technology Governance

The Changing Role of the IT Department

The ultimate objective of governance is to ensure that IT objectives are aligned with enterprise objectives.

Enterprises have now realised that IT which was once considered as only an enabler of its business strategy / goals is really an integral part of that strategy.

In this context, the role of the Information Technology Department has been changing from a purely technical role to a more managerial and strategic role.

Fig.1.4 The Changing Role of the IT Department

Traditional Role

- Managing systems and project development.
- Managing computer operations and the data centre.
- Training, staffing and developing IS skills.
- Providing technical services.

New Role (incorporating the traditional role)

- Initiation and design of strategic information systems.
- Infrastructure planning, acquisition, control and implementing improvements.
- Linking the business with the Internet and e-commerce processes.
- Systems Integration.
- Educating non technical staff about IT and technical staff about the business.
- Support for end user computing through help desks etc.
- Constant liaison with top management.
- Business process reengineering.
- Managing related outsourced function.

Definition of IT Governance

IT governance is the responsibility of executives and the Board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.

IT Governance is a sub set of corporate governance which describes how the Board of directors will consider IT in their supervision, control, monitoring and direction of the organisation. It encompasses the following:

- Information systems
- Technology
- Communications
- Business legal and other issues
- All stakeholders – directors, senior management, process owners, vendors, users and auditors.

Purpose of IT Governance

The twin purposes of IT governance are to ensure that:

- IT delivers value to the business, by aligning IT with the objectives of the organisation, and

- IT risks are reduced by embedding accountability into the processes of the enterprise.

With a good IT environment and infrastructure, good IT governance will be able to support good corporate governance. This again is dependant on the:

- availability of the right information to the
- right persons
- at the right time
- at the right place most effectively and efficiently.

Some benefits of good IT governance

- By ensuring that IT resources are used optimally and responsibly, it can help to decrease costs and, therefore, promote efficiency
- By optimising resources for automation it ensures effective use of resources.
- Helps the business to avail better opportunities and maximise benefits by aligning IT and business objectives.
- Promotes the management of risks by providing for adequate security, compliance and reliability of information.

Who needs IT governance?

Those enterprises where:

- Good corporate governance is lacking.
- There is insufficient liaison between the Board and the IT department.
- IT is not a regular item on the Board meetings agenda.
- There are no well defined rules and procedures.
- People are not clear about what IT is doing.
- There are many IT mishaps.
- There are many IT issues pending resolution for a long time.
- The IT skills are decreasing.
- There are frequent network problems.
- There is no planning for contingencies , etc.

Best Practices in IT Governance

IT / IS Assurance Systems

These auditors are in the best position to:

a. Recommend best practices to the Board in order to improve the effectiveness and quality of the governance processes.
b. Provide assurance on compliance with the governance processes.

IT Strategy Committee

- This is, as mentioned in the section on Enterprise Governance, merely an advisory committee to the Board for bringing in IT governance into the enterprise governance processes.
- It ensures that the board is provided with the right information in order to make effective decisions.

It should be noted that this committee works at the Board level and differs from the Steering Committee which works at the executive level. They both differ in their Composition, Authority and Responsibility.

Fig.1.5 IT Strategy Committee vs. IT Steering Committee

Scope ↓	IT Strategy Committee (Board Level)	IT Steering Committee (Executive Level)
Composition	Board and expert non-board members.	CIO, IS Audit, Key End Users, Legal, Finance etc.
Authority	Given by the Board to advise on IT strategy.	Help the executive in the delivery of IT strategy.
Responsibility	Advise the Board on issues like alignment of IT and business direction.	Decide on issues like approval of the IT architecture.

The Balanced Score Card

This topic was introduced in the section on Enterprise Governance and is being elaborated here.

It was developed by Dr. Robert Kaplan and Dr. David Norton in the early 1990's in order to solve a "measurement problem" but it is also a management system. They felt that traditional financial measurements could not capture the value creating activities in an organisation like skills, competencies, IT etc. It provides a prescription as to what enterprises should measure in order to 'balance' the financial perspective. If something cannot be measured, it cannot be improved on. Metrics allow managers to see their enterprise from many perspectives and, therefore, make better decisions. The scorecard suggests a view of the organisation from four perspectives, and to develop metrics, collect data and analyse it in relation to these perspectives:

- **The Financial Perspective**

The strategy for profitability, growth and risk as viewed from the shareholder's

perspective. Apart from the regular financial data on corporate performance, they suggest additional financial data on risk assessment and costs versus benefits.

- **The Customer Perspective**

This is the strategy for creating value from the customers' perspective. The metrics generated here will indicate the extent of customer satisfaction with the products or services supplied.

- **The Internal Business Process Perspective**

These are the strategic priorities for various business processes, which create customer and shareholder satisfaction. The metrics for this perspective will allow the managers to determine how well the business is performing and whether their products meet customer requirements, which is the mission.

- **The Learning & Growth Perspective**

The priorities to create a culture that support organisational change, employee training, corporate cultural attitudes, growth and innovation.

The balanced scorecard has been used in some enterprises to translate strategy into action while others have used it to measure non-financial performance indicators.

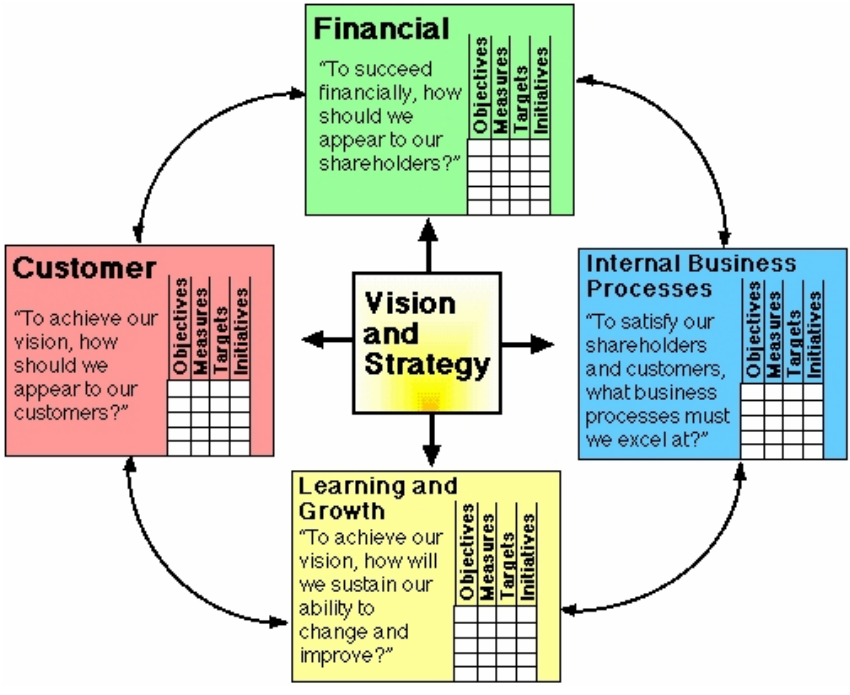


Fig.1.6 The Balanced Scorecard

How does it work?

The balanced scorecard uses a three-layered structure for IT in order to determine its performance from the four perspectives:

1. **Mission**
   Examples: a. o be the preferred supplier of an IS process.
   b. Develop technology to address future needs.
2. **Strategies**
   Examples: a. To develop superior applications and processes.
   b. Provide better service levels.
3. **Measures**
   Example: a. To provide a set of balanced metrics like Key Performance Indicators in order to guide business focussed IT decisions.

Information Security Governance

IT Governance is a subset of Information Security Governance and it should be given a very high priority by top management.

Good security governance will ensure that:

- Information security risks are properly managed.
- Resources are used responsibly and effectively e.g. return on IT investments is optimised.
- Information security is aligned with business strategy.
- Information security processes are measured, monitored, reported and improved on through appropriate metrics like Key Performance Indicators and Key Goal Indicators.

It should encompass all information assets with respect to:

- Integrity
- Availability
- Confidentiality.

In addition, the following can also be involved in Information security:

- Authenticity
- Accountability
- Non-repudiation and
- Reliability.

Module - V

Enterprise Architecture

Enterprise Architecture is a key component of the information technology governance process for any organization of significant size. Enterprise Architecture involves applying a comprehensive method for describing the current and/or future structure and behaviour of an organization's processes, information systems, personnel and the organization's sub-units, with the objective of aligning them with the organization's goals and strategic direction.

The pioneer of Enterprise Architecture (EA) was John Zachmann, who first published his work in 'Zachmann Framework for Enterprise Architecture' in 1987. Since then several other models have been published including ISO 15704. In the U.S.A, by law a Federal organisation is required to develop an EA model and governance structure, through their Federal Enterprise Architecture (FEA). More and more companies are implementing a formal enterprise architecture process to support the governance and management of IT.

EA involves documenting the organisation's IT assets in a systematic and structured method in order to promote the:

a. Management
b. Planning and
c. Understanding for IT investments from a technology and business perspective.

The Zachmann model uses diagrams, flowcharts, code and data class models in order to convey different aspects of an organisation's systems at greater levels of detail.

	What	**How**	**Where**	**Who**	**When**	**Why**
	Data	Function	Network	People	Time	Motivation
Scope (contextual) Planner						
Business Model (conceptual) Owner						
System Model (logical) Designer						

Technology Model (physical) Builder						
Detailed Representations (out of context) Subcontractor						
Functioning Enterprise	e.g. Data	e.g. Function	e.g. Network	e.g. Organisation	e.g. Schedule	e.g. Strategy

Fig.1.7 The Zachmann Framework for Enterprise Architecture

By filling in details in the cells, the enterprise can develop an architecture framework in order to describe a series of "current", "intermediate" and "target" reference architectures and applying them to align change within the enterprise. Another way of describing these terms are "as-is", "to-be" and the "migration plan".

Risk Management

This subject has been discussed in detail in Module VI, The IS Audit Process, but briefly it encompasses the following:

a. **Risk Assessment**

- Define the risk assessment approach of the organization by :
  1. Identifying an appropriate risk assessment methodology.
  2. Develop and identify criteria for acceptable risk levels.
- Identify the risks by identifying:
  1. the assets in the IS and their owners.
  2. the threats to those assets.
  3. the vulnerabilities that might be exploited by the threats.
  4. the impact of loss of Confidentiality, Integrity and Availability on the assets.
- Analyse and evaluate the risks by :
  1. Assessing the business impacts on the organization due to loss of CIA.

2. Assessing the realistic likelihood of security failures with respect to the risk assessment and the controls implemented.
3. Estimate the levels of risks.
4. Determine whether the risks are acceptable or require treatment.

b. **Risk Treatment**

- Identify and evaluate the options for risk treatment possibly by :
  1. Applying appropriate controls.
  2. Knowingly and objectively accepting the risks.
  3. Avoiding the risks and.
  4. Transferring the risks to say insurers or suppliers.
- Selecting suitable control objectives and controls for the treatment of those risks.
- Obtain management approval for the proposed residual risks.
- Constantly, improve the risk management process.

e-Governance

This section is being included here in order to remove any confusion between IT governance and e-governance.

Definition

e-governance refers to the use of information technology in order to exchange information and services with citizens, businesses, and other arms of the government.

Users

It may be used by the legislature, judiciary or the administration in order to improve internal efficiency, delivery of public services, or processes of governance.

Models

The main models are:

- Government-to-Citizen or
- Government-to-Customer (G2C),
- Government-to-Business (G2B) and
- Government-to-Government (G2G).

Benefits

The benefits of e-Government include:

- Better efficiency

- Transparency
- Convenience and
- Better access to public services.

Summary

The need of Governence has gained prominence after companies started using IT in business operations. This need gained even more importance after a series of accounting scams took place and resulted in the passing of legislations like SOX. IS auditor should understand the risk in a computerized environment while applying a comprehensive method for describing the overall structure and behaviour of an organization through which objectives can be achieved. The balanced scorecard method has been used translate strategy into action in enterprise Governance. Various roles have been defied in IT governance as to differentiate the responsibility of the Board of Directors at the level of Top management. At a broader level, an IT Governance is essential for the organization to ensure that IT delivers value to the business and IT risks are reduced by embedding accountability into the processes of the enterprise.

Questions:

1. Which of the following is NOT an element of information security governance :
   a. Confidentiality
   b. Repudiation
   c. Integrity
   d. Availability
2. Which of the following options is a part of information security governance :
   a. Authenticity, Reliability, Accountability
   b. Accountability, Reliability, Non-repudiation
   c. None of the above
   d. All of the above
3. The benefits of a good security governance are:
   a. Information security risks are properly managed.
   b. Information security is aligned with business strategy.
   c. Information security processes are measured, monitored, reported and improved on through appropriate metrics like Key Performance Indicators and Key Goal Indicators.
   d. All of the above.
4. Which of the following is the LEAST appropriate goal of enterprise governance :
   a. Providing tactical direction.

b. Ensuring that objectives are achieved.
c. Ascertaining that risks are managed appropriately.
d. Verifying that the organisation's resources are used responsibly.

5. Which of the following would NOT be a part of the conformance aspect of enterprise governance :
   a. Internal Controls
   b. Compliance with regulations
   c. Executive remuneration
   d. Making strategic decisions.

6. While auditing the corporate governance aspects of an enterprise an IS auditor would exclude which of the following :
   a. Audit committee
   b. Role of the Chairman and CEO
   c. Training given to the board members
   d. None of the above.

7. While auditing the business governance aspects of an enterprise an IS auditor is LEAST likely to examine the evidence relating to which of the following :
   a. Resource utilisation
   b. Performance measurement
   c. Risk appetite
   d. Executive remuneration.

8. Which of the following would an IS auditor consider to be an inappropriate indicator of good governance :
   a. The enterprise has a strong and dominating CEO.
   b. The enterprise uses a strong management team to implement its strategy.
   c. The enterprise has a strong corporate culture based on customer service and employee satisfaction.
   d. The enterprise has a strong ability to adapt to changing market situations.

9. Which of the following are considered to be the best practices in enterprise governance:
   a. Strategic Oversight and enterprise risk management
   b. Enterprise risk management and the acquisition process
   c. The acquisition process and board performance
   d. All the above.

10. Corporate governance excludes which of the following elements:
    a. Continued value addition
    b. Transparency in conduct

c. Accountability in conduct
d. Better access to public services.

11. The traditional Balanced Scorecard suggests a view of the organisation from certain perspectives, and to develop metrics, collect data and analyse it in relation to these perspectives. The complete list of perspectives is:
    a. Financial and Customer
    b. Financial, Customer and Learning
    c. Financial, Customer, Learning and Growth and Internal Business Processes
    d. Financial, Customer, Learning and Growth.

12. The IS auditor is collecting the evidence on the role of an IS department. Which of the following options includes an emerging role of the department?
    a. Management of systems, project development, operations and data centre.
    b. Management of systems, project development, data centre and IT staff training.
    c. Management of systems, project development, data centre and technical services.
    d. Management of project development, data centre, technical services and non-It staff training.

13. The IT strategy committee works at:
    a. Board level only
    b. Executive level only
    c. Board and Executive levels
    d. None of the above.

14. Which of the following is NOT an element of risk assessment?
    a. Identification of assets
    b. Identification of controls
    c. Identification of threats
    d. Identification of vulnerabilities.

15. Risk treatment includes which of the following options:
    a. Transferring the risk to a third party.
    b. Assessing the realistic likelihood of security failures with respect to the risk assessment and the controls implemented.
    c. Estimation of the levels of risks.
    d. Assessing the business impacts on the organization due to the loss of Confidentiality, Integrity and Availability.

16. Which of the following standards relates to enterprise architecture?
    a. ISO 27001

b. ISO 15704
c. ISO 19011
d. ISO 22000

17. An IS Auditor would EXCLUDE which of the following while gathering the evidence on indicators of poor corporate governance :
    a. There is inadequate liaison between the Board and the IT department.
    b. Board meetings include IT as a regular item on the agenda.
    c. There is no evidence of well defined rules and procedures.
    d. There are frequent IT mishaps.

18. The Board has asked the IS Auditor to advise them on identifying the critical success factors before the acquisition of a company which has an IS department of strategic importance. The IS Auditor would recommend all the following except:
    a. Use of effective and experienced full time project managers together with experienced specialists in mergers and acquisitions.
    b. Thorough evaluation of corporate synergies and ruthless implementation.
    c. Effective due diligence.
    d. Identification of risks and risk reduction actions after the acquisition process is complete.

19. Which of the following statements is true?
    a. The ultimate objective of governance is to achieve desired goals.
    b. The traditional balanced scorecard is more effective than the CIMA scorecard.
    c. Data processing is the only activity that requires thorough IS auditing.
    d. Business to Business (B2B) is an e-Governance model.

20. Which of the following statements is false?
    a. Information Security Governance is a subset of IT Governance.
    b. Enterprise governance excludes risk management.
    c. The traditional balanced scorecard also deals with internal business processes.
    d. A benefit of e-governance is better access to citizen centric services.

Answers:

1. B	2. D	3. D	4. A	5. D	6. D	7. D	8. A	9. D
10. D	11. C	12. D	13. A	14. B	15. A	16.B	17.B	18.D
19.A	20. B							

1. The correct answer is **b)** Repudiation.

   All the other options are an integral part of information security governance.

2. The correct answer is **d)** All of the above. Information security governance encompasses options a) and b) as well as Confidentiality, Integrity and Availability.

3. The correct answer is **d)** All of the above. The benefits of information security governance encompass all the options as well as alignment of information security processes with business goals.

4. The correct answer is **a)** providing tactical direction. While all the other options are goals of enterprise governance, providing strategic direction would have been more appropriate than providing tactical direction.

5. The correct answer is **d).** Making strategic decisions is a part of the performance aspect of enterprise governance which really deals with making business decisions.

6. The correct answer is **d).** None of the other options listed should be excluded by the IS auditor because they are considered to be good corporate governance processes.

7. The correct answer is **d)** Executive remuneration. This is because while all the other options relate to business governance i.e. performance, executive remuneration falls in the domain of corporate governance which deals with compliance aspects of governance.

8. The correct answer is **a).** A strong and dominating CEO is considered to be inappropriate to good governance as evidenced by the cases of Enron and HIH.

9. The correct answer is **d)** All of the above. All the practices listed are considered to be the best practices for enterprise governance.

10. The correct answer is **d**)Better access to public services is the exclusive domain of the government sector which falls under e- Governance. All the other options relate to the corporate and the government sector.

11. The correct answer is **c)** This includes all the four perspectives required by the traditional Balanced Scorecard.

12. The correct answer is **d).** The emerging role of the IS Department includes training imparted to non-IT staff as well. All the other options describe the traditional role of the IS Department.

13. The correct answer is **a)**. The IT Strategy Committee works at the Board level while the IT Steering Committee works at the executive level.

14. The correct answer is **b).** The identification of controls is a part of risk treatment, while all the other options are a part of risk assessment.

15. The correct answer is **a).** All the other options are a part of the risk assessment process.

16. The correct answer is **b).** ISO 15704 deals with the Requirements for Enterprise Reference Architecture and Methodologies. ISO 27001 deals with Information Security Management Systems.

    ISO 19011 deals with the guidelines for Quality Management Systems Auditing.

    ISO 22000 deals with Requirements for Food Safety Management Systems.

17. The correct answer is **b)**. The inclusion of IT as an agenda item in the Board meetings is a sign of good corporate governance. All the other options are indicators of poor corporate governance.

18. The correct answer is **d)**. While risk management is desirable, it would be more appropriate before the acquisition rather than after the acquisition. All the other options are crucial to the acquisition process.

19. The correct answer is **a)**. Governance processes are required to achieve the stated goals of the organisation. The CIMA scorecard is considered to be a more effective tool than the balanced scorecard. IS encompasses many other activities including data processing. B2B is actually an e-Commerce model.

20. The correct answer is **b)**. Risk management is an integral part of enterprise governance. All other options are true.

Glossary of Terms

Business to Business (B2B)

A model used in electronic commerce for conducting transactions between businesses.

Balanced Scorecard

A system developed by Drs. Robert Kaplan and David Norton in the early 1990's to translate strategy into action and to bring non-financial performance indicators into better focus in order to give a more balanced picture of the enterprise than those given by financial performance indicators.

Business Process Re-engineering (BPR)

The process of IS / IT innovations or re-designing an organisation's business processes and / or organisation structure. The ultimate objectives of BPR are a) a more effective organisation structure b) cost savings and c) better response to customer needs and market conditions

Business Governance

An element of enterprise governance that deals with the performance of internal processes.

CIMA Scorecard

A system developed by the Chartered Institute of Management Accountants, which has four basic elements strategic position, options, implementation and risks. It is aimed at helping the Board to ensure that all strategic aspects are covered by making the Board aware of what work is being done and when.

Contingencies

Unforeseen events typically controlled by IS processes like business continuity management.

Corporate Governance

A system, which consists of, leadership, process and organisational structures which enables organisations to be directed and controlled.

Communications

The process which uses a path or medium that enables the data to be transferred between two locations.

E-Governance

The employment of Internet technologies and electronic commerce, in order to provide information and services to the public, business partners, vendors and those in the public sector.

Government-to-Citizen or

A model used to provide e-Governance services to the citizens.

Government-to-Customer (G2C)

A model used to provide e-Governance services to customers.

Government-to-Business (G2B) and

A model used to provide e-Governance services to the business sector.

Government-to-Government (G2G).

A model used to provide e-Governance services to the govenrment sector.

Enterprise Governance

The processes used by an enterprise in order to achieve organisational goals, provide strategic direction, manage risks and use resources effectively.

Enterprise Architecture

The process of documenting the organisation's IT assets in a systematic and structured method in order to promote the management, planning and understanding for IT investments from a technology and business perspective.

Governance

The processes of achieving the desired goals of the organisation.

Impact

The loss or adverse consequences resulting from an undesirable event.

Internal Controls

The methods employed to address risk, which includes policies, guidelines, procedures, practices, and organisational structures, which provide a degree of assurance that the organisation's goals will be met and that threats will be prevented, detected or corrected.

Information systems

The overall system, which consists of formal rules and procedures for providing information to the management, in order to enable then to make effective decisions.

Information Security Governance

A superset of IT governance which involves using a business risk approach, in order to plan, implement, monitor and improve information security.

ISO

International Organisation for Standardisation, an organisation based in Geneva.

ISO 27001

The ISO standard for Information Security Management Systems.

ISO 15704

The standard for Enterprise Reference Architecture and Methodologies.

ISO 19011

The guidelines for Quality Management Systems Auditing.

ISO 22000

The standard for Food Safety Management Systems.

IT Governance

A subset of corporate governance, entrusted to executives and the Board of directors, comprising of the leadership, organisational structures and processes which ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.

IT Strategy Committee

An advisory committee to the Board for bringing in IT governance into the enterprise governance processes**.** It ensures that the Board is provided with the right information in order to make effective decisions.

IT Steering Committee

A committee appointed by the Board to oversee IS department activities and ensure that they are in harmony with the corporate objectives.

Key Performance Indicators

Metrics used to determine how well an IT process is performing.

Key Goal Indicators

Metrics that determine the achievement of IT process goals.

Mission

A mission statement defines the organisation's business, objectives and how it will reach those objectives.

Outsourced Functions

The processes employed to acquire any product or service from another organisation.

Oversight Gap

The gap between the conformance and performance aspects of an enterprise.

Risk Appetite

The extent to which management is willing to take risks.

Risk Management

Coordinated activities in order to direct and control an organisation with respect to risk comprising, risk assessment and risk treatment.

Risk Assessment

The process of risk analysis and evaluation.

Risk Treatment

The process of selecting and implementing measures to reduce risk.

Stakeholders

The persons or entities who affect or may be affected by the organisation's decisions, e.g. vendors, employees, shareholders, investors, government, labour unions, industry associations etc.

Threats

Undesirable events which may adversely affect a system or a process.

Technology

The use of skills, know how, systems, organisational methods and automation in order to perform a function.

Value Addition

Refers to the additional value created at a particular stage of production or process.

Vision

A statement, which describes the desired future position of the organisation.

Vulnerabilities

Internal system weaknesses which may allow undesirable acts, i.e. threats, to damage a system.

Zachmann Framework

See Enterprise Architecture above.

Reference Sources:

1. PD 6668, Managing Risk for Corporate Governance, Mike Robbins & David Smith.
2. Information Systems Audit and Control Foundation, 2001.
3. Enterprise Governance, Getting the balance right, CIMA & IFAC.
4. Introduction to IT, Turban, Rainer & Potter.
5. ISACA.
6. CoBIT.
7. www.balancedscorecard.org
8. ISO 27001:2005.
9. www.zifa.com
10. http://en.wikipedia.org/
11. CISA Review Manual.

2 The Information System Management Process

Learning Goals / Objectives

The key objectives of this chapter are to ensure that the DISA candidate can comprehend and can apply a systematic approach to auditing the IS Management Process by applying the Deming Cycle. The latter is more popularly known as the Plan-Do-Check-Act (PDCA) cycle.

At the end of this chapter, the DISA candidate should be able to:

- Comprehend the importance of managing information systems
- Understand the concepts of the PDCA cycle and its application to management processes
- Comprehend the types of plans, steering committees and distinguish policies, standards, guidelines and procedures and the importance of leadership
- Understand the processes for acquisition of and the types of the IS resources
- Comprehend control methods like :
    - Benchmarking
    - IS Budgets and Variances
    - Transfer Prices
    - User Satisfaction
    - Capacity Management & Growth Planning
    - Financial Management
    - Quality Management
    - Goal Accomplishment
    - HR Controls
    - Outsourcing
    - Performance Measurement
    - Change Management
    - Documentation Standards
    - Project & Line Management Structures

- The risks and controls of the various roles performed by personnel in the IS Department
- Separation of Duties

- Appreciate the importance of effecting improvements in the IS department processes.

Introduction

This chapter explains what are the objectives of an organization, the importance of management and the importance of managing the IS department. It explains how the Plan-Do-Check-Act cycle can be used for any management process.

Planning involves making long and short range plans by the IS Steering Committee for all the business units as well as the IS department. These plans should be in line with the business goals of the organization. The steering committee will also make policies, standards, guidelines and procedures for the IS processes. This function requires that the organization has appropriate leaders in order to guide the organization towards its objectives.

Management has to acquire resources and implement systems and processes in order to ensure that the plans are executed. The processes include benchmarking, financial management, user satisfaction surveys, capacity management and growth planning, goal accomplishment and performance measurement indicators, quality management, sourcing, HR, documentation, setting up organization structures along with roles and responsibilities while ensuring separation of duties.

Management should also ensure that they monitor, evaluate and report on the actual results of the processes against the established goals.

Lastly management should make necessary improvements on a continual basis by taking appropriate corrective action.

The objectives of an organization

The main objective of an organization is to survive. It does this by:

a. Identifying and meeting the needs of customers and other stakeholders, in order to achieve competitive advantage, in an effective and efficient manner, and
b. To achieve, maintain and improve its performance and capabilities.

In order to achieve these objectives, the management of the organization's systems and processes, functions in a way that is systematic and visible.

The importance of management

"Management is the organ whose performance determines the performance and even the survival of the institution". It is the art of getting things done in order to meet the objectives of an organization.

In order to do this, management must first determine the goals of the organization based on customer needs. Then, it should implement and operate the required resources and processes. Next, it should monitor and review the processes and resources, and finally maintain and improve the system.

Management studies over the last few decades show that "structure follows strategy". Without understanding the mission, strategies and objectives of the organization, managers cannot be managed, organizations cannot be designed, and functions cannot be made effective and efficient.

Management success rests on appropriate empowerment of people with responsibility, authority and accountability.

The importance of managing the information systems department (ISD)

Many organizations have now realised that the ISD has an operational as well as a strategic role to play in the success of the organization. Many organizations are now bent on transforming themselves into global businesses using major investments in e-Business, e-Commerce, and other IT initiatives. These organizations are also realising that if good management controls, on the roles performed by personnel in the ISD, are not in place and working effectively and efficiently, then the application controls are not likely to be effective. Thus, a thorough evaluation of management controls is important to the IS auditor before deciding on the extent of his reliance on application controls. It is clear that, we cannot evaluate the IS management unless we understand what the IS management should be doing.

The process of The Deming Cycle

The Deming Cycle, PDCA, is a simple yet powerful concept conceived by Walter Shewhart in the 1930's, and later popularised by Dr. W. Edwards Deming, who is considered as the leader in Modern Quality Control. PDCA is an iterative four-step problem solving process typically used in business process improvement. In Six Sigma, which is a quality control system, this cycle is known as DMAIC, i.e. Define, Measure, Analyse, Improve and Control. The abbreviation PDCA means:

Plan

The organization should establish the goals and required processes in order to deliver results in conformance with requirements. In other words, the organization should define the problem or opportunity, analyse the situation, determine the best course of action and develop an implementation plan.

Do

Implement the processes, taking small steps in controlled circumstances, in order to reach the organization's goals. This involves, implementing the decided course of action, documentation of procedures and collection of the data.

Check

Monitor, evaluate and report the processes and results against the established goals to ascertain any differences. This stage involves analysing the data, monitoring trends and comparison of actual against planned results.

Act

Analyse the differences to determine their cause. Apply necessary actions in order to bring about necessary improvements. This may involve repeating the PDCA cycle with changes, adopting the change or abandoning it and restart the planning process.

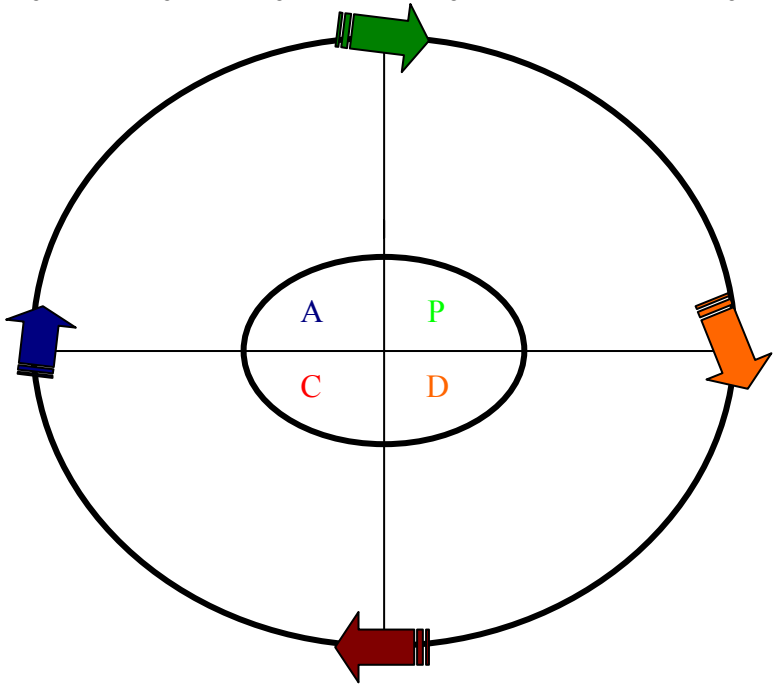


Fig. 1.The PDCA Cycle

PDCA is not a one time exercise; rather it is an ongoing exercise to be adapted and repeated regularly for any process, with each cycle producing more improvements in the organization's march towards its desired goals.

Some real world examples:

The PDCA cycle has been used in many ISO standards and organizations like:

- ISO 9001 – Requirements for Quality Management Systems
- ISO 27001 – Requirements for Information Security Management Systems
- The Pearl River, New York, a 2001 recipient of the Malcolm Baldrige National Quality Award, used the PDCA cycle as a model for defining most of their work processes, from the boardroom to the classroom.

The impediments to the success of the PDCA cycle are:

- Complacency
- Loss of focus
- Inability to communicate and train employees
- Emergence of new priorities
- Lack of resources
- Lack of management commitment etc.

The Planning Function

The word planning can mean several things like development, preparation, setting up, arrangement, scheduling, forecasting etc. It is a management process required to decide in advance:

a. What should be done?
b. How should it be done?
c. When should it be done? and
d. Who should do it?

In short, a plan is an action statement. Plans are the means to achieve the objectives, without which the organization would become rudderless. The planning and related processes are some of the many Critical Success Factors (CSFs) in organizational success.

The planning aspect of managing an information system, basically involves formulating a Master Plan which contains two types of plans:

a. Long Range Plans, and
b. Short Range Plans

The development of these plans are the responsibility of the IS Steering Committee. It is considered to be one of the best practices to be employed in any organization, whether in the public or private sector.

The IS Steering Committee

Appointment

The IS Steering Committee is appointed by the Board in order to oversee the IS Department's processes, and it operates at the executive level.

Responsibilities

The duties, responsibilities, authority and accountability of the Steering Committee should be defined in a formal charter, which should be approved by the Board. Members should know the IS department policies, practices and procedures. Each member should have the authority to make decisions within the group for his or her respective areas.

Objective

The primary objective of the Steering Committee is to ensure that the IS department is aligned with the organization's mission and objectives. It provides planning and control for the organization's IS function.

Chairman

It should preferably be chaired by a member of the Board of Directors who understands information technology risks and issues.

Representation

The membership of the committee should be broad-based and should include a cross-section of senior business managers including legal and finance, senior management, user management and the IS department.

Functions

The steering committee should:

- Act as an overall review board for large IS projects only. It should not be involved in minor and routine operations, which are best left to lower level management.
- Review and approve long and short range plans in order to ensure that they are in accordance with the organization's mission and objectives.
- Establish size and scope of the IS function and sets priorities within the scope.
- Review and approve major acquisitions of the IS resources within the limits approved by the Board of Directors.
- Approve and monitor the progress of major projects, lay down priorities, and develop policies, standards, guidelines and procedures.

- Liaise between the IS and user departments.
- Approve major projects, budgets and the status of the IS plans.
- Review the adequacy and allocation of the IS resources with respect to time, personnel, equipment, software, services and technology.
- Make decisions on centralisation versus decentralisation of the IS function and allocation of duties and responsibilities of the IS department.
- Review and approve sourcing plans for some or all of the IS activities.
- Receive regular and appropriate feedback reports from various departments including, IS, audit and users, in order to ensure the effective and efficient utilisation of the IS resources.
- Initiate corrective action in order to achieve the desired results by monitoring the IS performance.
- Ensure the planning, implementation, monitoring and improvement of information security.
- Facilitate and resolve conflicts and ensure availability of a viable communication system between the IS department and its users.
- Support development and implementation of an enterprise-wide information security management program.
- Provide appropriate feedback to the Board of Directors on the IS activities on a regular basis.
- Minute the proceedings of their meetings.

Advantages

- Top management involvement
- User representation
- Centralization of authority
- Promotes user ownership of systems
- Promotes planning and control
- Establishes user focus in IS

The Master Plan of the Organization

This is the main plan prepared by the Board of Directors to guide the organization towards its objectives. It includes the following elements for the organization:

- A statement of its Mission, Vision and Values
- A statement describing its strategic objectives
- The strategies for achieving those objectives
- The factors that may, favourably or adversely, affect the achievement of those objectives.

The creation of the master plan will aid in the development of the long and short range plans of the organization.

Long Range Plans

Dimensions of Long Range Plans

The long range plans are sometimes called strategic plans. The word "strategy" is derived from the Greek word "strategia" i.e. the art or science of being an army general, which requires them to lead an army, win or hold territory, protect them from invaders, defeat the enemy etc. Over time it was proposed to be redefined in 1962, by the business historian, Alfred D. Chandler as:

"The determination of basic long term goals of an enterprise, and the adoption of courses of action and the allocation of resources necessary for carrying out these goals".

Strategic planning is the process by which top management determines the overall organizational purposes and objectives and how they are to be achieved. In the context of IS, it refers to planning undertaken by top management towards meeting long-term IT objectives of the enterprise.

Strategic plans are oriented towards the following three dimensions:

- **Time**
  These plans typically span a period of two to five years.
- **Project**
  The projects to be completed are clearly defined.
- **Goals**
  The link between the goals of the organization and the projects are clearly identified.

The inputs for effective and efficient planning include e.g.

- Strategies and defined organizational goals.
- Defining and meeting the needs of customers and stakeholders.
- Evaluating compliance with statutory, regulatory and contractual needs.
- Evaluating performance data on products and processes.
- Lessons learned from previous experiences.
- Any related risk assessment and treatment information.

The outputs of good planning include e.g.:

- Defined product outcomes and support processes.

- Skills and knowledge required by the people.
- Responsibility, authority and accountability of processes and improvement plans.
- Resource needs.
- Metrics for evaluating performance.
- Need for improvement methods and tools.
- Need for documentation and records.

Contents of Long Range Plans

These plans typically deal with the following macro issues:

1. Current IS Assessment

A thorough assessment of the present IS resources is made which include applications, information, infrastructure and people. Simply put, it answers the question: what do we have or where are we?

2. Future IS Assessment

Similarly, a thorough assessment of the future IS resources is made which include applications, information, infrastructure and people. Simply put, it answers the question: where do we want to be in the next five years in order to meet our strategic objectives?

3. Development Strategy

This details the methodologies and vision used to reach the stated strategic objectives. It basically answers the question: how should we bridge the gap between our present and our future situations?

Methods of creating long range plans

These can range from formal to less formal methods and may start by using techniques which include:

- **SWOT analysis**

This is an evaluation of the strengths, weaknesses, opportunities and threats which can affect the identified strategic opportunities of the organization. E.g. Dell used SWOT analysis to make a strong business strategy which included mass **customisation**; just-in-time manufacturing, letting customers design their own machines through the e-Commerce website etc.

Strengths	**Weaknesses**
1.	1.
2.	2.
3.	3.

4. 5.	4. 5.
Opportunities 1. 2. 3. 4. 5.	**Threats** 1. 2. 3. 4. 5.

Fig.2 SWOT Analysis

- **Team building**

These look at strategic visioning questions like: who are our customers, how can we add value by using an e-Business model, how can we make a value chain if we start an e-Business enterprise?

- **Scenario models**

Where teams of the IS and business managers evaluate various scenarios, in order to determine the role that the ISD can play in reaching the business objectives. This technique has been successfully used by Royal Dutch Shell for more than 20 years which has helped them to overcome the oil market crisis of the 1970s and 1980s.

- **Consensus creating exercises**

Alternative scenarios may be considered before arriving at a consensus, based on various other factors which may include stakeholder's expectations, political, business, social, and technological changes that may occur.

Short Range Plans

These plans are sometimes known as operational or tactical plans. They are derived at regular intervals from long-range plans. They typically deal with the following micro issues to be addressed within the next one year.

1. **Progress reports**
   These reports help the management to assess what has or has not been achieved.
2. **Resource allocation**
   This determines the IS resource needs during the remaining period.
3. **Implementation schedule**
   This outlines the timelines proposed for the projects along with their start and end dates.

4. **Initiatives to be undertaken**
   This details the actions to be taken for the IS department in order to achieve the laid down targets.

Operational planning is defined as the process of assuring that specific tasks are carried out effectively and efficiently.

It is important to note that each of the long and short range business plans of

the organization, will also have plans for the ISD.

Why does the planning process often fail?

1. It is time consuming and there are other immediate tasks to be completed.
2. Planning requires intensive mental effort which managers often like to neglect.
3. It makes the future look more uncertain after strategic planning than before.
4. If no plans are made, managers feel freer to look at other options, while planning forces managers to look at a smaller range of options.
5. If the plans are imposed, the opposite reaction may occur, i.e. managers may oppose or ignore the plans.
6. Good planning requires inter-departmental co-ordination, knowledge and team building which may be difficult to achieve.
7. Managers may lack internal confidence in their ability to meet the corporate targets.
8. Managers may not have enough or appropriate information in order to make proper decisions.

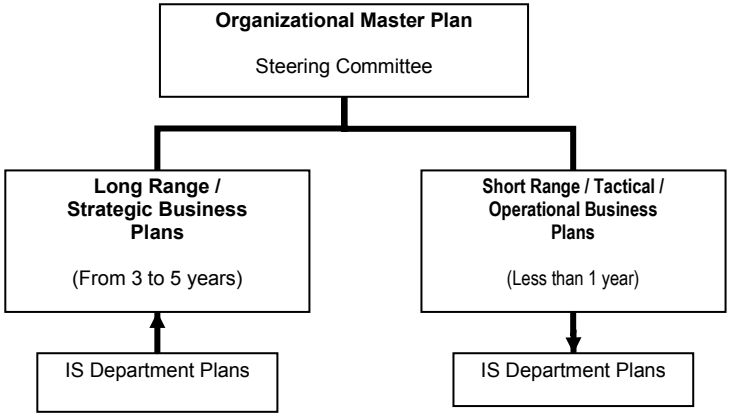


Fig.3 Summary of the Planning Process

Policies

As stated in section 2.3.1 above, one of the functions of the IS Steering Committee is to develop policies, which are implemented through standards, guidelines and procedures for the ISD. Internal controls will flow from the creation of policies, which are required to ensure that the stated objectives are met. The development of policies takes place after the organizational strategic goals have been determined.

Definition

Policies may be defined as:

1. Formal statements made by the management of their overall intention and direction, or
2. A stated course of action, with a defined purpose and scope, in order to guide decision-making, under a given set of circumstances, within the framework of the organization's objectives, goals and management philosophies.

They represent formal expressions of the philosophy, culture and belief systems of the organization. They can apply equally to the government and the private sector. They can be political, technical, financial or administrative by nature with the ultimate objective of reaching desired goals.

A typical policy for an organization might read as follows:

It is the company's policy to protect its information assets from all threats, by ensuring the protection of information and facilities against unauthorised access, assure confidentiality and integrity of information, comply with legal, regulatory and contractual requirements, develop, implement, test and improve business continuity management, provide information security training and detect all breaches of information security and take necessary action thereon.

- Policies are usually high-level and static documents and define what is or is not allowed in the organization
- They are the starting point for creating the standards, guidelines and procedures that are needed in the organization
- Because they are developed by the top management, they let lower-level management know that there is consensus at the top
- In some organizations, individual departments are permitted to define lower-level, i.e. operational policies only
- Their development is the responsibility of the top management
- In order to be effective they should:
    - Ideally be in writing.
    - Be clear, concise, communicated in writing or orally.

- Understood by all employees.
- Regularly reviewed and updated to reflect new technology and significant changes within the organization or department.
- Be made by the top management in order to ensure consistency. A bottom-up approach, where corporate policies are made from lower-level policies (made by lower levels of management), may be practical but it may lead to conflicts and inconsistencies.
- Clearly state their purpose, scope, applicability, effective date and the persons responsible for their implementation.

- Examples of policies made by some organizations include :
  - Marks and Spencer, who have policies for selling goods of only their brand name and concentrating their buying in the U.K.
  - The Body Shop, uses strong environment policies which include avoiding animal testing, using only recyclable containers and natural raw materials.
- Policies accompanied by standards, guidelines and procedures should be made for all IS related processes, including for example:
  - Use of Internet and e-mail
  - Data security
  - Change management
  - Outsourcing
  - Data retention
  - Human resources
  - Project management, etc.

An important by-product of policy making is the determination of required processes or practices, procedures and work instructions that are required to implement the policy.

Standards

After the creation of policies, standards conforming to the best practices can be designed for the organization. They are documents which state management rules, legal and regulatory issues that are mandatory.

They ensure uniformity in their use throughout the organization. E.g. A standard could be the mandatory use of virus controls, passwords and encryption of all data categorised as critical in order to provide for information security.

Guidelines

The creation of standards will in turn lead to the creation of guidelines or codes of practice which are also a collection of best practices from which the organization can

choose the most appropriate practice for them. They clarify what and how things should be done, in order to achieve the objectives of the policy. In other words they provide a framework for understanding the standards and list the tools which can achieve the objectives. Continuing from the example above, the company management requires the use of RSA 128-bit encryption technology, for encrypting the critical data.

Procedures

Procedures are detailed documents that define, in writing, how to enforce or apply the policy. They are derived from the parent policy and define the steps to be taken for specific events. In other words, they are "How to do it" statements. It may be noted that these procedures are to be made for the business processes in place which in turn are based on business goals.

Procedures must be written in a clear and concise manner so that they may be easily and properly understood by those governed by them. They document business processes and the controls embedded therein. They are more dynamic than the parent policy since they must reflect the regular changes in business focus and environment. Hence, they must be frequently reviewed and updated.

Continuing from the example above, the document will describe the steps detailing how a user can encrypt the critical data using RSA 128-bit encryption.

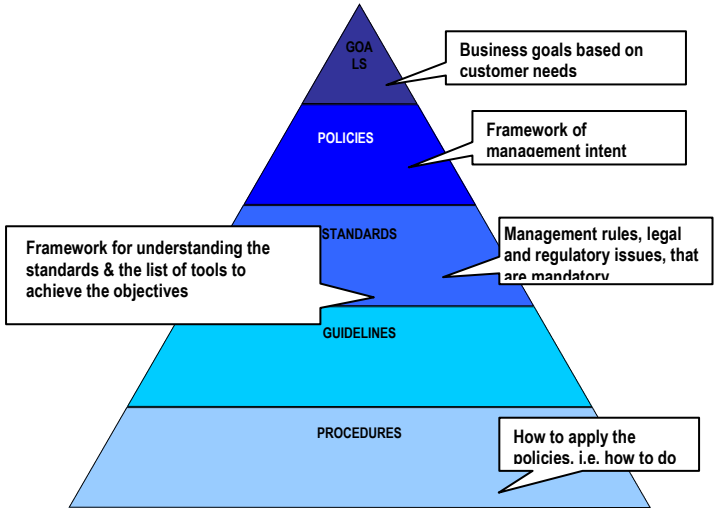


Fig.4 Hierarchy of planning goals, policies, standards, guidelines and procedures

The policies, standards, guidelines and procedures have to be specific to the requirements of the organization. In other words, the uniform has to be tailor-made to fit the soldier, which is the organization.

The importance of leadership

Leadership is the ability of a person to influence the behaviour of a working group in order to achieve the desired objectives. While there are many theories on the subject, some of the qualities found in many good leaders are that they:

- Establish a clear vision of the future, policies and objectives that guide their actions in an ethical manner.
- Understand customer needs.
- Create an organization that fosters the development and involvement of people.
- Provide the structure and resources to support the plans.
- Think only in positive terms like success, not worrying, focusing on the present etc.
- Lead by example in order to develop trust with their people and take calculated risks based on that trust.
- Always look for new opportunities, improvement projects and breakthrough changes.
- Do the right things and in the right way.
- Can motivate, empower and inspire people.
- Can effectively direct, supervise and delegate authority to people.
- Have good communication and organizational skills.
- Have the ability to act as mediators in resolving disputes.
- Have the ability to build and foster team management.
- Recognise and reward individual or group contribution.
- Obtain feedback on the effectiveness and efficiency of their processes.
- Identify the support processes that result in adding value to the organization, like information management, training, finance, facility and service maintenance, office safety and marketing.
- Can measure organizational performance in order to determine whether the planned objectives are being met.

Example: General Electric

Jack Welch was appointed as the Chairman of General Electric (GE) in 1981.His immediate aim was to make GE the leader in every business in which it was competing. He went about the pursuit of his goals with a single-minded determination and made sweeping changes in the company's business mix and corporate culture.

He discovered that the key ingredients to getting things done were initiative, managerial freedom and a dislike for non-performing managers. Within ten years he reduced the management layers by half, delegated more authority to managers, reduced employee strength and sold USD 12 billion of business. He transformed GE by bringing about a passion for change and a vision of how to compete in a demanding global market.

In 1981 GE's profits were USD 1.65 billion, which rose to USD 7.28 billion by 1996!

"My job is to find great ideas, exaggerate them and spread them like hell around the business with the speed of light and to put resources in to support them. Keep finding ideas. That's the job of just about all our CEOs".

He further adds that in his opinion, leaders should have four main qualities:

1. Energy – They should love to be on the go, love action and relish change.
2. Energise – They should have the ability to energise others by inspiring them to move mountains when they have to.
3. Edge – They should have the edge or courage to take tough decisions.
4. Execute – They should have the ability to execute plans coupled with emotional intelligence.

The Acquisition of resources and Implementation of processes

Having completed the planning process and determined the best course of action i.e. the business goals, specific policies need to be made relating to those goals. The policies will determine the resources to be acquired and processes to be put into place. It is the responsibility of the top management to ensure that the required resources are made available, in order to meet the goals. Sometimes, the word practice is used, instead of process, both of which determine what is to be done. They are inter-related activities which transform inputs into outputs.

The creation of processes will lead to the determination of procedures.

Procedures provide detailed steps of action that should be followed in order to perform a specific task.

A procedure is a documented practice which is capable of:

a. Verification,
b. Validation, and
c. Approval.

Verification means determining whether the procedure is accurate or complete. Validation means determining whether the procedure is right or wrong in the given context.

The procedures specify detailed work instructions. These instructions detail how the required steps are to be performed.

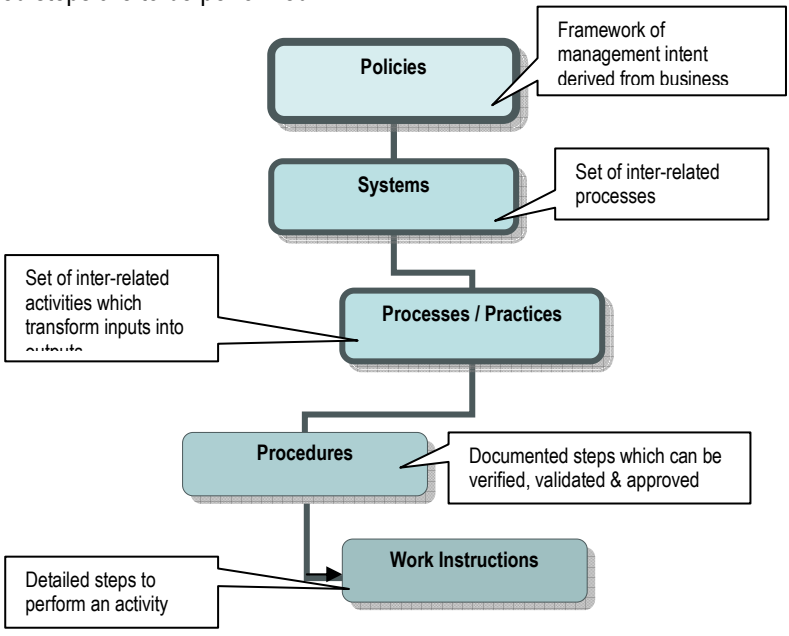


Fig.5 Sequencing of policies, systems, processes, procedures and work instructions

The acquisition of the IS resources

The following IS resources need to be identified and acquired, in order to assist in the creation of systems and processes which are documented, monitored, measured, analysed and continually improved on:

Applications

These are the computerised or manual user systems and procedures that process the data and information for a specific user task.

Information

This is the data that is input, processed and output by the organization's information systems for decision making, based on facts. The organization should be able to

identify its needs for information and the sources of information, convert the data into information and knowledge that can be used in reaching organizational goals, provide appropriate security for it, and evaluate the benefits of using information in order to improve the management of knowledge and information.

IT Infrastructure

It comprises of the following technologies and facilities:

- Operating systems
- Database management systems
- Networking
- Multimedia
- Computer hardware and
- Facilities that house and support the processing of the applications and the work environment.

People

They consist of the personnel required to plan, organize, acquire, deliver, implement, monitor, support, evaluate and improve the information systems and allied services. These persons may be internal, outsourced or contractual persons as required.

The processes for the acquisition and or development of the IT hardware will cover processes like:

- Make or buy decisions
- In-house or out-sourced acquisition or development
- Development of contract requirements
- Tendering
- Selection criteria for vendors
- Empanelment of vendors
- Controls over vendors like contract acceptance and maintenance
- Legal clearance for vendor agreements
- Compliance with contract terms etc.

The Implementation of processes

Some of the important processes that need to be implemented are:

Benchmarking processes

What are benchmarks?

Industry standards or benchmarks provide the means to compare the

performance of the organization with those organizations having comparable

IS environments. Some of the key questions it asks are:

a. How much should we spend on the IS Department?
b. Are we getting value from the IS Department?

What are the goals of benchmarking?

The ultimate objective of benchmarking is to implement the best practices

prevailing in the industry, in order to improve IS the process performance.

Where can benchmarking statistics are obtained from?

Benchmarking statistics and the best practices can be obtained from various sources like industry publications and professional associations. Some examples are:

- Information Technology Infrastructure Library (ITIL)
- India Benchmarking Centre
- http://www.qaiindia.com
- http://www.stqc.nic.in

Some uses of benchmarking

Benchmarking can be used for various activities like:

- System workloads
- CPU performance
- Software development

For further details please see the section dealing with the Capability Maturity Model, and

- Quality processes

For further details please see the section dealing with ISO 9001.

Some problems with benchmarking

- It may force organizations to spend more than it should on the IS department.
- Higher spending on the IS department may have no correlation with better organizational performance.
- The determination of value may be very subjective.
- Spending on innovations in the IS department often leads to their quick copying by competitors.

Module - V

Financial Management processes

a) IS Budgets and Variances

It is considered a good practice to have a budgeting process for the IS department because budgets are a control instrument for:

- Detecting variances and determining their correction.
- Forecasting, monitoring and analyzing financial information.
- Allocation of appropriate funds in order to enable the IS department to achieve the organization's objectives.
- Eliminating or reducing process and product failures.

The IS budget should be linked to short and long-range IT plans.

b) User Pays Scheme and Transfer Prices

IS departments have traditionally been viewed as cost centres while The other departments are credited with the revenues and benefits realised from the investments made in IT. The User Pays Scheme allows the chargeback of the IS expenses to the end-users (other departments) who are the ultimate beneficiaries of the services. It provides the IS personnel and users with a tool to measure the effectiveness and efficiency of the IS service. It can improve the application and monitoring of IS expenses and available resources. The chargeback may be based on the actual, standard or market prices or any other agreed method. The chargeback of expenses forces users to ask for more effective and efficient IS services which may be formalised in an Operating Level Agreement (OLA). OLA is an internal agreement for the provision of the IS services between the end users and the IS department.

User satisfaction survey processes

The objective of user satisfaction surveys is to determine the effectiveness of the IS department after the users and the IS department have agreed on a level of service through service level and or operating level agreements. The basic belief that underlies is that the user satisfaction is highly correlated with system success and at regular intervals the management should measure customer satisfaction to identify shortfalls in service levels and establish improvement objectives. This can be done through appropriately designed questionnaires in order to collect factual evidence on various issues like:

- Any adverse effects of the system on the quality of the users working lives
- System availability
- Report distribution timeliness

- System downtime
- The existence of unknown risks, and poor controls, etc.

The above issues may be considered for a periodic auditing.

Capacity Management & Growth Planning processes

Capacity management is the process of planning, sizing and continuously Optimising the IS capacity in order to meet long and short term business goals in a cost effective and timely manner. Its primary goal is to ensure that IT capacity meets current and future business requirements in a cost-effective manner. It is used in order to assess the effectiveness and efficiency of the IS operations. Capacity includes the following:

- Storage space
- Network throughput
- Human resources
- Electronic messaging
- Customer Relationship Management
- Quantum of data processed, etc.

The ITIL version on this subject provides a set of the best practices in service delivery and views capacity management from three dimensions:

- Business Capacity Management
- Service Capacity Management and
- Component or resource Capacity Management.

The success of capacity management depends on factors like:

- The availability of precise and timely business forecasts
- Having a thorough understanding of present and future technologies
- Proper communication with service management processes
- Planning and acquiring appropriate levels of resources in order to meet business needs.

The benefits of good capacity management are:

- Enhanced customer satisfaction
- Better justification of spending on the IS resources
- Avoiding incorrect capacity sizing which may lead to inappropriate utilisation of the IS resources and insufficient capacity to process the production workloads
- A reduction in capacity failures
- Better alignment of business needs and the IS resources
- Better service level management.

Goal Accomplishment processes / indicators

These are used in order to determine the effectiveness of a system by comparing actual performance with predefined business and IT goals. This can be done by using manual or automated logs in order to issue early warnings, for various processes like:

- Productivity improvements like lower data entry time taken and errors
- Meeting customer requirements for quality
- Lower hardware or software errors
- Lower the IS risks
- Standardised processes
- Lower security violations etc.

These goal indicators will determine whether the targets are being met for the processes.

Performance Measurement processes / indicators

This is considered to be an important part of the IT governance processes. They say that what cannot be measured cannot be improved on. Therefore, metrics should be generated for e.g. all products and processes, financial measurement, benchmarking and external party evaluation, satisfaction of customers, internal staff and stakeholders, in order to ensure that they are achieving the desired results.

Uses of performance measurement

Performance measurement is used to:

- Measure and manage products and services
- Assure accountability
- Make budgeting decisions and
- Optimise performance i.e. improve the productivity of the IS to its highest possible level without making unnecessary added investments in the IS infrastructure.

Phases of performance measurement

Performance measurement typically has the following phases:

- Plan, establish and update performance measures.
- Plan and establish the accountability of persons for the performance measures.
- Collect and analyse the data on performance.
- Report on performance information and
- Take corrective action.

Performance indicators or metrics will determine how well the process is performing in enabling the goals to be achieved. They are also the indicators of capabilities and skills of the IS personnel.

Examples

- Better use of communications bandwidth and computing power.
- Lower number of non-compliance with prescribed processes reported.
- Better cost and efficiency of the process.
- Lower numbers of complaints made by stakeholders.
- Better quality and increased innovation etc.
- Lower number of errors and rework.
- Improved staff productivity.

The Link between Critical Success Factors, Goal Indicators and Performance Indicators

The Critical Success Factors are the most important things that the management must do, based on the choices made in the planning and related processes, while monitoring by using performance indicators in order to determine whether the organization will reach its goals set out in the goal indicators.

Quality Management processes

Definition

Quality management is a system of processes and activities considered necessary in order to plan, develop, monitor and improve a product or service, in an effective and efficient manner in order to meet stated requirements.

ISO 9000:2000 Series

Application

The most well known quality standards are the ISO 9000 series, which are process certification standards, and they apply to all organizations including those offering IT products and services.

Name

The name ISO was derived from the words “isos” and “iso”, which in Greek and French both mean equal. For anything to be equal, it must contain uniform or standard characteristics.

Location

ISO actually stands for The International Organization for Standardization, which was

founded in 1946 and is based in Geneva, Switzerland along with the International Electro technical Commission (IEC) and the International Telecommunication Union (ITU).

Certification

ISO is not responsible for certification, which is actually done by over 750 accredited certifying organizations in the world.

While the certification is not mandatory, it can be chosen by the organization or enforced on a vendor by a client, who may insist on dealing only with organizations which have ISO certified processes.

Evolution

In their early years, ISO developed mainly technical standards for various organizations like:

- Paper sizes- ISO 216
- Punching filing holes into paper- ISO 838
- International standard book numbering(ISBN) - ISO 2108
- Identification cards - Physical characteristics - ISO 7810
- Identification cards - Integrated circuit cards - ISO 7816
- C programming language - ISO 9899
- Open Systems Interconnection (OSI) - ISO/IEC 10026
- Information Technology - Metadata Registries (MDR) - ISO/IEC 11179
- Portable Document Format (PDF) - ISO 15930

In the last two decades, ISO have made two generic standards which apply to all organizations where there is a process.

a. ISO 14000 series

This series deals with Environmental Management Systems.

b. ISO 9000 series

This series deals with Quality Management Systems, i.e. what the organization does to enhance customer satisfaction, continual process improvement and compliance with regulations. It is based on the P-D-C-A model.

Objective

The main objective of the ISO 9000 series is to give the management of an organization and its customers, the confidence that it is in control of the way it conducts its business. They prescribe what standards the organization should meet,

but they do not prescribe how they should be met, leaving organizations free to conduct and organize their business processes as they wish.

Certification

The certification is valid for three years subject to periodic assessments by certifying bodies, like British Standards Institute, Det Norske Veritas, Bureau Veritas (BVQI), etc.

ISO 9000:2000

Provides the starting point for understanding the standard and it defines the fundamental terms and definitions used.

ISO 9001:2000

This deals with the requirements, i.e. the standards, for quality management systems. It stresses on:

a. managing and measuring performance in all spheres in the organization, and
b. the need for a documented quality management system in all areas like quality manuals, human resources, purchasing etc. It does not deal with a system of documents. It enables each individual organization to decide on the minimum amount of documentation required to demonstrate the effective planning, operation and control of its processes.

It is based on eight management principles:

a) Customer focus
Organizations must not only meet but strive to exceed current and future customer expectations.

b) Leadership
Leaders should be clear about the mission and values of the organization.

c) Involvement of people
People at all levels should be involved in collective decision making in order to reach the organizational goals.

d) Process approach
Related activities and resources should be managed as a process in order to achieve the corporate objectives more efficiently.

e) System approach to management
Interrelated processes should be identified, understood and managed as a system in order to improve the organization's effectiveness and efficiency in achieving its objectives.

f) Continual improvement
Continual improvement of the organization's overall performance should be a permanent objective.

g) Factual approach to decision making
Data and information should be analysed based on which effective decisions can be made.

h) Mutually beneficial supplier relationships
The organization and its suppliers are interdependent and a mutually beneficial relationship will enhance the ability of both to create value.

An organization wanting to develop a quality management system complying with ISO 9001:2000 requirements needs to perform a gap analysis against the requirements in the standard. This allows for improvements in the company's processes to fill the gaps and comply with the standard. After successfully meeting requirements of an internal process audit of the quality management system, an ISO certificate is issued.

ISO 9004:2000

This provides guidance on quality management systems and concepts for continual process improvement.

ISO 9126 Software Quality Model

This is the international standard for the evaluation of quality of software products which includes source code, executables, architecture descriptions etc. It provides a framework for organizations to define a quality model for a software product. It thus leaves organizations free to specify the exact model which may apply to them. The standard is divided into four parts: ISO 9126-1, ISO 9126-2, ISO 9126-3 and ISO 9126-4.

ISO 9126-1 Quality Model

This part classifies software quality in a structured set of six attributes and several related sub-attributes as follows:

1. Functionality	**Are the required functions available in the software?**
Sub-attributes	*Suitability, Accuracy, Interoperability, Compliance, Security*
2. Reliability	**Is the software capable enough to maintain its level of performance?**
Sub-attributes	*Maturity, Recoverability, Fault Tolerance*

3. Usability	**Is the software easy to use?**
Sub-attributes	*Learnability, Understandability, Operability*
4. Efficiency	**Does the software use the least amount of resources?**
Sub-attributes	*Time behaviour and resource behaviour*
5. Maintainability	**Can the software be modified easily?**
Sub-attributes	*Stability, Analysability, Changeability, Testability*
6. Portability	**Can the software be easily transferred from one environment to another?**
Sub-attributes	*Installability, Replaceability, Adaptability, Conformance*

ISO 9126-2 External Metrics

These metrics apply to running software.

ISO 9126-3 Internal Metrics

These are statistics which do not rely on software execution.

ISO 9126-4 Quality in use metrics

These are available only when the final product is used in real life conditions.

Ideally, the internal quality determines the external quality and external quality determines quality in use.

The Software Capability Maturity Model (CMM)

Development

This model was initially developed by The Software Engineering Institute of Carnegie Mellon University in 1986. The project was funded by the US Department of Defense, in order to establish standards for excellence in software engineering and to enable the use of advanced technologies into practice. The basic reason for it was to develop a model based on which software vendors could be evaluated. The ISO is soon going to release some standards and guidelines on this subject e.g.:

ISO/IEC 25001:2007- Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Planning and management

ISO/IEC 25030:2007- Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) – Quality requirements.

Assumption

The basic assumption of the CMM is that the quality of a software product is a direct function of the associated development and maintenance processes.

Application

It is used by software development organizations to:

a. Identify best practices required to assist them in increasing the maturity of their processes, and
b. Develop the means to graduate towards a culture of excellence in software engineering and management, in order to achieve their goals.

As with ISO 9001 and ISO 9126, it focuses on what organizations must do, leaving them free to choose the best methods in order to achieve their goals. The model can be used to benchmark or compare different software development organizations.

Basic Concepts

A software process is defined as a set of activities, methods, practices and transformations that people use to develop software and associated products, i.e. project plans, design documents, code, test cases, and user manuals. Software Process capability describes the range of expected results that can be achieved by following a software process. It provides the means to predict the expected outcomes from the next software project undertaken by the organization. Software process maturity is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective.

The model defines five levels of organizational maturity which serve as the foundation for continual process improvement and the quality processes which are associated with each level. As the organization makes and improves its software processes, it progresses through the levels of maturity. It cautions organizations to try to avoid jumping through the levels and urges them to progress through the levels using small evolutionary steps instead of employing revolutionary methods. It prescribes key practices that describe what should be done, but not how to achieve them.

The Five Maturity Levels

The five maturity levels and their key characteristics, starting from the lowest (level 1) to the highest (level 5) are:

1. Initial

In such organizations:

- Reliance is placed on the competence of key personnel rather than proven processes.
- Software development and maintenance environment is unstable.
- Processes are informal and ad hoc or chaotic.
- Sound management practices like planning are not there.
- Success depends on individual performance, hence success cannot be repeated for next project unless the same individual is assigned to that project.
- Personnel tend to over-commit, abandon processes in times of crisis and the projects frequently exceed budget and time targets.
- The software process capability of Level 1 organizations is a characteristic of the individuals, not of the organization.

2. Repeatable

In these organizations:

- Policies and procedures for project management are there.
- Basic project management principles are used to track costs, timelines and check functionality. Hence, problems in meeting commitments are identified when they arise.
- Disciplined processes are there in order to repeat earlier successes on projects with similar applications.
- New projects are planned and managed based on the experience with similar projects.
- Software requirements and the work products developed to satisfy them are base-lined, and their integrity is controlled.
- Software project standards are defined.
- The software process capability of Level 2 organizations can be summarized as disciplined.

3. Defined

In such organizations:

- The software process for both management and engineering activities is documented, standardized and integrated into a standard software process.
- There are standardised processes which are tailored to specific projects.
- Data and information from projects is regularly and systematically collected and organized so that the same can be reused by other projects.
- Training programs are implemented.

- The software process capability of Level 3 organizations can be summarized as standard and consistent.

4. Managed

In such organizations:

- Detailed measures of software process and product quality are established and performed. Both the process and products are quantitatively understood and controlled.
- Projects achieve control over their products and processes by narrowing the variation in their process performance to fall within acceptable quantitative boundaries. The risks are known and carefully managed.
- High quality software products are produced.
- The software process capability of Level 4 organizations can be summarized as being quantifiable and predictable.

5. Optimised

In these organizations:

- Best practices are used.
- Continual process improvement is achieved after a detailed cost-benefit analysis.
- Appropriate methods are used to prevent software defects.
- Improvements are achieved by making incremental advances in the present processes (using quantitative feedback from the processes) and by using innovative technologies and methods.
- The software process capability of Level 5 organizations can be characterized as continuously improving.

Some of the leading companies in level 5 are:

- 3i Infotech Ltd.
- Birlasoft Ltd.
- Caretor India(P) Ltd.
- IBM
- Infosys Technologies Ltd.
- Mindtree Consulting Pvt. Ltd.
- Motorola
- Northrop Grumman
- Oracle
- Patni Computer Systems Ltd.

- Satyam Computer Services Ltd.
- Siemens Information Systems Ltd.
- TCS
- Wipro Technologies Ltd.

Variants

a. SW-CMMI

In 2002, the model was upgraded and renamed SW-CMM Integration, which has been generalised over the years to include other organizations dealing with:

- Product and service development (CMMI-DEV)
- Service establishment, management, and delivery (CMMI-SVC)
- Product and service acquisition (CMMI-ACQ)

The latest release is version 1.2, which was released in 2006.

The generic model components under CMMI are:

0 – Incomplete
1 – Performed
2 – Managed
3 – Defined
4 – Quantitatively Managed
5 – Optimising.

The model also provides for two architectural structures: Staged and Continuous. The staged model provides a proven sequence of improvements starting with the basic management practices to successive levels. The continuous model allows the organization to select the order of improvement process areas that best meets the organization's business objectives and mitigates the organization's areas of risk.

b. SSE-CMM

Systems Security Engineering CMM focuses on security engineering process areas. It applies to developers and integrators of secure products and also to all types of organizations that provide security services and security engineering.

SSE-CMM serves the following purposes:

- Provides a tool for evaluating security engineering practices and defining improvements.
- Provides a basis against which customers can evaluate the service provider's capability as regards secure products and services.

- Serves as a self improvement model for helping developers of secure products and security service providers, to build confidence and assurance.

Did you know?

Process issues cause 53 percent of IT incidents—most often because no process is in place to manage the incident.

Sourcing processes

Definition

The procurement practices of an organization in order to find, evaluate and engage vendors of goods and services are called sourcing processes.

The purchasing processes should ensure that the processes are defined and capable of meeting organizational needs.

This involves several activities like:

- Timely identification of needs.
- Evaluation of product cost, performance and delivery and installation logistics.
- Method of evaluating that quality needs have been met.
- Contract administration, guarantee replacement or warranty, access to the vendors premises, vendor development and
- Reduction of vendor related risks.

Outsourcing

Outsourcing is an agreement in which part or all of an organization's IS functions are transferred to a third party for a fee as well as an agreed service level. It may involve the transfer of the IS resources no longer needed by the organization to the vendor.

After deciding to outsource an IS function, a rigorous process should be followed, including the following steps:

- Define the IS function.
- Describe the service levels required and minimum metrics to be met.
- Know the expected service provider's knowledge, skills and quality desired.
- Know the current in-house cost information to compare with third-party bids.

Variants

a. Out-tasking

Here, the responsibility of providing a particular service is given to multiple firms, instead of giving it to a single large organization.

b. Co-sourcing

This is normally done in human resource outsourcing, where the client is responsible for the management of outsourced activities, while the vendor provides consultancy services and experienced personnel when needed by the client organization.

Goals

"… the maxim of every prudent master in never to make at home what it will cost him more to make than buy". – Adam Smith

Outsourcing is a strategic decision for the management in order to achieve long-term improvement in business performance, by utilising the vendor's core competencies.

Successful implementation

We will see in the sections that follow, that its successful implementation depends on the 7 Cs:

1. Core competency
2. Contract duration
3. Control loss
4. Credibility of service provider
5. Conflict of interest
6. Cost of service provider
7. Continuity of operations.

Reasons

a. **Cost**
In this competitive world, there is a great need for cost savings and increase in sales due to the increasing pressure on profitability.

b. **Benefits**

The benefits are:

- Focus on the core activities only.
- Faster recycle times by using the time differences between say, USA and India.

- Obtaining economies of scale by reusing e.g. software components made for a previous client.
- Vendors often have more experience and specialization, develop better specifications and are likely to be able to devote more time and focus than internal staff, thereby reducing the chances of increasing scope of the assignment also known as "scope creep".
- Better specifications and contractual agreements than if developed only by in-house staff.
- Using the latest world class systems.

c. **Flexibility**
By having "a lean and mean organization", after restructuring, an organization can have a flexible organization structure.

d. **Risk**
Risks may be reduced by outsourcing, but as we shall see later, outsourcing has certain inherent risks which need to be addressed.

Risks

a) Costs
If there are hidden costs or the costs exceed expectations, then the business may end up with uncompetitive costs.

b) Confidentiality
There may be low data security because the information is traversing several international boundaries through the Internet.

c) Control
Once an internal department is closed down and its functions outsourced to a party, it may result in the loss of experienced staff and also it may be difficult to change the contract terms. Control loss may also occur where the vendor subcontracts the work to another party.

d) Competence
If the vendor IT systems become obsolete, or provides reduced services, then the strategic advantage of using the vendor may soon disappear.

e) Dependence on the vendor
The client may become dependent on the same supplier for many years to come, even beyond the period of the contract.

f) Business Continuity
The vendor's failure may result in the loss of quality or continuity of service.

g) High HR turnover

Vendors who run BPO units often have high staff attrition rates because employees do not consider them as the preferred choice for their long term careers.

h) Legislative impact

The country from which the vendor provides services may enact laws which may adversely affect the services provided. E.g. reducing the working week to less than seven days or preventing ladies from working during late night shifts.

Control of risks

The auditor's underlying thought process should be to ensure that the contract (a) protects the organization's interests, and (b) treats the vendor as a part of the organization from a controls perspective.

The organization should:

1. Establish a system of rewards and penalties for non-compliance of the contract terms.
2. Use several vendors instead of relying on a single vendor.
3. Withhold a part of the business in order to motivate the vendor.
4. Outsource only those functions which meet business needs instead of outsourcing all the IT functions.
5. Use domain experts to form a cross-functional contract management team, in order to provide the required assistance in negotiations.
6. Periodically review and benchmark the vendor's performance.
7. Use service level agreements and defined metrics to control the performance of the vendor which should also specify escalation procedures.
8. Try to implement short-term contracts.
9. Select vendors of good reputation, financial standing and those who can provide global services.
10. Not sign incomplete contracts.
11. Implement controls which prevent sub-contracting.
12. Design contracts with the assistance of the legal team, which are relevant to the organization, instead of using the vendor's standard contract.
13. Include arbitration and termination clauses where appropriate.
14. Ensure that the contract should have a right to audit clause or the vendor should provide a SAS 70 report as prescribed by AICPA. This also assists in a) validating the supplier's processes b) monitor their ability to deliver products or services which conform to required specifications and c) implementing supplier improvement programs.

15. Have backup plans in case of vendor failure.
16. Look for references before selecting a vendor.
17. Examine the vendor's organization controls for compatibility with the culture of the employing organization.
18. Carefully examine the clauses dealing with intellectual property rights.
19. Ensure that highly sensitive functions like research and development are considered for in-house development instead.
20. Clearly define the responsibility and accountability of the employer and vendor with respect to meeting insurance and regulatory requirements.
21. Ensure that vendors who provide similar services for competitors should have appropriate controls over e.g. data security.
22. Optimise the number of vendors.
23. Ensure two-way communication with vendors in order to solve problems and avoid delays and disputes.

Services provided

a) IS Facilities

- Telecom, voice, network, and data management.

b) IS Systems

- Systems development and maintenance
- Vendor, project, security and risk management
- Converting legacy systems to new application platforms
- Help desks and
- Call centres.

c) Finance

Management of:

- Banking
- Securities
- Insurance claims
- Tax returns
- Consumer finance
- Payroll etc.

d) Legal

- Knowledge and legal process outsourcing.

India is expected to capture 70% of the industry, about Rs. 53,000 crore, and employ 2.5 lac KPO / LPO professionals by 2010.

HR processes

These are the practices that should be employed by organizations in order to ensure that there are adequate controls over the entire lifecycle of the employee. The control practices will cover:

- Recruitment
- Indoctrination
- Promotion
- Training
- Scheduling
- Time reporting
- Performance evaluations
- Forced vacations
- Job rotation
- Exit practices.

According to a survey by Accenture of 40 HR heads in India, the order of effectiveness of HR in business metrics, with 1 being the most effective, is as follows:

1. Rewards, recognition and compensation
2. Alignment of workforce skills to business
3. Knowledge management
4. Recruiting
5. Career development
6. Leadership development
7. Change management
8. Performance measurement
9. Learning
10. Knowledge capture and transfer.

a. Recruitment

Controls

The objective of these practices is to ensure that the most effective and efficient staff is selected while complying with legal, regulatory and contractual requirements. The practices should encompass the following:

- Creating documented job descriptions and responsibilities.
- Communicating job requirements clearly to the applicant.

- Signing of confidentiality, non-disclosure, conflict of interest and non-compete agreements.
- Employee bonding required where there is high staff turnover, typically found in many IS departments.
- Checking of background and references.
- Screening applicants for mental and physical health.

Risks

In the absence of the above controls, there is a possibility of

- Unsuitable staff getting selected.
- Reference checks not carried out.
- Temporary staff and third-party contractors introducing uncontrolled risks.
- Compromise in the overall security due to lack of the awareness of confidentiality requirements.

b. Indoctrination

These programmes for staff are normally given on or soon after joining in order to ensure that the staff is made aware of the organization's corporate culture and code of conduct.

Controls

The programmes should explain:

- The organization's policies and procedures.
- Security policies and procedures.
- Employer expectations, company exceptions, employee benefits etc.
- Vacation and overtime rules.
- Prohibition of outside employment.
- Performance appraisal process.
- Emergency procedures in case of fire etc.
- Disciplinary proceedings in case of excessive absence from employment, breach of confidentiality and/or security, and non-compliance with policies.

Risks

The risks of not having such controls are many, like indiscipline, breach of code of conduct and non-compliance with the policies of the organization.

c. Promotion

The main objective of these practices is to retain and reward the staff for effective and efficient performance of their duties in achieving the objectives set out for them.

Controls

Promotion practices should be:

- Fair
- Clearly communicated
- Understood by all
- Based on objective performance criteria which consider the employee's performance, qualification, experience, personality, skills and level of responsibility.

Risks

The absence of such controls may lead to de-motivated staff and high attrition rates.

d. Training

Training programmes can cover: a) soft skills like motivation, leadership, team building, problem solving, communication skills, cultural and social behaviour, creativity and innovation, as well as b) hard skills like technical and project management. Determining personality traits and competence, awareness and training for staff is an important ingredient in achieving organizational success.

Controls

- Classroom and on the job training must be given to all employees in order to "sharpen their axe", thereby ensuring effective and efficient utilisation of the IS resources as well as to strengthen staff morale.
- Training must be imparted to relevant staff when new hardware or software is to be implemented.
- Training records of staff members should be kept.
- The effectiveness of training programmes should be evaluated.
- The training should make the staff aware of how their performance is linked with organizational goals.
- Training should include relevant management training, project management and technical training.

Risks

Lack of training may result in, deteriorating skill sets of employees, leading to ineffective utilisation of resources.

Dimensions of training

i. Cross-training

Cross-training is training employees to do one another's work. This enables more than one individual to perform a specific job or procedure.

Advantages

- It decreases the reliance on one staff member.
- It can be used to provide short-term backup for an absent employee.
- It can be used as a part of the corporate succession planning processes.

Risks

It allows a single person to understand all the processes in the system, thereby increasing his ability to perform irregularities.

ii. Job rotation

This enables the management to detect possible irregularities perpetrated by a staff member who has been transferred to another function or location.

Controls

This should be a standard practice for all the IS and other staff members.

Risks

It allows a single person to understand all the processes in the system, thereby increasing his ability to perform irregularities.

e. Scheduling & Time reporting

Controls

- Scheduling enables the effective and efficient use of the IS resources, while time reporting enables the scheduling process to be monitored by the management as per the time schedule.
- They both ensure that operations are performing efficiently and also assist in determining staff levels required.

Risks

Without the above controls, the effectiveness and efficiency of the IS resources may be impaired.

f. Performance evaluations

This process should be deployed for all IS staff to motivate employees who are measured against their job descriptions and other performance criteria.

Controls

- The HR department should ensure that managers and employees set mutually agreed-upon goals / expected results. Assessment should be based on these goals.
- Salary increments, performance bonuses and promotions should be based on performance.
- Employee aspirations and satisfaction should be judged from the process and problems should be identified.

Risks

Without this "stick and carrot" practice, the staff may be de-motivated to achieve the organizational goals.

g. Forced vacations

This process ensures that while one person is on leave, another person executes the functions of that person enabling the detection of possible irregularities.

Controls

This should be a standard practice for all IS and other staff members.

Risks

Without this practice, the possibility of irregular acts remaining undetected will be high.

h. Exit practices

These practices must define the steps for employee job termination, whether voluntary or forced by the employer, in order to secure the IS assets.

Controls

- The employee should return access and identity cards in order to prevent physical access to the premises.

- The employee's passwords and user IDs should be deleted from the system in order to prevent logical access.
- Related IS and security personnel should be intimated about the employee who is leaving the organization.
- The person leaving should be deleted from the payroll files after executing his full and final payment.
- All company property like, laptops, mobile phones, PDA's, etc. should be returned to the employer.
- An exit interview with the leaving employee should be arranged in order to gain insights regarding his reasons for leaving and his perception of the management.
- Security personnel should apply appropriate procedures like searching the person for portable devices like memory sticks which may contain sensitive corporate information.
- The person should be escorted from the organization's premises in order to prevent any irregular acts while leaving.
- The person should be made to sign a nondisclosure agreement for a period during which he should not disclose any confidential information after his exit from the organization.

Risks

The absence of these controls may lead to uncontrolled risks like theft, destruction of the IS assets, breach of confidentiality etc.

Documentation processes

Studies have shown that documentation was an important factor affecting the time taken to complete a project and ensure that processes are effective and efficient. Documentation of systems is also a requirement of standards like ISO 27001 and ISO 9001. The nature and extent of the documentation should include legal, regulatory and contractual requirements, decisions taken by the organization, any external source for the development of the competencies of the organization and the needs and expectations of stakeholders.

Management's problem is to determine the level of documentation needed in the information system. The benefits should outweigh the costs. It provides guidance and is useful in ensuring that standard procedures are followed across the organization. Documentation should exist for the primary functions within the IS enterprise. These typically include:

- IS operations
- System software

- Hardware and software acquisition and maintenance
- Application software
- Management reporting
- Physical and logical reporting
- Physical and logical security
- Time reporting
- Short and long term planning
- Quality processes
- Organizational structure
- Human resource management.

Documents should be approved, reviewed, updated when necessary; available to those who need it, legible, readily identifiable and destroyed on becoming obsolete.

Management Organization Structures

The important functions of management like planning, organising resources and implementing processes and controls have been discussed above. We will now discuss another very important area which is to organize the people and resources in the organization.

Organization structure defines the hierarchy, authority, roles, responsibilities and reporting structure of an enterprise. It determines the type of job done by each class of employees and provides job descriptions.

The following areas will be discussed:

a. Project and Line Management

b. The risks and controls of the various roles performed by personnel in the IS Department

The Management must organize the people in such a manner that the organizational goals are achieved. The structures shown in the succeeding sections are suggestive instead of being prescriptive.

The two kinds of management structures that may be found in organizations, are project and line management.

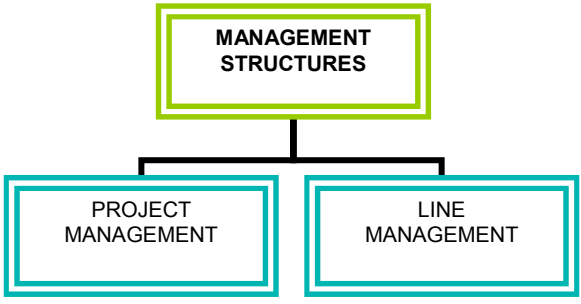


Fig. 6 Types of Management Structures

i. Project management structure

Project management is responsible for implementing IT projects within the framework of project management guidelines. It may be done in-house or outsourced for one time projects, and they consist of people who are drawn from line management. The key aspects include defining project ownership, clearly outlining user involvement, implementing project management plan and methodology and quality assurance methods and plans. All projects should have specific:

- Objectives or deliverables.
- Phases with timelines or milestones in order to measure the achievement of the objectives.
- Specific start and end dates.
- Work breakdown structure for determining the sequencing of the project activities.

All such projects are headed by a Project Manager who is, normally, appointed by the IS Steering Committee. The project manager in turn will appoint a project team consisting of those persons who have a stake in the making of the project, e.g.:

- Technical experts
- Relevant users
- IS auditors who act as control experts
- Quality assurance professionals
- Security professionals etc.

Project teams tend to have a flat organization structure with few hierarchy levels:

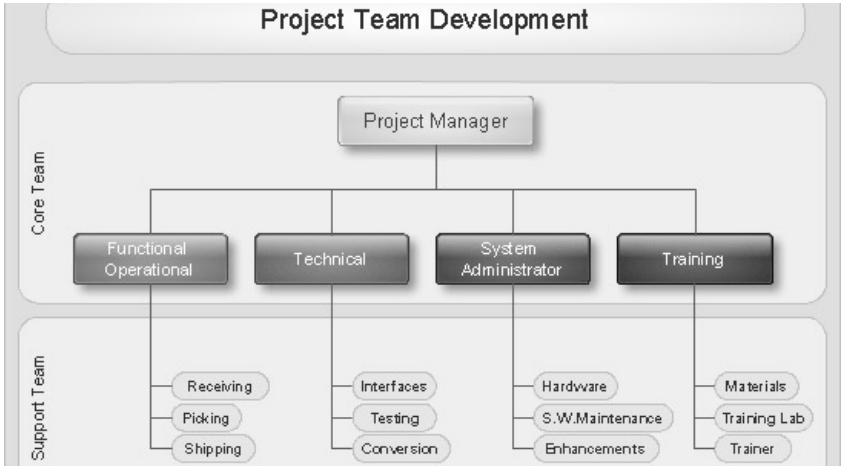


Fig.7 A typical project management team

ii. Line Management Structure

Line management is responsible for regular business processes and operations. It, normally, deals with the daily routine functions which are not related to projects. The IS management subsystems in an enterprise attempt to ensure that the development, implementation, operation and maintenance of information systems proceed in a planned and controlled manner. Such structures are normally found in most organizations and typically have many layers of reporting as shown below:

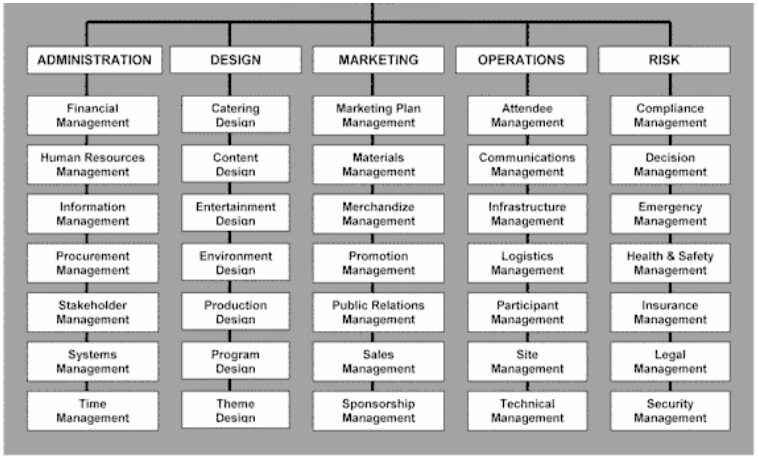


Fig.8 An extract from a line management structure (Suggestive).

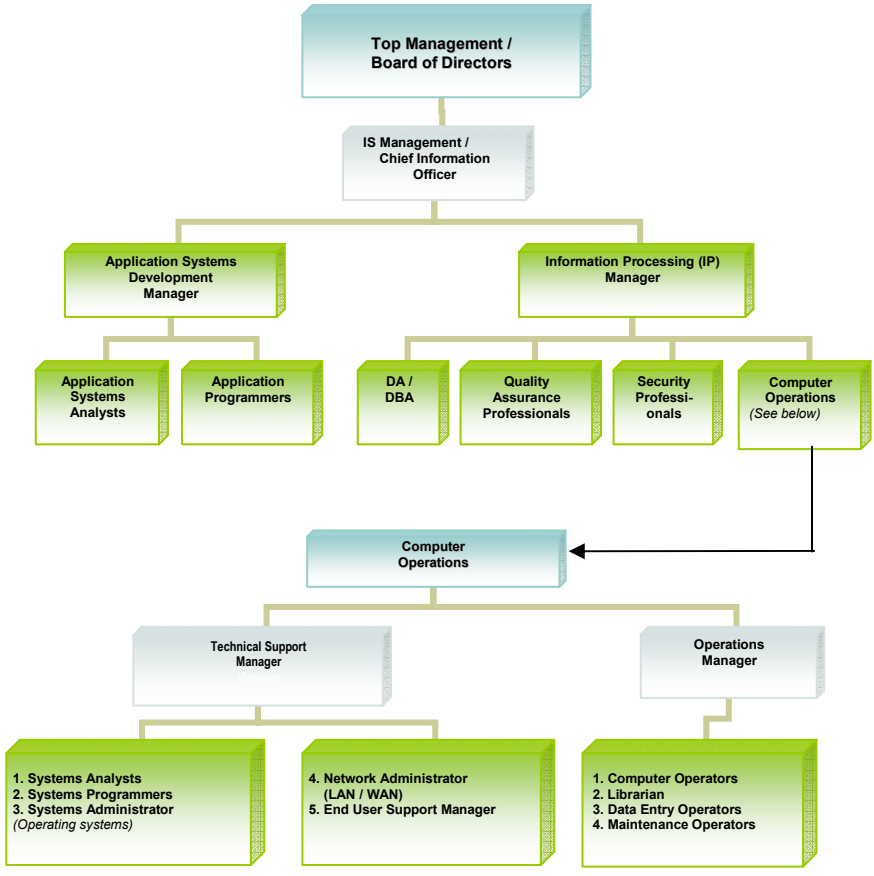


Fig.9 IS Line Management Structure (Suggestive).

The risks and controls of the various roles performed by personnel in the IS Department

1. Chief Information Officer, CIO

Roles & Responsibilities

The CIO reports to the Chief Operating Officer or the Board of Directors and is the overseer of all IT activities in most organizations. He is responsible for the alignment of strategic business goals with the IT processes. Instead of routine day-to-day functions, he focuses on business, IT planning and strategy. The IT processes cover delivery and support of:

- Traditional computer data processing services
- Internet technology
- Telecommunications
- Network services
- User support etc.

Controls

In view of the importance of this function, the following internal controls may be employed:

- Regular interface with the Board of Directors.
- Training and other appropriate HR controls discussed above in order to ensure his competency and trustworthiness.
- His work should be documented and subject to regular reviews.
- Access should be granted on a "need to know", "need to do" basis.

Risks

- Inadequate interface with the top management may result in the loss of alignment with business and IT processes.
- This position may give him unrestricted access to the system.
- Inadequate background checking and performance review may bring in uncontrollable risks.

2. Application Systems Development Manager (ASDM)

Roles & Responsibilities

The main role of the ASDM is to oversee the work of (a) application systems analysts and (b) application programmers, who design, develop and maintain new or existing application programs.

Controls

- Employ a competent and trusted person by deploying the HR controls discussed earlier.
- Regular interface with the CIO.
- His work should be documented and subject to regular reviews.
- Access should be granted on a "need to know", "need to do" basis.

Risks

- Inadequate communication with the CIO may result in the loss of effectiveness and efficiency of this important function.
- Work may not have been documented and subject to regular reviews.

- Access may have been granted without reference to his job needs.

3. Application Systems Analysts

Roles & Responsibilities

Such persons are responsible for designing application systems based on user specifications, resulting in the development of functional specifications and other high level systems design documents required by the application programmers.

Controls

- Employ a competent and trusted person by deploying the HR controls discussed earlier.
- Work should be documented and subject to regular reviews.
- Access should be granted on a "need to know", "need to do" basis.

Risks

- Inadequate HR controls may introduce an undesirable person in the company.
- Work may not have been documented and subject to regular reviews.
- Access may have been granted without reference to his job needs.

4. Application Systems Programmers (ASP)

Roles & Responsibilities

The main role of the ASP is to develop new application systems and maintain the existing production systems based on the design made by the application systems analyst.

Controls

- Employ a competent and trusted person by deploying the HR controls discussed earlier.
- He should not have access to live programs and data.
- He should work in a test–only environment.
- He should not be allowed to have any change control duties that would enable him to say, modify a program and launch it in the live environment without going through change controls like quality control, security and end user signoff.

Risks

The main risks are the manipulation of live programs and the data in order to perpetrate a fraud.

5. Data Management

This function may be segregated into two parts.

a. Data Administrator (DA)

Roles & Responsibilities

This role may only be found in large IT environments only, while in smaller IT environments, the functions of the DA may be merged with those of the database administrator. The DA is responsible for the long term planning of the data architecture and management of data. It is, basically, a policy making and administrative role.

The DA functions are to:

- Undertake strategic data planning, determining user needs.
- Specifying validation criteria for data.
- Specifying new conceptual and external schema definitions.
- Specifying retirement policies for data.
- Determining end-user requirements for database tools; testing and evaluating end-user database tools.

b. Database Administrator (DBA)

Roles & Responsibilities

The DBA performs a technical role, and is responsible for short term planning, design, definition, maintenance and integrity of the database systems in an organization.

The DBA functions are to:

- Define, manage, create and retire the data.
- Specify and change the physical data definition.
- Make the database available to users.
- Service the users' needs.
- Maintain database integrity.
- Monitor database operations.
- Set up new installation, perform upgrades and migrations.
- Select and implement database optimization tools.
- Test and evaluate programmer and optimization tools.
- Implement database definition controls, access controls, update controls and concurrency controls.

- Monitor database usage, collect performance statistics and tune the database.
- Define and initiate backup and recovery processes and procedures
- Ensure security of the data.
- Mediate between users in case of conflicting requirements.

The difference between the duties of the DA and DBA may be summarised as follows:

	Data Administrator	Database Administrator
Nature of work	Administration: making policies and standards	Technical: implementing policies made by the DA through database controls
Liaison with	Chief Information Officer	Application programmers and analysts
Horizon	Long term data planning	Short term database development
Scope	All databases	Specific database(s)
Data Design	Logical design	Physical design
Focus of work	Metadata Data Dictionary Data Analysis Independent of the DBMS	Data Database Data design DBMS specific

Controls

- Separate the duties of the DA and DBA wherever possible.
- The DBA's job profile and activities should be approved by the management.
- Access logs should be enabled and reviewed by an independent person.
- The use of database tools should be subject to detective controls.
- Employ a competent and trusted person by deploying the HR controls discussed earlier.
- He should be given appropriate training in the latest DBMS tools and systems.
- He should not have any application programming or end user responsibilities.
- He should be prevented from accessing live data in the databases.

Risks

- The DBA is a very technical person who can use the tools to access and modify live data and programs in order to perpetrate a fraud.

6. Quality management

Quality management is the means by which the IS department based processes are controlled, measured and improved. Processes in this context are defined as a set of tasks that when properly performed, produce the desired results. These processes may be split between assurance and control functions. These processes which impact all IT related functions, also follow the PDCA cycle, namely:

- Formulate quality goals.
- Implement standards.
- Monitor processes, report and train users.
- Suggest programs for obtaining improvement in the processes.

Roles & Responsibilities

a. Quality Assurance Manager

This function deals with assuring adherence to prescribed quality processes in all IT related functions like programming, data entry etc., e.g. ensuring that programs and allied documentation adhere to the prescribed standards and computer naming conventions adopted by the organization.

b. Quality Control Manager

This function deals with applying quality control procedures, e.g. conducting tests in order to verify and ensure that the software and other allied processes are free from defects before they are transferred to the live operations and that it meets the needs and expectations of the end users.

Controls

- Employ a competent and trusted person by deploying the HR controls discussed earlier.
- He should be given appropriate training in the latest quality management systems.
- He should not have any application programming responsibilities because he is the “checker” not the “maker” of a system.
- He should report to the CIO in order to maintain his independence.

Risks

There will be impairment in quality processes if:

- A person is allowed to carry out a quality review of his own work.
- Incompetent persons are recruited due to inadequate HR controls.
- Quality management do not have independence in their reporting function.

7. Security management

Roles & Responsibilities

Top management should demonstrate their commitment to security by developing an information security management policy within the characteristics of the business, its assets, technology and the organization. This includes the development of business continuity and disaster recovery plans related to the IS functions. The approved policy should state the:

- Framework for setting objectives that gives a sense of direction to information security.
- Business, legal, regulatory and contractual requirements that apply.
- Alignment of the policy with the organization's strategic risk management process.
- Criteria for determining how risk will be evaluated.

The main functions of the security manager are to:

- Maintain the access rules for the data and other IS resources.
- Ensure security and confidentiality for the issuance and maintenance of authorised user IDs and passwords.
- Monitor activities for security breaches and take appropriate corrective actions.
- Review the security policy and suggest necessary changes.
- Provide appropriate training and awareness programs to users.
- Test the security processes in order to determine their strengths and weaknesses and detect possible threats.
- Implement new or better security software.

Some organizations reference the responsibilities of the security manager to the security management policy document or in an annexure to the policy document.

Controls

- The security manager should report directly to the CIO in order to maintain his independence. In small organizations where this is not possible, he may report to the operations manager, in which case some compensation controls like monitoring and awareness may apply.
- Employ a competent and trusted person by deploying the HR controls discussed earlier.
- He should be given appropriate training in the latest security management systems.

- He should not have any conflicting duties like application programming responsibilities because he is the "checker" not the "maker" of a system.

Risks

There will be an impairment in the security management processes if:

- The security manager is allowed to carry out conflicting work like application programming.
- Incompetent or dishonest persons may be recruited due to inadequate HR controls.
- The security manager does not have independence in the reporting function.

8. Technical support manager

Roles & Responsibilities

This function is responsible for overseeing the following technical support functions:

- Systems Analyst
- Systems Programmer
- Systems Administrator
- Network Administrator
- End User Support Manager.

Controls

- Employ a competent and trusted person by deploying the HR controls discussed earlier.

Risks

- Incompetent or dishonest persons may be recruited due to inadequate HR controls.

9. Systems Analyst

Roles & Responsibilities

This function is not likely to be seen in most organizations because it involves the designing of operating systems, which are now available off-the-shelf by leading companies like, Microsoft Windows OS and Apple's Mac OS. They are responsible for designing systems software and therefore, they may have complete access to the system libraries. They interpret the user needs and develop requirements and functional specifications, as well as high-level design documents; which enable programmers to create the particular application.

Controls

- Employ competent and trusted persons by deploying the HR controls discussed earlier.
- Their activities should be recorded in the computer logs in order to detect access breaches.
- Access to the system libraries should be granted on a “need to know”, “need to do” basis.

Risks

- Inappropriate HR controls as discussed earlier may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer logs are not enabled, any breach of security will remain undetected.

10. Systems Programmer

Roles & Responsibilities

Again, this function may not be seen in most organizations because the programmers are responsible for developing and maintaining the operating systems and systems softwares designed by the systems analyst. Therefore, they may have complete access to the system libraries.

Controls

- Employ competent and trusted persons by deploying the HR controls discussed earlier.
- Their activities should be recorded in the computer logs in order to detect access breaches.
- Access to the system libraries should be granted on a “need to know”, “need to do” basis.
- Usage of domain administration and superuser accounts should be tightly controlled and monitored.

Risks

- Inappropriate HR controls as discussed earlier may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer logs are not enabled, any breach of security will remain undetected.

11. Systems Administrator

Roles & Responsibilities

In view of the fact that large organizations may have LANs spread over many geographical locations, each LAN will require an administrator for technical and administrative control of the LAN. The responsibilities of this function include:

- Creation and deletion of user accounts.
- Installation and maintenance of systems software e.g. the operating system.
- Taking proactive virus prevention measures.
- Allocating storage space for the data and programs.
- The addition and configuration of client machines.
- Maintenance of major multi-user computer systems, including local area networks as well as mainframe systems.
- Initiating backups at the end of or during the day.

Controls

- Employ competent and trusted persons by deploying the HR controls discussed earlier.
- Their activities should be recorded in the computer logs in order to detect access breaches.
- Access to the system libraries should be granted on a “need to know”, “need to do” basis.
- He should not have any application programming duties.

Risks

- Inappropriate HR controls as discussed earlier may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer logs are not enabled, any breach of security will remain undetected.

12. Network Administrator

Roles & Responsibilities

They are responsible for the entire network of the organization which may include LANs, WANs and wireless communication and voice networks. The infrastructure of the network may include routers, hubs, switches, firewalls, network segmentation through e.g. VLANs etc. They are also responsible for network performance management, network maintenance, remote access etc.

This position is responsible for technical and administrative control over the LAN. This includes ensuring that transmission links are functioning correctly, backups of the system are occurring, and software/hardware purchases are authorized and installed properly.

Controls

- Employ competent and trusted persons by deploying the HR controls discussed earlier.
- He should not have any application programming responsibilities.
- His activities should be recorded in the computer logs in order to detect access breaches.

Risks

- Inappropriate HR controls as discussed earlier may lead to employment of persons who may be incompetent or untrustworthy.
- He may breach the confidentiality, integrity and availability of data by eavesdropping on the communication between two nodes on the network or by launching denial-of-service attack..

13. End User Support Manager

Roles & Responsibilities

This function is responsible for the liaison between the end users and the IS department, including the management of the help desk. The function of the help desk is to resolve the users' hardware and software technical problems through e-mail, telephone or the fax machine. All the reported problems are recorded and the user is given a reference number for his complaint. The help desk will send this complaint to the appropriate engineers who will resolve the problem by telephone, fax, e-mail or by personal visit to the user. The help desk may also acquire hardware or software and train users in order to enable the user to function effectively and efficiently. In very large organizations this function is becoming more and more important. The function may be performed in-house or outsourced.

Controls

- All user complaints should be logged and allotted a complaint number.
- Depending on the severity of the complaint, the complaint should be forwarded to the appropriate engineer.
- All unresolved problems should be followed up and closed by an independent person.

- Competent and trusted staff should be employed.
- Complaints should be periodically summarised and reviewed for the nature and frequency of the complaints.

Risks

- Inappropriate HR controls as discussed earlier may lead to employment of persons who may be incompetent or untrustworthy.
- If the computer complaint logs are not enabled, the resolution, frequency and nature of complaints will remain undetected.

14. Operations Manager

Roles & Responsibilities

The operations manager's functions include responsibility for computer operations personnel including computer operators, librarians, data entry personnel and maintenance operators. They are also responsible for physical and data security of the department.

Controls

- A competent and trusted person should be employed based on the HR controls discussed earlier.
- Only operations personnel should have access to the operations department, based on the "need to know", "need to do" access principle.
- All operations and programming functions should always be separated.

Risks

- Inappropriate HR controls as discussed earlier may lead to employment of persons who may be incompetent or untrustworthy.
- Unauthorised access to the operations centre may result in breach of security.

15. Computer Operators

Roles & Responsibilities

They are mainly responsible for scheduling and allied activities in order to run the computer system effectively and efficiently. This role is not likely to be seen in most modern organizations due to such activities being automated by the more powerful computer systems used now.

Controls

The controls are the same as those for the operations manager discussed above.

Risks

The risks are the same as those for the operations manager discussed above.

16. Librarian

Roles & Responsibilities

The librarian function may be performed manually or by software which can also provide for version control etc. The librarian is the stock keeper of all data and program files kept on storage media like tapes and hard disks. He is responsible for recording, issue, receipt and maintenance of computer files and the data. It may be a full time function or it may be performed by the data entry department depending on the size of the organization.

Controls

The librarian should:

- Be a competent and trustworthy person employed using the HR controls described earlier.
- Keep a log of all files and media issued against an authorisation.
- Rotate the data on the media and degauss it when necessary.
- Provide for appropriate physical and environmental controls in order to protect the data from damage.
- Ensure that file retention and purge dates are maintained for all files.
- Segregate sensitive files in order to alert the librarian that such a file is being used or requested for.
- Provide for onsite and offsite backups of the data and programs.
- Ensure that media is kept in a secure manner.
- Ensure that files are up to date and have internal and external file headers.
- Ensure that software is not stolen, misused, duplicated or destroyed.
- Ensure that the software license terms are not violated.

Risks

- Inappropriate HR controls as discussed earlier may lead to employment of persons who may be incompetent or untrustworthy.
- Unauthorised access to the library may result in the breach of security.

17. Data entry operators

Roles & Responsibilities

Data entry can be performed in batch (offline) or online mode. In the modern environments, this function is performed by the user departments. The users are

provided with appropriate application programs which can verify and validate the data using e.g.:

- Range checks
- Alpha-numeric checks
- Limit checks and
- Reference to predefined value checks from an internal table.

Batch controls would include e.g.

- Retaining source documents until the processing is complete.
- Batch headers, control totals and hash controls.
- Proper scheduling of input.
- Verification of logs e.g. error logs.
- Distribute output to authorised persons only.
- Ensuring the confidentiality of information.

Controls

- Only authorised persons should be allowed to perform data entry through appropriate logical access controls.
- All data accepted for input should be validated, accurate, complete and authorised.
- Only authorised persons should be permitted physical access into the data entry department.
- Competent and trustworthy persons should be employed using the HR controls described earlier.
- Staffing levels should be adequate, data entry personnel should be subject to rotation of duties and only two operators should be allowed per shift.
- Work schedules should be adhered to and monitored.
- Work should only be done in compliance with standard written procedures and instructions.
- Staff should be adequately supervised.
- Exceptions and rejected input should be notified to the originating department, corrected, resubmitted on time and go through the data entry process again from the start.
- Staff should ensure the confidentiality of the data and be allowed to modify the data.
- Staff should be trained for backups and emergencies.
- Source documents should be kept for the retention period.
- Data entry personnel should not have any application programming duties.

- Data entry and data correction duties should be separated from data authorisation duties in order to ensure that the output is accurate and complete.

Risks

- If the integrity and confidentiality of the data is lost then the information produced may lead to inappropriate decision making.
- Inappropriate HR controls as discussed earlier may lead to employment of persons who may be incompetent or untrustworthy.
- Unauthorised access to the data entry area may result in breach of security.

18. Maintenance operators

Roles & Responsibilities

This function may be performed by the help desk in-house or it may be outsourced. Their main function is to ensure that the hardware is working properly.

Controls

- The organization should adhere to the vendor's maintenance schedule.
- Maintenance should be done on time.
- Logs on maintenance should be kept showing dates, names, costs, nature of problem etc.
- Maintenance reports should be issued in order to monitor performance by using maintenance software.
- In order to discover irregularities, the work of one engineer should be evaluated by another and their duties should preferably be rotated.
- Sensitive data and programs should be removed from the machine before it is handed over to the engineer.
- Maintenance engineers should be subject to HR controls like background checking, signing of non-disclosure agreements etc., discussed earlier.

Risks

- If the integrity and confidentiality of the data is lost then the information produced may be modified leading to incorrect decision making or it may be disclosed to unauthorized parties.
- Inappropriate HR controls as discussed earlier may lead to employment of persons who may be incompetent or untrustworthy.
- Equipment that may require to be retired may not be identifiable if maintenance reports are not kept.

- Breach of the supplier's maintenance terms may lead to cancellation of the equipment warranty or guarantee.

Separation of Duties

Separation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions. The main purpose of separation of duties is to prevent or detect errors or irregularities by applying suitable controls. It diminishes the likelihood of errors and wrongful acts going undetected because the activities of one group or individual will serve as a check on the activities of the other.

The irregularities are frauds due to e.g.:

a. Theft of assets like funds, IT equipment, the data and programs.
b. Modification of the data leading to misstated and inaccurate financial statements.
c. Modification of programs in order to perpetrate irregularities like rounding down, salami etc.

The controls will ensure that the threats and irregular acts minimise the potential damage from the actions of a person or persons. The organization structure and allied controls should be structured in a manner that ensures the highest level of separation of duties.

The critical factors to be considered in segregation of duties in a computerized information system are:

- Nature of business operations
- Managerial policy
- Organization structure with job description
- Information technology resources deployed such as:
    - Operating system
    - Networking
    - Database
    - Application software
    - Technical staff available
- IT services provided in-house or outsourced
- Centralized or decentralized IT operations.

Based on the above factor, appropriate separation of duties has to be achieved. The most important aspect is to define access to information based on "need to know" or "need to do" basis. Access to each class/type of data has to be defined based on the specific job responsibility.

The traditional notion of separation of duties is to separate those persons:

a. Who can initiate a transaction, from those
b. Who can approve the transaction, from those
c. Who have custody of assets, from those
d. Who can record the transaction.

For example, if a cashier can raise a purchase order, approve the vendor's invoice, make payment against the invoice and record the transaction in the cash book, it would be considered an inappropriate situation.

While the traditional notion of separation of duties will continue to apply, it may not apply always to computer-based systems where the controls are embedded in the computer application system. For example, an application program could match a vendor's invoice against the purchase order and print a cheque for the amount due to the vendor and record it in the database.

Therefore, computer systems need to be approached in a different manner in order to check for incompatibility of functions.

In this connection the following general guidelines may be followed in conjunction with concepts like, the maker should not be the checker:

1. Separate those who can run live programs e.g. operations department, from those who can change programs e.g. programmers. This is required in order to ensure that unauthorised programs are prevented from running.
2. Separate those who can access the data e.g. data entry and the DBA, from those who can run programs e.g. computer operators. This is required in order to ensure that unauthorised data entry cannot take place.
3. Separate those who can input data e.g. data entry, from those who can reconcile or approve data e.g. data authorisation persons. This is required in order to ensure that unauthorised data entry cannot take place.
4. Separate those who can test programs e.g. users, quality assurance and security, from those who can develop programs e.g. application programmers. This is required in order to ensure that unauthorised programs cannot be allowed to run.
5. Separate those who can enter errors in a log e.g data entry operator who transfer the data to an error log, from those who can correct the errors like the end user departments. This is required in order to ensure that unauthorised data entry cannot take place.
6. Separate those who can enter data e.g. data entry personnel, from those who can access the database e.g. the DBA. This is required in order to ensure that unauthorised data entry or data modification cannot take place.

Compensating controls

There may be situations where it may not be possible to have adequate separation of duties due to business reasons. This is likely to be the case in small organizations where the same person may be performing conflicting duties like program development and also launch the program in the live environment without going through adequate change management controls.

In such cases, the IS auditor should look for compensating controls.

Compensating controls are internal controls that are intended to reduce the risk of an existing or potential control weakness where the duties cannot be appropriately separated. In other words, the existing controls cannot prevent, detect or correct the control weakness. These controls may take many forms like:

- Monitoring activities through observation or enquiry or an independent review through assurance processes like auditing.
- Enabling audit trails and transaction logs in order to determine the accountability of actions like, who initiated the transaction, at what time, and entered what data in which file.
- Transaction reconciliation procedures like control totals and balancing sheets, which ensure that totals of batches sent for processing, agree with those received back from the processing department.
- Exception reports may be produced and reviewed by a senior manager before the day's activities are closed and backups taken.

Check

As stated earlier, this part of the Deming cycle involves monitoring, evaluation and reporting of the processes and results against the established goals. This stage involves analysing the data, monitoring trends and comparison of actual results against planned results.

The inputs of a management review or check may include:

a. Results of process assurance reviews.
b. Feedback from employees, vendors etc.
c. New management techniques which could improve the efficiency and effectiveness of the management processes.
d. The status of preventive and corrective actions.
e. Addressing threats and vulnerabilities which may not have been properly addressed in the risk analysis programme.
f. Results from effectiveness measurements like equipment maintenance reports, help desk reports.

g. Follow-up action of previous reviews.
h. Recommendations for improving the processes, from audit reports, quality reports, benchmark reviews, performance of suppliers etc.
i. External factors e.g. new technology, research and development, competitor performance.
j. Process performance and product conformity.

The results that could be expected from the review process are:

a. Suitability of resource needs and the organization structure.
b. Improvements in products and processes.
c. New strategies for meeting the needs of interested parties.
d. Better risk mitigation plans.
e. Identification of information required for future strategic planning needs.

The result of the management review may include decisions related to:

a. Improving the processes.
b. Updating risk management plans.
c. Modifying processes, procedures and work instructions in order to ensure that IT processes are properly aligned with business objectives.
d. Meeting legal, regulatory and contractual requirements defined in e.g. SLAs or OLAs.
e. Modifying resource needs.
f. Improving the effectiveness of controls being used to measure performance.

The process assurance reviews noted above or internal audits can be conducted at planned intervals in several areas, e.g.:

- The effectiveness and efficiency of the implemented IS processes and resources.
- Any opportunities for improvement.
- The capability of processes to deliver.
- Analysis of the data on costs and quality.
- Comparison of actual against budgeted results.
- Relationships with stakeholders like vendors.
- Self assessment of the maturity of processes.

Act

As stated earlier, the purpose of this phase of the Deming cycle is to apply necessary actions in order to bring about necessary improvements. This may involve repeating the PDCA cycle with changes, adopting the change or abandoning it and restart the planning process.

The ultimate objective of this phase is to ensure continual improvement in the IS processes. This is done by eliminating any non-compliances in order to prevent their recurrence, which is often more cost effective than corrective action, by:

a. Identifying the root cause of the problem.
b. Determining the appropriate corrective action required.
c. Recording the results of the action taken and its subsequent review.

The sources from which the management can take corrective action are:

1. Customer complaints,
2. Reports on non compliance with processes,
3. Internal audit reports,
4. The outputs from the management review, data analysis and satisfaction measurements,
5. Relevant IS management system records,
6. Staff feedback and suggestion programmes,
7. Process measurements, and
8. The results of self assessment exercises.

Summary

The IS management process is to establish a fundamental basis for managing information technology to deliver value to the organization. The best practices and standards are implemented to align IT to the organization business processes. To realizing the value of IT requires a partnership between the organisational management and the IT management personal. The IS management process includes a shared strategy, managing enterprise risk, establishing shared goals, and methods to measure the performance of all parties. These measures are to be aligned to the objectives of the organization, the underlying data needs to be accurate and timely, and reporting needs to be in a format that is easy to understand.

Questions:

1. An IS auditor's review of an organization's management controls reveals that there is no review of organization charts, separation of duties, documentation and succession plan. From these findings, he would most likely conclude that the organization is prone to which of the following risks:
   a. Lack of governance
   b. Low organizational productivity
   c. Lack of internal controls
   d. All of the above.

2. An IS auditor discovers that there are no policies and systems to prevent unauthorised disclosure of data. From this finding, he is most likely to conclude that the organization is prone to the following risks:
   a. Possible lawsuits
   b. Leakage of data to competitors
   c. Both A and B
   d. Neither A nor B.

3. An IS auditor's findings during the audit of third party outsourcing, show that there are no documentation to support service level agreements, right to audit clause, software escrow agreement. Based on these findings, he would most likely conclude that:
   a. Vendor failure will lead to the organization's failure.
   b. Vendor's business failure has no relationship with the organization's future success.
   c. The only guarantee to the organization's success is to audit the vendor's internal controls.
   d. Service levels are not required to be defined.

4. Which of the following is the correct order of the Deming Cycle:
   a. Plan, Do, Act, Check
   b. Plan, Check, Do, act
   c. Plan, Act, Do, Check
   d. Plan, Do, Check, Act.

5. An IS auditor has read the minutes of the meeting of the IS Steering committee, dated a year ago, which recommended the use of the Deming cycle in their management processes. However, on investigation, he finds that there is no evidence of its deployment in the processes of the organization. He would most likely conclude that there may have been impediments to its use like:
   a. Lack of resources and lack of management commitment
   b. Management complacency and emergence of urgent tasks
   c. Management complacency and inadequate communication to the employees
   d. All the above.

6. Which of the following options for corporate management is the desirable order in order to translate the desired goals into statements of action:
   a. Policies, Standards, Guidelines, Procedures
   b. Policies, Guidelines, Standards, Procedures
   c. Policies, Standards, Procedures, Guidelines
   d. Policies, Procedures, Guidelines, Standards.

7. An IS auditor is conducting an audit of the strategic planning process of an organization. Which of the following statements would be true if the strategic document states:
   a. The immediate IS resource needs
   b. The desired future position of the organization after three years
   c. The project completion dates during the next year
   d. The operational business plans

8. Which of the following options would the IS auditor consider to be false with respect to making good policies by the management:
   a. Policies are usually low level and static documents and define what is or is not allowed in the organization.
   b. They are the starting point for creating the standards, guidelines and procedures that are needed in the organization.
   c. Because they are developed by the top management, they let lower level management think that there is consensus at the top.
   d. In some organizations, individual departments are permitted to define lower level, i.e. operational policies only.

9. An IS auditor has been requested by the top management to guide them in the best practices for making policies. He would ideally recommend all the following except:
   a. High level policies should only be made by the top management.
   b. Low level policies should only be made by the top management.
   c. Employees should be communicated through clear communication channels and receive appropriate training.
   d. Policies should be regularly reviewed and updated.

10. The statement "We have made the right product as required by the user" is best described by the word:
    a. Verification
    b. Validation
    c. Authorisation
    d. Accountable.

11. During an IS audit of the planning function, which is the most likely order in which he will examine the related documents:
    a. Goals, Policies, Standards, Guidelines, Procedures.
    b. Goals, Policies, Standards, Procedures, Guidelines.
    c. Policies, Goals, Standards, Guidelines, Procedures.
    d. Policies, Goals, Standards, Procedures, Guidelines.

12. An IS Auditor of a multinational company has been asked by the Board of Directors to list the attributes that they should look for while examining candidates for the post of the CEO. Which of the following attributes is he least likely to recommend:
    a. Clarity of strategic objectives and ethical conduct,
    b. Lead by example and take calculated business risks,
    c. Identify breakthrough innovations in processes,
    d. Deep knowledge of IT.

13. Which of the following would the IS auditor consider to be the least appropriate activity for an IS steering committee:
    a. Act as an overall review board for all the IS projects irrespective of their size.
    b. Review long range and short range plans in order to ensure that they are aligned with the organization's mission and objectives.
    c. Review and approve major acquisitions of the IS resources within the limits approved by the Board.
    d. Monitor the progress of major projects, lay down priorities, and develop policies, standards, guidelines, procedures.

14. The best document to be reviewed by an IS auditor for formalising an internal agreement for the provision of the IS services between the end users and the IS department would be:
    a. An out-tasking agreement,
    b. An Operating Level Agreement,
    c. A Service Level Agreement,
    d. A co-sourcing agreement.

15. An organization opting for certification of their processes for compliance with the requirements of quality management systems would opt for which of the following:
    a. ISO 9000
    b. ISO 9001
    c. ISO 9004
    d. ISO 9126.

16. Which of the following are the main attributes of ISO 9126-1:
    a. Fault tolerance
    b. Learn ability
    c. Stability
    d. Portability.

17. The Optimised phase of the Capability Maturity Model would have which of the following characteristics in its software development processes:
    a. There are sound policies for software project management.
    b. Software training programs are implemented.
    c. High quality software products are produced.
    d. Methods to prevent software defects are employed.

18. A software development team has made a new financial accounting application program for the organization. Which of the following person(s) would the IS auditor expect to sign off on the acceptability of the program before it is moved into the live environment:
    a. Application programmer
    b. Quality control
    c. Security
    d. End users.

19. HR controls in the IS department like, background checking, are relevant for which of the following:
    a. Full time staff
    b. Part time staff
    c. Contractors
    d. All of the above.

20. Which of the following is the most appropriate role for the Data Administrator:
    a. Long term planning of the data architecture
    b. Service the users' needs
    c. Define, manage, create and retire the data
    d. Make the database available to users.

21. The role of a Technical Support Manager would not normally include overseeing the work of which of the following functions:
    a. Systems Administrator
    b. Network Administrator
    c. Operations Manager
    d. End User Support Manager.

22. Which of the following controls are not relevant to the librarian?
    a. Provide for onsite and offsite backups of the data and programs.
    b. Ensure integrity of the data.
    c. Ensure that media is kept in a secure manner.
    d. Files are up to date and have internal and external file headers.

23. During the IS audit of a small company the IS auditor noticed that there was inadequate separation of duties because the programmer could launch a program into the live environment without approval. In such cases the IS should recommend which of the following?
    a. Immediate termination of the employee.
    b. Background checking,
    c. Development of the software by a CMM level 5 company.
    d. Monitoring and review of the programmer's activities.

24. The most cost effective and quickest way by which the management can effect continual improvement in existing IS processes, is by:
    a. Engaging temporary outsourced IS auditors.
    b. Performing a root cause analysis and taking appropriate corrective action.
    c. Creating a long term plan for business process reengineering.
    d. Planning for certification of their processes against ISO 9001.

25. In a computer-based information system, separation of duties:
    a. Can always be attained in the same way as in a manual system.
    b. Might have to be implemented in different forms compared with manual systems.
    c. Is less important than in a manual system because programs make fewer errors than clerks.
    d. Usually is easy to automate, especially in microcomputer systems.

26. Which of the following is most likely to be a characteristic of an information systems operational plan?
    a. Focuses on the next five years of information systems activities.
    b. Explains how proposed application systems will enhance the competitive advantage of the organization.
    c. Identifies the major milestones in the development of major application systems.
    d. Assesses the strengths and weaknesses of the current hardware/software platform.

27. Which of the following statements is false in connection with planning?
    a. It involves deciding in advance what should be done amongst other things.
    b. It is an action statement.
    c. It should be entrusted to the IS steering committee only.
    d. It is the best practice applicable to the private sector only.

28. Which of the following statements is false in connection with the IS steering committee?

a. It oversees the IS activities.
b. It should be chaired by a non-technical board member.
c. It should have representation by user management.
d. Its meetings should be minuted.

29. The inputs for effective planning include which of the following?
    a. Defining customer and stakeholder needs.
    b. Resource needs,
    c. Performance metrics,
    d. Determining improvement methods.

30. Long range planning does not deal with which of the following?
    a. Assessment of current IS resources.
    b. Actions to be taken in the remaining part of the year.
    c. Future IS resource needs,
    d. Methods to bridge the gap between present and future IS resource needs.

31. Leadership qualities include:
    a. Planning and organizing,
    b. Motivating and controlling,
    c. Both A and B,
    d. Neither A nor B.

32. Which of the following statements is false?
    a. Policies are documented processes which can be verified, validated and approved.
    b. Systems are a set of inter-related processes.
    c. Processes are a set of inter-related activities which transform inputs to outputs.
    d. Work instructions are detailed steps to perform an activity.

33. Which of the following statements is false?
    a. The objective of benchmarking is to implement industry's best practices.
    b. Benchmarking is used to compare internal performance with others having comparable IS environments.
    c. IS budgets are an instrument of control.
    d. An internal agreement for provision of the IS services between end users and the IS department is known as an SLA.

34. Which of the following is not a management principle of ISO 9001:2000?
    a. Customer focus,
    b. Leadership,
    c. Involvement of people,

d. Continuous improvement.

35. Which of the following is a preventive control in ensuring that the staff has the required capabilities for their job?
    a. Vacation and overtime rules,
    b. Performance appraisals,
    c. Promotion policies,
    d. Training.

36. Which of the following is a disadvantage of cross-training?
    a. It allows a person to understand all the processes for which he has been trained.
    b. It decreases the dependence on one staff member.
    c. It provides a short-term backup for an absent employee.
    d. It can be used for succession planning.

37. The role of the chief information officer (CIO) is not:
    a. To work with senior management to define strategic systems.
    b. To support business managers in defining information needs.
    c. To develop computer systems that business managers need.
    d. To resolve systems software problems.

38. The ISO 9000 series of standards focuses on which of the following areas?
    a. Products,
    b. Processes,
    c. Materials,
    d. Vendors.

39. The proper organizational position of the IS security function is reporting to :
    a. The corporate security department,
    b. A person one level below the CIO,
    c. The internal auditing department,
    d. The CIO or higher.

40. All of the following are duties of the IS security administrators except:
    a. Creating new system user accounts.
    b. Issuing new passwords.
    c. Implementing new security software.
    d. Approving new system user accounts.

41. An out of date IS security policy:
    a. Leads to misunderstanding between security staff.
    b. Leads to poor coordination among business units.

c. Fails to address significant risks.
d. Leads to inappropriate use of controls.

42. An IT operational plan answers all of the following questions except:
    a. How do we get there?
    b. When will it be done?
    c. What is our goal?
    d. Who will do it?

43. An IT operational plan does not include _____.
    a. Risk assessment,
    b. Project descriptions,
    c. Project resource estimates,
    d. Project implementation schedules.

44. Which of the following are compatible functions within the IS organization?
    a. Systems analysis and application programming,
    b. Telecommunications network and computer operations,
    c. Applications programming and systems programming,
    d. Data entry and production job scheduling.

45. Which of the following organizational and IT structures are conducive to staying competitive and responsive in the global economy?
    a. Flatter organizational structure, decentralized support, distributed decision making, loosely coupled systems, and loosely coupled teams.
    b. Taller organizational structure, centralized support, decentralized decision making, tightly coupled systems, and tightly coupled teams.
    c. Taller organizational structure, decentralized support, centralized decision making, loosely coupled systems, and loosely coupled teams.
    d. Flatter organizational structure, centralized support, distributed decision making, tightly coupled systems, and loosely coupled teams.

46. Which of the following is not a database administrator's responsibility?
    a. Establishing data usage and database usage standards.
    b. Recovering databases.
    c. Reorganizing databases.
    d. Maintaining databases.

47. The objective of separation of duties is that:
    a. No one person has complete control over a transaction or an activity from start to finish.
    b. Employees from different departments do not work together.
    c. Controls are available to protect all supplies.

d. Controls are in place to operate all equipment.

48. A data/tape librarian should not be responsible for:
    a. Record-keeping of tape and cartridge activity.
    b. Taking periodic inventory of tapes and cartridges.
    c. Logging movement of magnetic media.
    d. Operating the computer.

49. Planning is the:
    a. Formulation of future courses of action, which gives purpose and direction to the organization.
    b. Choosing among alternative courses of action.
    c. Formulation of the division of labour and the allocation of responsibility and authority through the organization.
    d. Analysis of deviations from past strategies when formulating new strategies.

50. In developing a data security program for an organization, who should be responsible for defining security levels and access profiles for each data element stored in the computer system?
    a. The database administrator,
    b. The systems programmer,
    c. The owner of the data,
    d. The applications programmer.

51. The activity most essential to computer capacity planning is:
    a. Scheduling of documents,
    b. Planning of room layout,
    c. Workload forecasting,
    d. Estimating electrical load.

52. Which among the following combinations of roles has maximum risk?
    a. Data entry and Operations,
    b. Librarian and Help desk,
    c. Systems Analysis and Quality assurance,
    d. Database Administration and Data entry.

53. Which maturity level of CMM is characterized by:
    "Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies."
    a. Level 5,
    b. Level 4,
    c. Level 3,
    d. Level 2.

54. In a small organization, where segregation of duties is not practical, an employee performs the functions of computer operator and application programmer. Which of the following controls should the IS auditor recommend?
    a. Automated logging of changes to development libraries.
    b. Additional staff to provide segregation of duties.
    c. Procedures that verify that only approved program changes are implemented.
    d. Access controls to prevent the operator from making program modifications.

55. Which of the following is most likely to be performed by the security administrator?
    a. Approving the security policy.
    b. Testing application software.
    c. Ensuring data integrity.
    d. Maintaining access rules.

56. Which of the following best describes an IS department's strategic planning process?
    a. The IS department will have either short–range or long–range plans depending on the organization's broader plans and objectives.
    b. The IS department's strategic plan must be time– and project– oriented, but not so detailed as to address and help determine priorities to meet business needs.
    c. Long–range planning for the IS department should recognize organizational goals, technological advances and regulatory requirements.
    d. Short–range planning for the IS department does not need to be integrated into the short–range plans of the organization, since technological advances will drive the IS department plans much quicker than organizational plans.

57. The key objective of capacity planning procedures is to ensure that:
    a. Available resources are fully utilized.
    b. New resources will be added for new applications in a timely manner.
    c. Available resources are used efficiently and effectively.
    d. Utilization of resources does not drop below 85 percent.

58. Which of the following activities performed by a database administrator (DBA) should be performed by a different person?
    a. Deleting database activity logs.
    b. Implementing database organization tools.
    c. Monitoring database usage.
    d. Defining backup and recovery procedures.

59. An IS auditor is auditing the controls relating to employee termination. Which of the following is the most important aspect to be reviewed?
    a. The related company staffs are notified about the termination.
    b. User ID and passwords of the employee have been deleted.
    c. The details of employee have been removed from active payroll files.
    d. Company property provided to the employee has been returned.

Answers:

1. d	2. c	3. a	4. d	5. d	6. a	7. b	8. a
9. b	10. b	11. a	12. d	13. a	14. b	15. b	16. d
17. d	18. d	19. d	20. a	21. c	22. b	23. d	24. b
25. b	26. c	27. d	28. b	29. a	30. b	31. c	32. a
33. d	34. d	35. d	36. a	37. d	38. b	39. d	40. d
41. c	42. c	43. a	44. a	45. d	46. a	47. a	48. d
49. a	50. c	51. c	52. d	53. a	54. c	55. d	56. c
57. c	58. a	59. b					

Glossary of Terms

AICPA

American Institute of Certified Public Accountants.

Applications

They are computerised or manual user systems and procedures that process the data and information for a specific user task.

Application Systems Analysts

They are responsible for designing application systems based on user needs, resulting in the development of user needs, functional specifications and other high level systems design documents required by the application programmers.

Application Systems Development Manager (ASDM)

The ASDM is responsible for overseeing the work of (a) application systems analysts and (b) application programmers, who design, develop and maintain new or existing application programs.

Application Systems Programmers (ASP)

Their role is to develop new application systems and maintain the existing production systems based on the design made by the application systems analysts.

BPO

Business Process Outsourcing. See Outsourcing also.

Benchmarks

A set of metrics designed to compare the performance of the organization with those organizations having comparable IS environments.

CIO, Chief Information Officer

The person who is in overall charge of the information systems management function.

Capability Maturity Model

A model developed by The Software Engineering Institute of Carnegie Mellon University in 1986, in order to establish standards for excellence in software engineering and to enable the use of advanced technologies into practice.

Capacity management

The process of planning, sizing and continuously optimising the IS capacity in order to meet long and short term business goals in a cost effective and timely manner.

Certification

The process of certifying an organization, by an accredited institution, for compliance with the requirements of an ISO or other standard.

Compensating controls

Compensating controls are internal controls which reduce the risk caused by an existing or potential control weakness where the duties cannot be separated.

Computer Operators

They are responsible for scheduling and allied activities in order to run the computer system effectively and efficiently.

Co-sourcing

A variant of outsourcing, which is normally done in human resource outsourcing, where the client is responsible for the management of outsourced activities, while the vendor provides consultancy services and experienced personnel when needed by the client organization.

Critical Success Factors

The most important actions that the management should take, whether strategic, technical, organizational or procedural, in order to control its IT processes.

For example:

- Defined and documented plans, processes and policies,
- Clear accountability in functions,
- Strong commitment of management,
- Proper communication to stakeholders,
- Consistent measurement practices.

Cross training

An internal control, which enables more than one person to perform the job duties of another employee.

Data

Raw facts, figures or observations which are not organized to convey any meaning.

Data Administrator (DA)

The DA is responsible for the long term planning of the data architecture and management of data. It is basically a policy making and administrative role.

Data entry operators

They are responsible for entering the data into the computer. Data entry can be performed in batch (offline) or online mode. In the modern environments, this function is performed by the user departments.

Data security

The controls encompassing, confidentiality, integrity, availability, along with authenticity, accountability, non-repudiation and reliability, with respect to the data.

Database Administrator (DBA)

The DBA performs a technical role, and is responsible for short term planning, design, definition, maintenance and integrity of the database systems in an organization.

Deming Cycle

See P-D-C-A.

e-Business

The process of buying and selling goods, services and information, using computer networks, particularly the Internet.

e-Commerce

See E-business.

e-Mail, Electronic mail

An application system which allows communication of messages by electronic methods between two parties using computers, instead of paper-based communication.

Encryption

A method of storing and transmitting the data in a form which can only be read by the intended recipient. This is done to protect the confidentiality and integrity of the data.

End User Support Manager

This function is responsible for the liaison between the end users and the IS department, including the management of the help desk, in order to resolve the users' hardware and software technical problems.

Exit practices

A set of internal controls which must define, in clear terms, the steps for employee job termination, whether voluntary or forced by the employer, in order to secure the IS assets.

Exit interview

An internal control involving an interview arranged with the leaving employee in order to gain insights regarding his reasons for leaving and his perception of the organization.

Goal Accomplishment processes

These are used in order to determine the effectiveness of a system by comparing actual performance with predefined business and IT goals.

Goal Indicators

A measure of what has to be achieved by the process goal, i.e. a target to be achieved.

Guidelines

These are codes of the best practices which clarify what and how things should be done, in order to achieve the objectives of the policy.

IEC

International Electrotechnical Commission.

Information security management (ISM)

ISM describes controls that an organization needs to implement to ensure that it is sensibly managing the risks of loss, misuse, disclosure or damage of information and information infrastructure assets.

Intellectual property rights (IPRs)

The term intellectual property means that the subject in question is a product of the intellect i.e. mind. IPRs are an umbrella term for many legal entitlements relating to names (e.g. domain names, copyrights, patents, trademarks), written (e.g. books, articles etc.) and recorded media (e.g. films and songs), and inventions (e.g. industrial design rights, trade secrets) etc.

Efforts are being made to harmonise IPR laws through international treaties like the 1994 World Trade Organization Agreement on Trade-Related aspects of IPRs (TRIPs).

ITU

International Telecommunication Union.

Industry Standards

See benchmarks.

Information

Data which has been processed, organized, stored, analysed, compared, calculated and generally worked on to produce understandable messages in the form required by the user.

Internet

A massive network of electronic and telecommunications, which connects the computers of organizations spread across the world, which permits the exchange of information using communication standards and protocols.

IS Department

The information systems department, which encompasses manual as well as automated systems.

ISO

International Organization for Standardisation, an organization based in Geneva.

ISO 216

The ISO standard for paper sizes.

ISO 838

The ISO standard for punching filing holes into paper.

ISO 2108

The ISO standard for International Standard Book Numbering (ISBN).

ISO 9899

The ISO standard for C programming language.

ISO 7810

The ISO standard for physical characteristics of identification cards.

ISO 7816

The ISO standard for integrated circuit identification cards.

ISO 15930

The ISO standard for Portable Document Format (PDF).

ISO/IEC 10026

The ISO standard for Open Systems Interconnection (OSI).

ISO/IEC 11179

The ISO standard for Information Technology - Metadata registries (MDR).

ISO 14000

The ISO standard for Environmental Management Standards in production environments.

ISO 9000

The ISO standard which defines the terms used in the 9000 series dealing with Quality Management Systems.

ISO 9001

The ISO standard which deals with the requirements for Quality Management Systems.

ISO 9126

This is the international standard for the evaluation of quality of software products.

ISO/IEC 25001:2007

The ISO standard for Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) - Planning and management.

ISO/IEC 25030:2007

The ISO standard for Software engineering - Software product Quality Requirements and Evaluation (SQuaRE) – Quality requirements.

ISO 27001

The ISO standard which deals with the requirements for Information Security Management Systems.

IS Steering Committee

A committee appointed by the Board in order to oversee the IS department activities.

IT Infrastructure

The technology and facilities e.g. hardware, software, networks etc.

Job rotation

An internal control which enables the management to detect possible irregularities perpetrated by a staff member who has been transferred to another function or location.

Just-in-time (JIT) manufacturing

An approach to scheduling inventory systems that reduce, inventory in process, space and costs. It also improves workflow by scheduling the arrival of materials at an assembly or manufacturing station exactly when they are required, thus reducing inventory and idle production facilities.

Knowledge

Expertise and skills acquired by a person through experience or education.

Legacy systems

An existing computer system or application software which continues to be used because the organization does not want to replace or redesign it, and are often called "antiquated" systems.

Legal, regulatory and contractual requirements

These state the compliance requirements with laws, directives of trade or regulatory agencies and contracts.

Librarian

The librarian is the stock keeper of all data and program files kept on storage media like tapes and hard disks.

Line management

Line management normally deals with the daily routine functions which are not related to projects. Such structures are normally found in most organizations and typically have many layers of reporting.

Maintenance operators

Their main function is to ensure that the hardware is working properly.

Malcolm Baldrige National Quality Award

This award is governed by the Malcolm Baldrige National Quality Improvement Act of 1987, USA, and is supported by the Foundation for the Malcolm Baldrige National Quality Award established in 1987. It is in honour of Malcolm Baldrige, who served as U.S. Secretary of Commerce from 1981, until he died in an accident in 1987. It recognizes U.S. organizations in the business, health care, education, and non-profit sectors for performance excellence.

Management review

An internal control function performed by the management in order to identify consistency with and deviations from plans, or adequacies and inadequacies of management processes.

Master Plan

This is the main plan prepared by the Board of Directors to guide the organization towards its strategic and short-term objectives.

Mission

A statement which, defines the organization's business objectives and its approach to achieve those objectives.

NASSCOM

National Association of Software and Services Companies, an organization based in India.

Network Administrator

They are responsible for the entire network of the organization which may include LANs, WANs and wireless communication and voice networks.

Non-compete agreements

A term used in contract law in which a party e.g. a staff member, agrees not to undertake a similar trade or profession in competition against the other party e.g. the employer. In other words, it is an agreement not to compete with the employer on leaving, in order to prevent the possibility of using the knowledge gained from the employer to join a competitor or setup a competing business.

Operating Level Agreement (OLA)

An agreement between entities (parties/functions/associates/sister organizations) for the provision of the IS services between the end users and the IS department.

Operations manager

The operations manger is responsible for computer operators, librarians, data entry personnel, maintenance operators and for physical and data security of the department.

Outsourcing

A sourcing practice formalised in an agreement, in which part or all of an organization's IS functions are transferred to a third party for a fee and an agreed service level.

Out tasking

A variant of outsourcing, in which the responsibility of providing a particular service is given to multiple firms, instead of giving it to a single large organization.

PGP

A proprietary encryption system which stands for, Pretty Good Privacy.

P-D-C-A

Plan-Do-Check-Act, a quality model popularised by Dr. W. Edwards Deming.

People

They consist of internal, outsourced or contractual personnel required to plan, organize, acquire, deliver, implement, monitor, support, evaluate and improve the information systems and allied services.

Performance Indicators

These are metrics which determine how well the process is performing in enabling the goals to be achieved.

Performance measurement

The process of generating metrics for all products and processes, financial measurement, benchmarking and external party evaluation, satisfaction of customers, internal staff and stakeholders, in order to ensure that they are achieving the desired results.

Plan

An action statement, decided in advance, in order to achieve the stated goals of the organization.

Policies

High level, static documents which define the overall management intent of an organization.

Practices

See process.

Procedures

Statements which provide detailed steps of the action that should be followed in order to perform a specific task.

Process

A group of interrelated or interacting activities, which transforms inputs into outputs.

Project Management

The processes utilised in order to manage any business project throughout its life cycle from inception to usage. Projects are, usually, a one time effort consisting of many interrelated activities lasting from a few weeks to years. It may employ project management tools like PERT and CPM for optimal scheduling and sequencing of activities.

Quality Assurance Manager

This function deals with assuring adherence to prescribed quality processes in all IT related functions like programming, data entry etc.

Quality Control Manager

This function deals e.g. with conducting tests in order to verify and ensure that the software and other allied processes are free from defects before they are transferred to the live operations and that it meets the needs and expectations of the end users.

Quality Management processes

The processes and activities considered necessary in order to plan, develop, monitor and improve a product or service, in an effective and efficient manner in order to meet stated requirements.

RSA

A proprietary encryption system which is considered to be a de-facto encryption standard, devised by Rivest, Shamir and Adleman.

SAS 70

Statement on Auditing Standards No. 70: Service Organizations, is an auditing statement issued by the Auditing Standards Board of AICPA, officially titled "Reports on the Processing of Transactions by Service Organizations". It defines the standards used by a service auditor in order to assess the internal controls of a service organization and issue a service auditor's report, which can be of two types:

- **Type I** reports include the auditor's opinion on the fairness of the service organization's internal controls at a specific point in time and the suitability of the controls in order to achieve the control objectives.
- **Type II** service reports include the information contained in the Type I service auditor's report and the auditor's opinion on whether the controls were operating effectively during the period under review.

SLAs, Service level Agreements

Are that part of a service contract where the level of service expected from the service provider is formally defined.

Scheduling & Time reporting

These are both internal controls.

- Scheduling enables the effective use of the IS resources, while time reporting enables the scheduling process to be monitored by the management.
- They both ensure that operations are performing efficiently and also assist in determining staff levels required.

Separation of Duties

The main purpose of separation of duties is to prevent or detect errors or irregularities by applying suitable controls such that the job of one person is checked by another.

Security manager

A person who is responsible for ensuring compliance with the security policies of the organization.

Six Sigma

A quality management system developed by Motorola in 1986, in order to improve processes by eliminating defect levels below 3.4 defects per one million opportunities. It has been successfully used by leading companies like General Electric.

Sourcing

The procurement practices of an organization, designed to find, evaluate and engage suppliers of goods and services.

SSE - CMM

Systems Security Engineering Capability Maturity Model, which focuses on security engineering process areas.

Standards

Documents which state management rules, legal and regulatory issues, that are mandatory.

Steering Committee

A committee appointed by the top management in order to oversee the IS department's processes, from a strategic and short term point of view.

Strategic Plans

The long range plans of an organization.

SW-CMMI

The latest version of the original CMM model which stands for, Software Capability Maturity Model Integration.

SWOT Analysis

A technique used in setting objectives in order to determine the strengths, weaknesses, opportunities and threats, faced by an organization, while setting its objectives.

System

A set of interrelated or interacting processes.

Systems Administrator

Where large organizations have LANs spread over many geographical locations, each LAN will require a systems administrator for technical and administrative control of the LAN.

Systems Analyst

They are responsible for designing systems software.

Systems Programmer

Systems programmers are responsible for developing and maintaining the systems software designed by the systems analyst.

Tactical Plans

The short range or operational plans of an organization.

Technical support manager

This function is responsible for overseeing the following technical support functions:

- Systems Analyst,
- Systems Programmer,
- Systems Administrator,
- Network Administrator,
- End User Support Manager.

Transfer Prices

An internal organizational scheme in which IT costs are charged back to the user departments.

User Pays Scheme

See transfer prices.

User satisfaction survey processes

A method of determining the effectiveness of the IS department after the users and the IS department have agreed on a SLA or OLA.

Validation

Validation means that the procedures can be checked at a high level as being right or

wrong against objective criteria like a standard or rules. E.g. data validation is the process of ensuring that, say, input data complies with predetermined formats, character length requirements etc. In other words it answers the question, "Did we build the right product required by the user?

Values

A statement which describes, the ethics employed by an organization in order to achieve its objectives.

Verification

This means that the procedures used can be checked objectively at a low level as being accurate and complete. It answers the question "Have we built the product right in accordance with specifications?

Vision

A statement which details, the desired future position of the organization.

Website

A set of web pages, images, videos and other digital content that is hosted on one or many web servers, which are usually accessible through the Internet, mobile phone, personal digital assistants (PDAs) or a LAN.

Sources:

1. James A. O'Brien, Managing IT in the Business Enterprise
2. ISACA,CISA 2002 Review Manual
3. ISACA,CISA Review Manual 2007
4. T. Lucey, CISA Examination Textbooks Volume 2: Practice 3rd Edition
5. J.A.F. Stoner, R.E Freeman, D.R. Gilbert, Management Information Systems
6. Ron Weber, Information Systems Control and Audit
7. D.P. Dube and V.P. Gulati,Information System Audit and Assurance
8. R.L. Krutz & R.D. Vines, The CISSP Prep Guide
9. Robert Slater,Jack Welch on Leadership
10. Peter F. Drucker, People and performance
11. Accenture, High Performance Work Force Study 2007,Times of India, 16th August 2007
12. ISO 9004
13. http://en.wikipedia.org
14. http://en.wikipedia.org/wiki/PDCA
15. http://www.bizmanualz.com/pdf/samples
16. http://sas.sei.cmu.edu

17. http://www.kulzick.com/isstcom.htm
18. http://en.wikipedia.org/wiki/Capacity_management
19. http://en.wikipedia.org/wiki/ISO_9126
20. http://en.wikipedia.org/wiki/Capability_Maturity_Model_Integration
21. http://www.campus.manchester.ac.uk/ssc/pastpapers/2006/Sem%201/informatics%20jan%20%2006/H53015(SoftQual)-2006.pdf
22. http://en.wikipedia.org/wiki/Information_security_management

3 Auditing Information Systems Organisation & Management

Learning Goals / Objectives

The key objectives of this chapter is to ensure that the auditor can apply a systematic approach to auditing the IS Organisation & Management Process by using an auditing checklist in order to ensure that all the audit areas are covered.

At the end of this chapter, the auditor candidate should be able to:

- Understand what is a checklist and its attendant advantages and disadvantages.
- Prepare a suitable checklist for the areas to be covered based on the suggested checklist given in this chapter which can be correlated with the P-D-C-A cycle.

Note: The suggested checklist is not meant to be a comprehensive list of the activities to be audited by the auditor. It is only meant to give the auditor a base from which tailor made questionnaires and audit programme checklists can be designed for each organisation.

Introduction

This chapter introduces the reader to understand the objective of an IS audit and compile a checklist or audit programme based on the area being audited. It invites the auditor to ask certain generic questions in order to collect the required evidence based on which the audit will evaluate the effectiveness of the area under audit.

For ease of comprehension, a suggestive checklist has been compiled based on the PDCA cycle outlined in the previous chapter. Readers are requested to use the suggestive checklist as a reference model only.

Checklists / Audit Programmes

Auditors should constantly be aware of the purpose of the audit, which in this case may be:

'To collect sufficient, reliable and relevant audit evidence in order to make an informed evaluation or judgement about the status of the information system organisation and related processes'.

In order to achieve the above objectives, the IS auditor may require the preparation of an audit checklist in order to ensure appropriate continuity and depth of the audit as well as save time. The checklist may in turn determine the sample of the evidence to be collected. The checklist is basically an aide-memoire and should not be a collection of Yes/No tick lists.

The checklist should lead the auditor to ask the following questions:

- Who
- What
- When
- Where
- Why
- How
- Show me
- Tell me

Advantages / Benefits

- Determines the sample relevant to the audit.
- Formalises the audit process by defining the audit procedures.
- Creating the checklist requires some amount of research which helps in the auditor's understanding of the processes.
- Helps in maintaining the pace of the audit.
- Assists in keeping the audit objectives clear.
- Acts as a historical record which can be used as an internal cross reference to the audit report.
- Reduces the auditor's workload.
- Assures a degree of auditor professionalism.
- Ensures that the auditor is aware of the processes to be audited.

Disadvantages

- May become a tick list of YES/NO answers only.
- If the process is not in the checklist, it may not be covered during the audit.
- It may reduce initiative and proper analysis of the processes.

Suggestive Audit Checklist for auditing information systems organisation and management.

Interview the following people in the context of the **P-D-C-A** cycle:

- Senior management e.g. the CEO, COO, CFO and CIO- **P, C,A**
- IS planning and steering committee members- **P, C,A**
- IS senior management and human resources staff – **P,D**
- Security officer – **P,C**
- Assurance managers – **P, C**
- Human resources manager & people – **D**
- Project owners / sponsors – **D**
- Contractors – **D**
- Selected users – **D, C, A**

Collect the following documents and records:

- Planning process related policies, standards, policies, information architecture etc - **P**
- Roles and responsibilities of steering committee management – **P, C**
- Strategic and tactical goals for the organisation and IS – **P**
- Minutes of steering committee members – **P, C**
- Technological infrastructure plan – **P**
- Quality assurance policies – **P**
- Communications programme – **P**
- Personnel policies, job descriptions, personnel files, training records – **D**
- IT contracts for acquisition of hardware, software and services – **D**
- Vendor documentation – **D**
- Organisational charts – **D**
- Capacity planning reports - **D**
- IT budgets and chargeback reports – **D**
- Help Desk processes – **D**
- Appropriate activity logs and process measurements – **C, A**
- Assurance reports **– C, A**
- User and customer satisfaction surveys – **C, A**
- Benchmarks – **C, A**
- Self assessment and management review exercises **- A**

Module - V

Name of organization	
Period under review	
Subject under review	Management Planning & Organisation of Information Systems
Prepared By (Name)	(Date)
Reviewed By (Name)	(Date)

Domain- Plan	Yes	No	N/A	Comments	Ref.
1. Is there a structured methodology for planning IT and business goals with respect to? e.g.: - Values. - Philosophy. - Management style. - IT awareness. - Organisation. - Policies. - Standards. - Legal, regulatory and contractual requirements					
2. Does the methodology cover all related areas? e.g.: - Organisations mission, goals and supporting IT initiatives - Opportunities for, feasibility studies and risk assessments of, IT initiatives. - Optimal investment of present and future IT investments. - Process re-engineering of IT initiatives in order to reflect the changes in the organisation's mission and goals. - Evaluation of any alternative					

strategies for applications, organisational changes, staff levels, sourcing practices, and technology evolution.					
3. Do IT plans exist, are current and linked with business goals?					
4. Do milestones exist in order to check the progress of IT and business plans?					
5. Have IT plans been reviewed and signed off by the process owners and senior management?					
6. Does IT plan assess the present information systems for appropriateness e.g.: - degree of automation - stability - functionality - complexity - strengths - weaknesses and - costs?					
7. Have plans been made to reflect any changing conditions?					
8. Have IT strategic plans been converted into tactical plans?					
9. Do tasks and adequate staffing levels exist in order to implement the plans?					
10. Is there a process to develop, and maintain an enterprise information architecture model based on plans?					
11. Does the technology plan address technology standards?					

12. Do the hardware and software acquisition plans link with the technology infrastructure plan and are approved?					
13. Have roles and responsibilities of steering committee members and other IS personnel been defined along with their authority and accountability?					
13. Does the charter for the steering committee address its link with business and IT goals?					
14. Are there processes to raise awareness, comprehension and skills required to resolve information management issues?					
15. Do policies exist to modify the organisational structure to meet changes in objectives and circumstances?					
1. Is there adequate **separation of duties** between? e.g. - systems development and maintenance - systems development and operations - systems development or maintenance and information security - operations and data control - operations and users - operations and information security - quality assurance and systems development					
2. Do the implemented **HR**					

policies address? e.g. : a) Recruitment and selection criteria of the organisation and professional associations. b) Job competencies, skills, experience and personality. c) Training, awareness programs and career development. d) How to address gaps in job skills, etc. e) Cross training and job rotation. f) Forced vacations. g) Periodic performance evaluation. h) Exit procedures. i) Compliance with legal, regulatory and contractual commitments. j) Promotion, non-compete clause, bonding etc.					
3. Does the **quality assurance** function?: a) Have adequate and skilled staff. b) Assure that quality processes exist for projects before final approval. c) Promote a continual improvement philosophy. d) Have an appropriate link with the IT plans.					
e) Ensure a standard approach to all projects. f) Ensure adherence to prescribed standards, guidelines etc.					

g) Apply to systems that have been changed. h) Issue reports on time and which are followed up. i) Ensure that metrics are generated for all processes in order to determine whether goals have been achieved.					
4. Do IT management refer to the **enterprise data architecture model** before identifying new IT solutions?					
5. Have appropriate **contract controls** been implemented for hardware, software and services? e.g. a) Empanelment of vendors. b) Criteria for selection of vendors. c) Contract bidding. d) Contract acceptance. e) Contract maintenance. f) Software licensing. g) Testing for acceptance of products. h) Impact on existing systems e.g. impact on security of data. i) Legal clearance. j) Preventive maintenance. k) Escrow clauses. l) Due diligence reports etc.					
6. **SLA controls**: a) Are SLAs detailed enough to allow their tracking, reporting and any opportunities for improvement?					

b) Are SLAs identifiable with policies? c) Are users involved in SLA development and modification? d) Are SLA costs fair, based on history, industry and benchmarks? e) Do SLAs include e.g.: - Service definition. - Cost of service. - Service metrics. - Continuity planning. - Security requirements. - Agreement modification procedures. - Written improvements. - Effective period and renewal clause. - Contract termination. - Right to audit clause. - Frequency of performance reporting. - Payment methods. - NDAs. - Confidentiality. - Calculation of charges. - Resolution of problems. - Service improvement commitment by the vendor.					
7. Are the following **documents** developed and maintained e.g.: a) user procedure manuals. b) operations manual. c) training manuals.					

8. **Capacity management** controls: a) Do capacity plans exist and reflect user needs? b) Are performance monitoring reports issued for all IT resources in order to optimise performance and capacity? c) Are users involved in capacity, performance and workload reviews / forecasting?					
9. Are controls for **chargeback** of IT costs in place? e.g.: a) Involvement of users in : - the development and maintenance of annual budgets. - The determination of the direction in which the IT resources are spent. b) Consistency in allocating costs to users. c) User sign off on allocation of costs. d) Reports on external benchmarks. e) OLAs.					
10. Evaluate the following **Help Desk** controls for internal staff and customers e.g.: a) Are user requests processed and assistance provided? b) What are the roles and responsibilities of the persons responsible for the help desk?					

c) Are the help desk activities properly documented and maintained? d) How are user complaints logged and service provided? e) What are the escalation procedures in case a problem cannot be resolved on time? f) What are the procedures for tracking and reporting trends in their activities? g) Are service level provision standards being met e.g. turn around times (TATs)? h) Are user satisfaction reports being generated? i) Is the help desk adequately staffed?					
11. Are **library management** software or manual procedures used for? e.g.: a) Software labelling. b) Producing an audit trail of program changes. c) Inventory management of software. d) Maintaining version numbers. e) Maintaining creation, retention, purge, and destruction dates, in accordance with organisational and legal requirements. f) Maintaining copies of earlier versions in case of emergencies. g) Controlling simultaneous					

update of files.					
12. Are metrics generated for **scheduling and time reporting** in order to confirm the full completion of all requirements?					
13. Is **equipment maintenance** being performed on time and as per vendor requirements?					
1. Are the management supplied with the following information? e.g. a) Reports on: - Whether the outsourcing functions are meeting business needs. - Contract / SLA performance and problems for their review e.g. by the contract management team. - Penalties imposed for non-compliance. b) Threats and vulnerabilities not addressed before. c) Performance monitoring and benchmarking reports for comparison with SLAs and OLAs i.e. Key Performance Indicators (KPIs). d) Help Desk reports on trends analysis for performance improvement initiatives. e) User, vendor and customer satisfaction reports. f) Evaluation of configuration management reports. g) Reports on effectiveness of					

compliance with legislation and internal policies and standards. h) Monitoring reports on the processes carried out by the management other than internal audit e.g. - Metrics on IT security. - Equipment failure. - Control failure reports etc, by using: ~ scorecards. ~ external benchmarks. ~ internal assessments of resource utilisation etc. i) New training needs. j) Evaluation of Critical Success Factors and Key Goal Indicators. k) Follow up of reports.					
2. Do the management suggest or are involved in the following? : a) Establishment of independence assurance processes or contracts for accreditation or certification e.g. against ISO 9001, CCMI etc. b) Proactive seeking of new solutions, audit involvement, compliance with forthcoming legislation. c) Development of improvement programmes through more effective controls e.g. better operating procedure and training manuals. d) Updating the risk					

management plans. e) Identifying new information for future planning needs. f) Modification of resource needs. g) Meeting legal, regulatory and contractual requirements.					
1. Are the management involved in effective implementation of? e.g. a) Performing root cause analysis. b) Determining the best corrective action required. c) Recording the results of action taken. d) Review of the action taken reports					

Summary

Auditing Information System Organization and Management includes the basic objectives of the IS audit and suggestive checklist programme based on auditing in computerised environment by the auditor. Before preparing the checklist, auditor should gain good understanding of the management as well as the organization behaviour. The auditor should ascertain that necessary evidence has been collected and based on the evidence, questions has been framed. It is suggested that the auditor should create their own checklists which should be tailored for the organisation being audited based on PDCA cycle.

Glossary of Terms

N/A = *Not applicable*
Ref. = *Reference to audit working papers*
SLAs = *Service Level Agreements*
OLAs= *Operating Level Agreements*

Reference Sources

1. *Cobit*
2. *The IIA, GTAG series*

Module – VI

IS Audit Process

1 IS Audit Process

Learning Objectives

- To gain an understanding of fundamentals for Establishing an IS Audit Function, Viz. Audit Mission, Audit Charter, infrastructure , reporting, staffing and organisation of IS audit function,
- To understand how an IS Audit is planned and carried out, viz. IS Audit Strategy, Phases in Information Systems Audit, Planning an IS audit, Use of Sampling in Information Systems Audits, Documentation Requirements , Evidence Collection, Reporting and Follow Up,
- To gain knowledge of Internal and External audit control framework, quality assessment, IS audit requirements, preliminary review, legal considerations and audit standards.

Introduction

The role of information System audit has become a critical mechanism for ensuring the integrity of information and the reporting of organization finances to avoid and hopefully prevent future financial fiascos such as Satyam in recent years. Electronic infrastructure and commerce are integrated in business process around the globe. There is a need to control and audit using IS to avoid such kind of scam in near future. IS auditing formerly known as electronic data processing [EDP], computer information systems , and IT auditing evolved as an extension of traditional auditing.

Traditionally, audits were mainly associated with gaining information about financial systems and the financial records of a company or a business. However, recent auditing has begun to include other information about the system, such as information about environmental performance. In financial accounting, an audit is an independent assessment of the fairness by which a company's financial statements are presented by its management. It is performed by competent, independent and objective person(s) known as auditors or accountants, who then issue an auditor's report based on the results of the audit. The IS audit compraises of several areas covering internal control practices, Management of IS , behavioral sciences, Statistical and mathematical models and computer science which contributes knowledge about control concepts, discipline, theory, and the formal models that

underlie hardware and software design as a basis for maintaining data Validity, reliability, and integrity.

IS auditing is an integral part of the audit function because it supports the auditor's judgment on the quality of the information processed by computer systems. Initially, auditor with IT audit skills are viewed as the technological resource for the audit staff. The IS auditor's role has evolved to provide assurance that adequate and appropriate controls are in place. The audit's primary role, except in areas of management advisory services, is to provide a statement of assurance as to whether adequate and reliable internal controls are in place and are operating in an efficient and effective manner. Therefore, whereas the management is to ensure, auditors are to assure.

Audits are performed to ascertain the validity and reliability of information; also to provide an assessment of a system's internal control. The goal of an audit is to express an opinion on the person/organization/system (etc) in question, under evaluation based on work done on a test basis. Due to practical constraints, an audit seeks to provide only *reasonable assurance* that the statements are free from material error. Hence, statistical sampling is often adopted in audits. In the case of financial audits, a set of financial statements are said to be true and fair when they are free of material misstatements - a concept influenced by both quantitative and qualitative factors.

Such systems must adhere to generally accepted standards set by governing bodies regulating businesses; these standards simply provide assurance for third parties or external users that such statements present a company's financial condition and results of operations 'fairly'.

What is IS Audit ?

An **information technology audit**, or **information systems audit**, is an examination of the controls within an Information technology (IT) infrastructure. An IS audit is the process of collecting and evaluating the evidence of an organization's information systems, practices, and operations. The evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively and efficiently to achieve the organization's goals or objectives. These reviews may be performed in conjunction with a financial statement audit, internal audit, or other form of attestation engagement.

IT audits are also known as automated data processing (ADP) audits and computer audits. They were formerly called electronic data processing (EDP) audits.

An IS audit should not be confused with a financial statement audit. While there may be some abstract similarities, a financial audit's primary purpose is to evaluate

whether an organization is adhering to standard accounting practices. The primary functions of an IS audit are to evaluate the system's efficiency and security protocols, in particular, to evaluate the organization's ability to protect its information assets and properly dispense information to authorized parties. The IT audit's agenda may be summarized by the following questions:

- Will the organization's computer systems be available for the business at all times when required? (*Availability*)
- Will the information in the systems be disclosed only to authorized users? (*Confidentiality*)
- Will the information provided by the system always be accurate, reliable, and timely? (*Integrity*)

The IS audit focuses on determining the risks that are relevant to information assets, and in assessing controls in order to reduce or mitigate these risks. By implementing controls, the effect of risks can be minimized, but cannot completely eliminate all risks.

In other sense the IS audit is " the process of collecting and evaluating evidence to determine whether a computer system has been designed to maintain data integrity, safeguard assets, allows organisational goals to be achieved effectively and uses resources efficiently".

An audit, whether it be financial audit, operational audit, internal audit or the IS audit, requires an independent and competent professional to objectively obtain and evaluate evidence to

a. Evaluate the management’s assertions as regards the audit subject and/or
b. Opine with regard to the stated audit objectives.

The fundamental principles of audit do not change with change in the audit subject, however, the perspective of audit and the methods, tools and techniques to achieve the audit objectives do undergo a change. As in a financial audit, audit focus is on the risk arising from inadequate or inefficient controls on recording of transactions which could result in misstatement of financial statements. In an Information Systems Audit the focus is on the risks arising from the use of information technology in carrying out business processes.

Information Systems Audit Strategy

Information Systems Audit is often misunderstood as a mere technical audit and a domain of Information Technology professionals. On the contrary, Information Systems Audit involves evaluating the adequacy and efficiency of internal controls in business processes that are either partly or fully computerized. Hence, Audit and

control professionals who have expertise in understanding of business processes and internal controls with exposure to information technology risks and controls are considered the most appropriate professionals to conduct information systems audits.

An Information Systems Audit cannot be viewed from a narrow perspective of audit of only automated information processing systems but would include the audit of non-automated processes and interfaces also.

Therefore, depending on the audit environment, objectives and scope, the audit could involve the audit of entire business processes, partially or fully automated, or audit of specified application, technology and related controls.

The audit strategy would also be influenced by a range of factors, some of which include:

Audit Objective: The entire audit program and methodology depends upon the audit objective and scope. The objective of the IS audit is to evaluate an auditee's computerized information system(CIS) in order to ascertain whether the CIS produces timely, accurate, complete and reliable information outputs as well as ensuring confidentiality, integrity, availability and reliability of the data. The main objective of the IS audit can be

- Ensuring Information Security (Confidentiality, Integrity & Availability) or
- Ensuring Compliance to a particular standard, law or regulation e.g. RBI Regulations, CERT-In Guidelines, SOX compliance, BASEL II Compliance etc. or
- Ensuring efficiency of Information Systems e.g. performance audits, stress or volume testing or
- Ensuring that the changes or additions in the information systems did not affect the functions that were previously functioning flawlessly i.e. Regression Audit.
- Obtaining certification like SAS 70, ISO27001 or
- Technology Service Provider (TSP) audits i.e. audit of a third party (vendors, service providers, BPOs) on behalf of and with respect to the security policy of the client organization before or as a condition of outsourcing of a business process or

Audit environment: The following factors, which constitute the audit environment, also have a significant bearing on audit strategy:

- Nature and Complexity of business
- Extent of automation

- Risk Profile of the business
- Technology environment and its complexity
- The level of competence of the Top management and IT Management.
- Degree of controls.

For example, the audit strategy for a business of trading in securities which involves a high transaction risk would be further impacted from the extent of automation. The securities broking firm could be connected to the Stock Exchange and Depositories Systems, whereby, significant risks mitigation controls would be believed to be taken care of by virtue of technological connection with the Stock Exchange and Depositories Systems.

In the same manner the audit strategy for a CBS branch and a Non-CBS branch of same bank would be different as in case of a CBS branch application controls which otherwise would have been an important aspect of audit and would be believed to be taken care by the Central Office.

Fundamentals for Establishing an IS Audit Function

Establishing an IS audit function may be critical in organisations that are specifically dependent on Information Technology. The IS audit function could be established either within the organisation as an internal department or the function could be fully or partly outsourced to an external agency. In either case there are certain fundamental principles that should be taken into consideration:

Audit Mission:

The mission statement defines the primary purpose of the audit function and provides an overview of the focus, priorities, values and principles that will measure audit decisions. It also outlines the value addition that will be provided and clarifies the purpose and meaning for the audit function.

IS audit function reviews the reliability and integrity of information, compliance with the policies and regulations, and the processes for safeguarding of assets, as well as to make suggestions for improvements in operating efficiencies and internal controls. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. The audit mission statement may vary between various organisations and audit functions.

The mission of the audit function is to provide value added services in auditing and consulting by timely, effective and efficient processes, encompassing all key business processes of the enterprise so as to facilitate the achievement of business objectives.

Audit Charter:

The audit charter is a top level document in an organisation that defines the purpose of the audit function, responsibility, authority and reporting of the audit function.

A charter for the audit function should be established by the senior management of the organisation. This document should outline the responsibility, authority and accountability of the audit function. It should be reviewed periodically to assure that the independence, authority and accountability of the audit function are maintained.

The management should ensure that the auditors responsible for the review of the organisation's IT activities are technically competent and collectively possess the skills and knowledge necessary to perform such reviews in an effective, efficient and economical manner. The management should ensure that audit staff assigned to an IS audit is technically competent and participates in continuous professional education

The IS auditor should have a clear mandate to perform the audit. This mandate is generally documented in an audit charter and endorsed by the management. The audit charter should clearly address three aspects: responsibility, authority and accountability.

Responsibility

- Mission Statement
- Aims/Goals
- Scope
- Objectives
- Independence
- Relationship with External audit
- Auditee requirements
- Critical success factors
- Key performance Indicators
- Other measures of performance

Authority

- Risk Management

- Right of access to information, personnel, locations and systems relevant to the performance of audits
- Scope of limitations to scope
- Functions to be audited vs. auditee expectations
- Organisational structure, including reporting lines to the board and senior management
- Grading of the IS audit staff.

Accountability

- Reporting guidelines to senior management
- Assignment performance appraisals
- Personnel performance appraisals
- Staffing/career development
- Auditee's rights
- Independent quality reviews
- Assessment of compliance with standards
- Benchmarking performance and functions
- Assessment of completion of the audit plan
- Comparison of budget with actual costs
- Agreed actions, e.g. penalties when either party fails to carry out its responsibilities.

Communication with Auditees

Effective communication with auditees involves:

- Describing the service, scope, availability and timeliness of delivery.
- Providing cost estimates or budgets, if they are available.
- Describing problems and possible resolution.
- Providing adequate and readily accessible facilities for effective communication.
- Determining the relationship between the service offered and the needs of the auditee.

The audit charter should be the basis for communication with auditees and should include references to service level agreements on the following aspects:

- Availability for unplanned work
- Delivery of reports
- Costs

- Response to auditee complaints
- Quality of service
- Review of performance
- Communication with auditees
- Needs Assessment
- Control risk self assessment
- Agreement on terms of reference for audits
- Reporting process
- Agreement of findings.

Structure and Reporting of the IS audit function:

The IS audit function should be placed in the organisation so as to ensure its objectivity and independence. The appointment of external agency should also be governed by stipulations for independence and objectivity, which is the foundation for an effective audit function. The composition and constitution of the IS audit function should ideally be decided by the Audit Committee and should be the prime reporting pointer for the IS Audit function.

Infrastructure and organization:

The IS audit function should be equipped with sufficient resources to discharge its duties efficiently and effectively. An important determinant in the quality of the IS audit function is the quality of human resource that staff the audit function. The skills and competence requirements should be clearly established as an IS Audit function should collectively posses the skills and knowledge necessary for performing an effective and professional audit. Even in cases where external agencies are engaged, the professional competence and skills of such agencies should be ensured. Continuing Professional Education should be incorporated as a part of the IS audit management plan.

The function might require special infrastructure for using CAATs. If so, availability of appropriate tools and infrastructure should be ensured.

Internal and External Audit Control Framework:

The Internal and External Audit control framework ensure the minimum quality of audits, which is important for the organisation to ensure setting in place an Audit Control Framework. Policies and procedures for risk assessment, planning, implementation and reporting should be established. The Audit contol framework assures the effectiveness and efficiency of operations, reliability of reporting and compliances with laws and regulations. The standards and professional

pronouncements should be strictly adhered to, which should be reflected in the organisation and operations of the audit function.Certain guidelines have been established to ensure the qalitative work under control environment.

Quality Assessment and Peer Reviews:

Quality Assessment ensures that the IS audit function is delivering in line with the best auditing practices and following the professional standards and pronouncements,.It also ensures that the IS Audit function should be subject to both internal and external quality assessments, peer reviews, certification and accreditation. Though the objective of the internal and external IS audit remains same, the scope and approach might vary. In case of an internal IS audit, the auditor reviews the internal control environment in detail whereas an external auditor takes an overall view of internal control environment and switches to substantive testing.

In case of external audit, engagement letter defines the objectives and scope of individual audit assignment.

Engagement Letter

Purpose

Engagement letters are often used for individual assignments or for setting the scope and objectives of a relationship between the external IS auditor and an organisation.

Content

The engagement letter should clearly address three aspects – responsibility, authority and accountability

Responsibility

- Scope
- Objectives
- Independence
- Risk Assessment
- Compliance audit requirements
- Specific Auditee requirements
- Requirements relating to maintenance of audit evidence and work papers
- Deliverables.

Authority

- Right of access to information, personnel, locations and systems relevant to the performance of the assignment

- Scope or any limitations to the scope
- Evidence of agreement to the terms and conditions of the engagement.

Accountability

- Intended recipients of reports
- Restrictions on distribution
- Auditee's rights
- Quality reviews
- Agreed completion dates
- Agreed budgets/fees if available

In addition, an engagement letter should also include

- Procedure for changes in the service level agreement, e.g. enhancing the scope of work
- Confidentiality clause or a non-disclosure agreement (NDA)
- Conflict of interest matters – like auditor should not be related to any technology vendor or directors etc.

Skills and Competence Requirements of an IS Auditor

The overall competence level required for an IS auditor depends on the nature, complexity and size of the IS audit engagement. The audit objective and scope would have a significant bearing on the skill and competence requirements of an IS auditor. However, a set of skills that is generally expected of an IS auditor included:

- Sound knowledge of business operations, practices and compliance requirements.
- Should ideally possess the requisite academic, professional and technical qualifications and certifications.
- A good grasp of Information Systems Risks and Controls.
- Knowledge of Information and related technology control framework.
- Knowledge of IT strategies, policy and procedure controls.
- Ability to understand the IT environment of the auditee.
- Good knowledge of Information Technology concepts and working knowledge, to the extent necessary for the engagement, including database, information technology architectures etc.
- Ability to understand systems design, development, implementation and project management concept.
- Understanding of technical and manual controls relating to Business Continuity.

- Good communication skills and the ability to highlight the business issues arising from IT risks.
- Good knowledge of Regulatory requirements and Laws relating to Information Technology controls and cyber crime.
- Good knowledge of Professional Standards and Best practices relating to IT controls and security.

The IS audit assignment begins by defining the scope and objectives. Based on this, the auditor should obtain a clear understanding of business operations, compliance requirements, technology deployed, organisation structure, related risks of technology deployment and system of internal controls. He could then adapt the standards and benchmark for the audit, develop an information model for collecting and evaluating evidence and execute the audit.

Phases in Information Systems Audit

Both conventional and Information Systems Auditing broadly follow the same procedures as regards the auditing process i.e. planning the audit, collecting and evaluating information, preparing audit report and follow-up. However, in Information Systems auditing the basic premise of the audit is to independently conduct an appraisal of the Risk Management as regards the risks to business arising from the use of IT.A detailed phases of the IS auditing has been explained in fig 1.1.

The broad phases in an IS audit would include:

1. **Audit Planning**
   One of the primary and important phases in an Information Systems Audit is planning which ensures that the audit is performed in an effective manner. Planning takes on more significance in case of Information Systems Audit since the audit risk in case of the IS audit are significantly impacted by inherent risks, hence for the audit effort to be successful, a good audit plan is a critical success factor.Planning developes the annual audit schedule and perform the individual audits.It includes budgets of time and costs, and state priorities according to organizational gols and policies.The objective of audit planning is to optimize the use of audit resources.

   As per ISA 300 on “Planning”:

   - Adequate planning of the audit work helps to ensure that appropriate attention is devoted to important areas of the audit, those potential problems are identified and that the work is completed expeditiously. Planning also assists in proper assignment of work to assistants and in coordination of the work done by other auditors and experts.

- The extent of planning will vary according to the size of the entity, the complexity of the audit and the auditor's experience with the entity and knowledge of the business.
- Obtaining knowledge of the business is an important part of planning the work. The auditor's knowledge of the business assists in the identification of events, transactions and practices which may have a material effect on the financial statements.
- The auditor may wish to discuss elements of the overall audit plan and certain audit procedures with the entity's audit committee, the management and staff to improve the effectiveness and efficiency of the audit and to coordinate audit procedures with work of the entity's personnel. The overall audit plan and the audit program; however, remain the auditor's responsibility.

The auditor should develop and document an overall audit plan describing the expected scope and conduct of the audit. While the record of the overall audit plan will need to be sufficiently detailed to guide the development of the audit program, its precise form and content will vary depending on the size of the entity, the complexity of the audit and the specific methodology and technology used by the auditor.

The audit should be guided by an overall audit plan and underlying audit program and methodology. Audit planning is often mistaken as a one time activity to be taken and completed in the beginning of the audit. While for all practical purposes, planning is a continuous activity which goes on throughout the entire audit cycle. Many times changes in conditions or circumstances or unexpected findings during the course of audit require changes in the audit procedures and methodology initially planned. Hence, an auditor is expected to modify the audit plan as warranted by the circumstances.

The documentation of the audit plan is also a critical requirement. All changes to the audit plan should follow a change in management procedure with every change being recorded with reason for change.

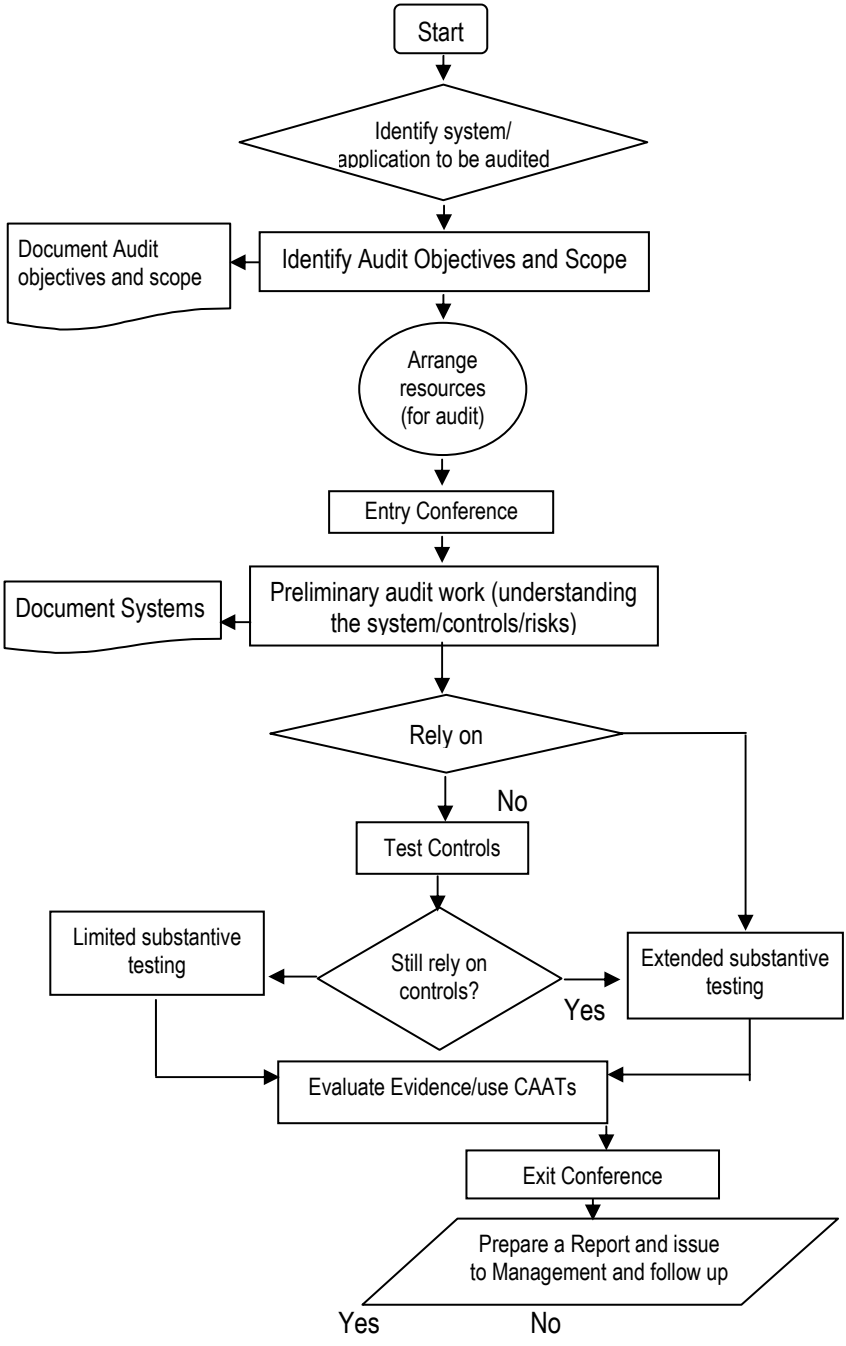


Fig 1.1 A Detailed Phase of the IS Audit

Preliminary Review

The extent of audit effort is dictated by the degree of audit risk, the assessment of which is critical to the effectiveness of the audit effort. Amongst the critical factors affecting the audit risk is the appropriate assessment of the control environment. The preliminary review of audit environment enables the auditor to gain understanding of the business, technology and control environment and also gain clarity on the objectives of the audit and scope of audit.

This phase of the audit allows the auditor to gather organizational information as a basis for creating their audit plan. The preliminary review will identify an organization's strategy and responsibilities for managing and controlling computer applications. An auditor can provide an in depth overview of an organization's accounting system to establish which applications are financially significant at this phase. Obtaining general data about the company, identifying financial application areas, and preparing an audit plan can achieve this.

The following are some of the critical factors which should be considered by an IS auditor as part of his preliminary review.

i. Knowledge of the Business

- General economic factors and industry conditions affecting the entity's business,
- Nature of Business, its products & services,
- General exposure to business,
- Its clientele, vendors and most importantly, strategic business partners/associates to whom critical processes have been outsourced,
- Level of competence of the Top management and IT Management,
- And finally, Set up and organization of IT department.

ii. Understanding the Technology

An important task for the auditor as a part of his preliminary evaluation is to gain a good understanding of the technology environment and related control issues. This could include consideration of the following:

- Analysis of business processes and level of automation,
- Assessing the extent of dependence of the enterprise on Information Technology to carry on its businesses i.e. Role of IT in the success and survival of business,
- Understanding technology architecture which could be quite diverse such as a distributed architecture or a centralized architecture or a hybrid architecture,

- Studying network diagrams to understand physical and logical network connectivity,
- Understanding extended enterprise architecture wherein the organisation systems connect seamlessly with other stakeholders such as vendors (SCM), customers(CRM), employees(ERM) and the government,
- Knowledge of various technologies and their advantages and limitations is a critical competence requirement for the auditor. For example, authentication risks relating to e-mail systems,
- And finally,Studying Information Technology policies, standards, guidelines and procedures.

iii. Understanding Internal Control Systems

- Gaining understanding of Internal Controls and decision on emphasis to be placed on compliance and substantive testing

iv. Legal Considerations and Audit Standards

- The auditor should carefully evaluate the legal as well as statutory implications on his audit work.
- The Information Systems audit work could be required as part of a statutory requirement in which case he should take into consideration the related stipulations, regulations and guidelines for conduct of his audit.
- The statutes or regulatory framework may impose stipulations as regards minimum set of control objectives to be achieved by the subject organisation. Sometimes, this may also include restrictions on the use of certain types of technologies e.g. strength of encryption systems.
- The IS Auditor should also consider the Audit Standards applicable to his conduct and performance of audit work. Non-compliance with the mandatory audit standards would not only impact on the violation of the code of professional ethics but also have an adverse impact on the auditor's work.

v. Risk Assessment and Materiality

Risk Assessment is a critical and inherent part of the Information Systems Auditor's planning and audit implementation. It implies the process of identifying the risk, assessing the risk, and taking steps to reduce the risk to an acceptable level, considering both the probability and the impact of occurrence. Risk assessment allows the auditor to determine the scope of the audit and assess the level of audit risk and error risk (the risk of errors occurring in the area being audited). Additionally, risk assessment will aid in planning decisions such as:

- The nature, extent, and timing of audit procedures.

- The areas or business functions to be audited.
- The amount of time and resources to be allocated to an audit

The steps that can be followed for a risk-based approach to making an audit plan are:

- Inventory the information systems in use in the organization and categorise them.
- Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
- Assess what risks affect these systems and the severity of the impact on the business.
- Based on the above assessment, decide the audit priority, resources, schedule and frequency.

Risks that affect a system and should be taken into consideration at the time of assessment can be differentiated as inherent risks, control risks and detection risks. These factors directly impact upon the extent of audit risk which can be defined as the risk that the information/financial report may contain material error that may go undetected during the course of the audit.

At this stage, the auditor needs to

- Assess the expected inherent, control and detection risk and identify significant audit areas.
- Set materiality levels for audit purposes.
- Assess the possibility of material vulnerabilities, including the experience of past periods, or fraud.

Assessing inherent, control and detection risk gives the final assessment of the overall Audit Risk i.e. the risk which the auditor is ready to accept in an audit assignment. Audit risk is the product of inherent risk, control risk and detection risk.

a. **Inherent Risk**

Inherent risk is the susceptibility of information resources or resources controlled by the information system to material theft, destruction, disclosure, unauthorized modification, or other impairment, assuming that there are no related internal controls. Inherent risk is the measure of auditor's assessment that there may or may not be material vulnerabilities or gaps in the audit subject exposing it to high risk before considering the effectiveness of internal controls. If the auditor concludes that there is a high likelihood of risk exposure, ignoring internal

controls, the auditor would conclude that the inherent risk is high. For example, inherent risk would be high in case of auditing internet banking in comparison to branch banking or inherent risk would be high if the audit subject is an off-site ATM in comparison to risk with an on-site ATM.

Internal controls are ignored in setting inherent risk because they are considered separately in the audit risk model as control risk. It is often an area of professional judgement on the part of an auditor.

b. **Control Risk**

Control risk is the risk that an error which could occur in an audit area, and which could be material, individually or in combination with other errors, will not be prevented or detected and corrected on a timely basis by the internal control system. Control risk is a measure of the auditor's assessment of the likelihood that risk exceeding a tolerable level and will not be prevented or detected by the client's internal control system. This assessment includes an assessment of whether a client's internal controls are effective for preventing or detecting gaps and the auditor's intention to make that assessment at a level below the maximum (100 percent) as a part of the audit plan.

c. **Detection risk**

Detection risk is the risk that the IT auditor's substantive procedures will not detect an error which could be material, individually or in combination with other errors. For example, the detection risk associated with identifying breaches of security in an application system is ordinarily high because logs for the whole period of the audit are not available at the time of the audit. The detection risk associated with identification of the lack of disaster recovery plans is ordinarily low since existence is easily verified.

In determining the level of substantive testing required, the IT auditor should consider both:

- The assessment of inherent risk.
- The conclusion reached on control risk following compliance testing.

Detection risk is a measure of the auditor's assessment of the likelihood that the vulnerability or gaps will be detected by the auditors. The Auditor will carry out more detailed audit to detect material vulnerabilities or gaps if the inherent risk and control risk are high.

Decision on Audit Risk and Materiality requires a thorough analysis of the audit subject, risk exposure, control environment and the circumstances and

conditions affecting the controlled environment. A prudent approach in determining the materiality and audit risk leads to successful audit planning.

In assessing materiality, the IT auditor should consider:

1. The aggregate level of error acceptable to the management, the IT auditor, and appropriate regulatory agencies.
2. The potential for the cumulative effect of small errors or weaknesses to become material.

While establishing materiality, the auditor may audit non-financial items such as physical access controls, logical access controls, and systems for personnel management, manufacturing control, design, quality control, and password generation.

While planning the audit work to meet the audit objectives, the auditor should identify relevant control objectives and determine, based on materiality, which controls should be examined. Internal control objectives are placed by the management and identifies what the management strives to achieve through their internal controls.

Where financial transactions are not processed, the following identifies some measures the auditor should consider when assessing materiality:

a. Criticality of the business processes supported by the system or operation.
b. Cost of the system or operation (hardware, software, third-party services).
c. Potential cost of errors.
d. Number of accesses/transactions/inquiries processed per period.
e. Penalties for the failure to comply with legal and contractual requirements.

Gather Information and Plan	
• Knowledge of business and industry • Prior year's audit results • Recent financial information	• Regulatory statutes • Inherent risk assessments
Obtain Understanding of Internal Control	
• Control environment • Control procedures • Detection risk assessment	• Control risk assessment • Equate total risk

Perform Compliance Tests	
• Identify key controls to be tested.	• Perform tests on reliability, risk prevention and adherence to organization policies and procedures.
Perform Substantive Tests	
• Analytical procedures • Detailed tests of account balances	• Other substantive audit procedures
Conclude the Audit	
• Create recommendations.	• Write audit report.

Fig. 1.2 -Risk-based Audit Approach

Audit Planning is a very important phase in an audit cycle. The most important deliverables of this phase would be:

Audit Program

Like any other audit, Information Systems Audit also follows a structured approach. The ISA 500 on "Planning" also requires the auditor to develop and document an audit program setting out the nature, timing and extent of planned audit procedures required to implement the overall audit plan.

The audit program serves as a set of instructions to assistants involved in the audit and as a means to control and record the proper execution of the work. The audit program may also contain the audit objectives for each area and a time budget in which hours are budgeted for the various audit areas or procedures.

In preparing the audit program, the auditor would consider the specific assessments of inherent and control risks and the required level of assurance to be provided by substantive procedures. The auditor would also consider the timing of tests of controls and substantive procedures, the coordination of any assistance expected from the entity, the availability of assistants and the involvement of other auditors or experts.

Hence, an audit program is an essential documented control to enable smooth, sequential completion of audit activities and to enable the auditor to assess the progress of the audit at any point of time. It is also quite possible that the audit program may itself require changes depending on newer information and trends coming to light as the audit progresses. For example, the auditor may restrict testing of backups based on results obtained at the time of compliance testing but a substantive test on a sample item such as say, payroll backup may show a corrupted media, indicating the lack of efficacy of recovery testing. This may necessitate the

auditor to extend the recovery testing to cover all critical datasets, thus resulting in the need for extended audit schedule and resources. The auditor may also be faced with a situation wherein the extended audit may be necessary but not justified by the enormous audit resources or extended schedule required. In such a situation, the auditor may be faced with the necessity of qualifying his opinion or even a disclaimer.

Developing an Audit Program

The Audit program should take into consideration the information obtained by the auditor as a part of his preliminary review and be so designed to enable him to effectively achieve the audit objectives. The audit program should essentially support the audit plan. The principles laid out in the Auditing and Assurance Standard on "Audit Planning" as regards audit program would also apply while drawing up an audit program for information systems audits:

- The auditor should prepare a written audit program setting forth the procedures that are needed to implement the audit plan. The program may also contain the audit objectives for each area and should have sufficient details to serve as a set of instructions to the audit team members, involved in the audit and as a means to control the proper execution of the audit work.
- In preparing the audit program, the auditor, having an understanding of the information systems and related business, internal and technology controls, may wish to rely on certain of these controls in determining the nature, timing and extent of required auditing procedures. The auditor may conclude that relying on certain internal controls is an effective and efficient way to conduct his audit. However, the auditor may also decide not to rely on internal controls when there are other more efficient ways of obtaining sufficient appropriate audit evidence (e.g. by application of CAATs). The auditor should also consider the timing of the procedures, the co-ordination of any assistance expected from the client, the availability of audit resources and the involvement of other auditors or experts.
- The auditor normally has flexibility in deciding when to perform audit procedures. However in some cases, the auditor may have no discretion as to timing, for example when observing controls during data migration, testing during implementation etc.
- The audit planning, ideally, commences at the conclusion of the previous year or period's audit and along with the related programme, it should be reconsidered for modification as the audit progresses. Such consideration is based on the auditor's review of the internal controls, his preliminary evaluation thereof, and the results of his compliance and substantive audit procedures.
- The IS audit requires audit programmers to be prepared, taking into consideration the technology environment and the related business process

controls. Techniques such as use of Internal Control Questionnaires (ICQs), checklists are extremely useful in the audit of technology controls as well as audit of general controls. Such questionnaires should be appropriately designed so as to achieve the audit objective. The ICQ design should collect information about the business area, data and process flow, and related controls so as to help the auditor in identifying the key controls and risk areas. Standard ICQs can also be developed based on certain standard technology, which can be applied with minimal or no modifications e.g. auditing Windows Server Security. However, care should be taken by the auditor to include special considerations that may have come to his knowledge as a part of the preliminary evaluation.

Internal Control Questionnaires offer advantages in enabling effective audit planning, implementation as well as during preliminary review phases. An ICQ evolves over time with modifications based on learning in various audits and results in an effective tool to provide significant advantages in terms of efficient utilization of audit resources, timing of audit resource usage and standardization of audit procedures. However, there is a tendency to adopt internal control questionnaires and checklists without any modification that may be critically required with respect to the audit environment or audit subject. Such an approach should be avoided since the same could affect the effectiveness of the audit and increase the audit risk.

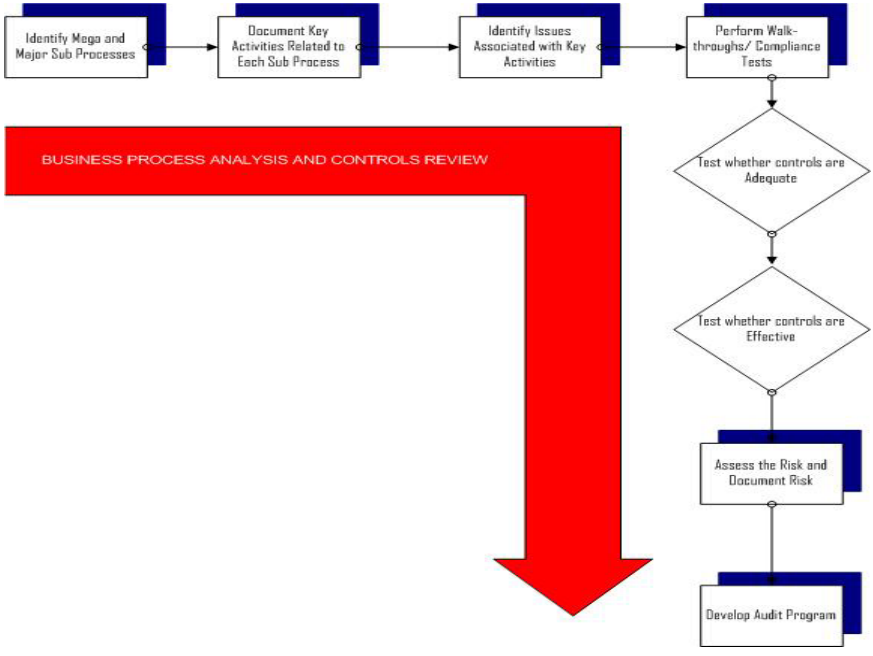


Fig 1.3 Audit program

IS Audit Methodology

Audit methodology is basically a set of audit procedures to be carried out to achieve the audit objective. An effective IS Audit methodology should essentially include;

- Objective of the IS Audit
- Scope
- Compliance Testing Procedures
- Procedures for determination of audit sample
- Substantive testing procedures
- Procedures to identify threats to assets and processes and associated controls
- Risk assessment methodology
- Methodology to test the adequacy, efficiency and effectiveness to various controls
- Procedure to identify and evaluate compensatory control
- Procedure to measure residual risk
- Reporting procedures – Interim audit Format
- Procedure for Corrective action plan
- Format of the audit report
- Compliance auditing procedure and reporting.

The IS Audit methodology is essentially a part of the IS Audit program. Audit program in addition to the audit methodology includes audit schedule, resource allocation for each of the above mentioned activity, detailed questionnaire etc. Audit plan provides input for making audit program and methodology.

While audit program is always specific to an audit assignment, audit methodology could be defined generally for specified nature of assignment. Sometimes, audit methodology forms a part of evaluation criteria before an assignment is allotted to the audit firm. In such case, a general audit methodology for the specified nature of assignment is give to the client for evaluation. E.g. Audit methodology for penetration testing or for the IS process Audit.

2. Examining and Evaluating Information

This phase entails the implementation of various procedures finalized in the audit methodology. The auditor's findings may be based upon:

- Observations
- Interviews and
- Verifications.

Verification may be manual or automated by using CAATs. CAATs might be used in performing various audit procedures, like:

- Making an audit sample by using sampling program.
- Compliance testing with reference to Application, OS or Database Controls, such as testing the parameters or configuration of the RDBMS/ OS. Many scripts, tools are available or can be developed to test the parameter setting in OS like Unix, Windows etc. or RDBMS like Oracle, MS-SQL etc.
- Tests of transactions and balances, such as recalculating interest to ensure the accuracy of process and effectiveness of controls over the process of the calculation of interest.
- Analytical review procedures for identifying inconsistent transactions or balances e.g. debit balance in deposit accounts, unclear items to ensure the controls to prevent or detect such transactions or balances are in place.
- Vulnerability Assessment.
- Penetration testing.

CAATs have been discussed in detail in Chapter 3.

Compliance Testing Vs. Substantive Testing

A compliance test determines if controls are being applied in a manner that complies with management policies and procedures.The broad objective of compliance test is to provide the IS auditors with reasonable assurance that the particular control on which the IS auditor plans to rely is operating as the IS auditor perceived in the preliminary evaluation. Compliance tests can be used to test the existence and effectiveness of a defined process, which may include a trail of documentary and/or automated evidence, for eg., to provide assurance that only authorized modifications are made to production programs.

The evaluation of internal control is accomplished through compliance and substantive testing. The purposes for compliance and substantive testing differ and will be achieved during the fieldwork.

- **Compliance Testing**--To provide reasonable assurance that the accounting control procedures are being consistently applied as prescribed by policies, procedures, rules and regulations and sound business practice.
- **Substantive Testing**--To obtain evidence of the validity and propriety of accounting treatment of transactions and balances or, conversely, of errors or irregularities therein.

Compliance tests are used to help determine the extent of substantive testing to be performed, as stated in *Statement of Auditing Standards*. Such tests are necessary if

the prescribed procedures are to be relied upon in determining the nature, time or extent of substantive tests of particular classes of transactions or balances.

Once the key control points are identified, the auditor seeks to develop a preliminary understanding of the controls to ensure their existence and effectiveness. It is achieved through Compliance testing.

Compliance testing helps an auditor determine that

- the controls exist and are working as expected
- the controls are applied in a manner that complies with policies and procedures.

A substantive test substantiates the integrity of actual processing and the outcome of compliance testing.. Substantive testing is the testing of individual transactions. It provides evidence of the validity and integrity of the balances in the financial statements and the transactions that support these balances. The IS auditors use substantive tests to test for monetary errors directly affecting financial statement balances. Substantive testing procedures focus on broadly two types of tests:

i. Tests of details of transactions and balance such as recalculating interest to ensure the accuracy of process and effectiveness of controls over the process of the calculation of interest.

ii. Analysis of significant ratios and trends including the resulting enquiry of unusual fluctuations and items in exceptions e.g. debit balance in deposit accounts, uncleared items to ensure the controls to prevent or detect such transactions or balances are in place.

There is a direct correlation between the effectiveness of controls and the extent of substantive testing required. If the auditor after compliance testing concludes that the controls are adequate and are working effectively as expected, then he is justified in reducing the size of his sample for substantive testing.

If testing of controls reveals weak controls, he might decide to go for increasing his sample for substantive testing.

Evidence Collection and Evaluation

Evidence is any information used by the IS auditor to determine whether the entity or data being audited follows the established audit criteria or objectives. It is a requirement that the auditor's conclusions must be based on sufficient, relevant and competent evidence. When planning the IS audit work, the IS auditor should take into account the type of audit evidence to be gathered, its use as audit evidence to meet audit objectives and its varying levels of reliability.

Audit evidence may include the IS auditor's observations, notes taken from interviews, material extracted from correspondence and internal documentation, or the results of audit test procedures. While all evidence will assist the Is auditor in developing audit conclusions, some evidence is more reliable than others. The rules of evidence and sufficiency as well as the competency of evidence must be taken into account, as required by audit standards.

Determinants for evaluating the reliability of audit evidence include:

- **Independence of the provider of the evidence-** Evidence obtained from outside sources is more reliable that from within the organization. This is why confirmation letters are used for verification of accounts receivable balances.
- **Qualifications of the individual providing the information/evidence-** Whether the provider of the information/evidence are inside or outside of the organization, the IS auditor should always consider the qualifications of the persons providing the information. This can also be true of the IS auditor. If an IS auditor does not have a good understanding of the technical area under review, the information gathered from testing that area may not be reliable, especially if the IS auditor does not fully understand the test.
- **Objectivity of the evidence-** Objective evidence is more reliable than the evidence that requires considerable judgment or interpretation. An IS auditor's count of cash fund is direct, objective evidence. An is auditor's analysis of the efficiency of an application, based upon discussions with certain personnel, may not be objective audit evidence.
- **Timing of the evidence-** The IS auditor should consider the time during which information exists or is available in determining the nature, timing and extent of substantive testing and, if applicable, compliance testing. For example, audit evidence processed by electronic data interchange (EDI), document image processing (DIP) and dynamic systems, such as spreadsheets, may not be retrievable after a specified period of time, if changes to the files are not controlled or the files are not backed up.

Audit evidence is evidence obtained during a financial audit and recorded in the audit working papers.

- In the audit engagement acceptance or reappointment stage, audit evidence is the information that the auditor is to consider for the appointment. For examples, change in the entity control environment, inherent risk and nature of the entity business, and scope of audit work.
- In the audit planning stage, audit evidence is the information that the auditor is to consider for the most effective and efficient audit approach. For examples, reliability of internal control procedures, and analytical review systems.

- In the control testing stage, audit evidence is the information that the auditor is to consider for the mix of audit test of control and audit substantive tests.
- In the substantive testing stage, audit evidence is the information that the auditor is to make sure the appropriation of financial statement assertions. For examples, existence, rights and obligations, occurrence, completeness, valuation, measurement, presentation and disclosure of a particular transaction or account balance.
- In the conclusion and opinion formulation stage, audit evidence is the information that the auditor is to consider whether the financial statements as a whole presents with completeness, validity, accuracy and consistency with the auditor's understanding of the entity.

According to **CICA Research Report** 'Auditors are working in an increasingly digital environment. Since audit work essentially consists of gathering audit evidence to support the content of the audit report, the fact that documentary and other evidence used as competent evidential matter for the audit is in electronic format impacts on the nature, format, reliability, accessibility and source of such evidence, that is, on the entire audit process. **Electronic Audit Evidence** addresses the numerous issues auditors face in this environment.'

The deliverable or the end product of the Information Systems Audit, like most other audits is the audit report. But the raw material for the audit report is the audit evidence, based on which the auditor forms his audit judgement. Audit Evidence includes all the information on which the auditor relies on to arrive at his audit opinion. Information collected should be sufficient, competent, relevant and useful to provide a sound basis for audit findings and recommendations.

In an Information Systems Audit such information would include significant parts of the information that are in electronic form.

Examples of evidence used in Information Systems audit include:

- logs relating to transactions, systems events or accounting logs generated by application software, database management systems, systems software etc.
- results obtained by the use of CAATs e.g. the results obtained from a generalized audit software or data extraction and analysis tools.
- electronic files containing system information on parameter settings.
- program listings, control documents such as batch job control sheet.
- systems development and testing documentation.

Besides the above, the information obtained from conventional audit procedures may also be important such as:

- observations – e.g. Inspection of physical controls, employee practices
- physical and electronic examination of media such as tapes, CDs etc.
- written policies, procedures and guidelines
- benchmarking reports, Product information and testing reports
- systems Flowcharts, Data Flow diagrams, Control Charts
- information obtained during interview with the management and personnel.

Such evidence can be obtained by application of audit procedures or a combination of:

- inquiry and Interviews with the management as well as users
- observation of processes
- inspection of electronic as well as non-electronic records and processes
- confirmation of findings through representation of information by external or independent or objective source
- recalculation, Re-performance and Use of analytical procedures.

The information obtained could broadly be categorised as:

- Auditor's recording based on observation of processes
- Audit Evidence in form of documents or in electronic forms
- Management Representations and declarations such as policies and procedures and minutes of Audit committee or steering committee meetings etc.
- Results obtained by the auditor from application of analytical procedures.

An important issue with the evidence in electronic form is that, in the absence of controls, such evidence is subject to tampering without trace of such tampering. For example, direct manipulation of values in a database may not be detected unless preventive and detective controls are put in place. Hence, one of the important qualities of the evidence that the auditor should ensure at the time of such collection is to secure the time and source of such evidence in such a manner that such evidence is capable of being retrospectively retrieved and verified.

The principles laid out in the Auditing and Assurance Standard on "Basic Principles Governing an Audit" can be extended to Information Systems Audits as well:

- The Auditor should obtain sufficient appropriate audit evidence through the performance of compliance and substantive procedures to enable him to draw reasonable conclusions from on which to base his opinion on the information resources audited.
- Compliance procedures are tests designed to obtain a reasonable assurance that those internal controls on which audit reliance is to be placed are in effect.

The auditor should obtain sufficient evidence to support his reliance on such controls designed and put in place by the management.

- Substantive procedures are designed to obtain evidence as to the completeness, accuracy, and validity of the existing internal and IT controls.

Types of audit evidence

During the planning for the IS audit work, the IS auditor should consider the quality of evidence required with respect to various audit objectives. The nature and degree of audit procedures would be significantly impacted by the quality of evidence desired.

The IS auditor should also consider whether testing of controls has been completed and attested to by an independent third party and whether any reliance can be placed on that testing.

The various types of audit evidence that the IS auditor should consider using include:

i. Observed processes and existence of physical items can include observations of activities, property and the IS functions, such as:

- An inventory of media in an offsite storage location.
- A computer room security system in operation.

ii. Documentary audit evidence, recorded on paper or other media, can include:

- Results of data extractions
- Records of transactions
- Program listings
- Invoices
- Activity and control logs
- System development documentation.

iii. Representations of those being audited can be audit evidence, such as:

- Written policies and procedures
- System flowcharts
- Written or oral statements.

iv. The results of analysing information through comparisons, simulations, calculations and reasoning can also be used as audit evidence. Examples include:

- Benchmarking the IS performance against other organisations or past periods
- Comparison of error rates between applications, transactions and users.

Availability of Audit Evidence

The IS auditor should consider the time during which information exists or is available in determining the nature, timing, extent of substantive testing and, if applicable, compliance testing. For example, audit evidence processed by electronic data interchange (EDI), document image processing (DIP) and dynamic systems such as spreadsheets may not be retrievable after a specified period of time if changes to the files are not controlled or the files are not backed up. Documentation availability could also be impacted by company document retention policies.

Selection of Audit Evidence

The IS auditor should plan to use the most appropriate, reliable and sufficient audit evidence attainable and consistent with the importance of the audit objective and the time and effort involved in obtaining the audit evidence.Where audit evidence obtained in the form of oral representations is critical to the audit opinion or conclusion, the IS auditor should consider obtaining documentary confirmation of the representations, either on paper or other media. The auditor should also consider alternative evidence to corroborate these representations to ensure their reliability.

Gathering Audit Evidence

Procedures used to gather audit evidence vary depending on the information system being audited. The IS auditor should select the most appropriate, reliable and sufficient procedure for the audit objective. The following procedures should be considered:

i. Inquiry
ii. Observation
iii. Inspection
iv. Confirmation
v. Reperformance
vi. Monitoring.

Communicating the Audit Results i.e. Reporting

The audit exercise results in the audit report, which is the deliverable or end product of the audit. The audit report, being the culmination of the auditor's work, should highlight all the key findings and recommendations. The design of the audit report would depend on the terms of engagement and audit objectives. The format and structure of the audit report should be taken into consideration at the audit planning stage itself. The audit report normally results in the identification of control weaknesses or areas of concern. The findings need to be analyzed as to their cause and consequence. Considering the prevalent practices and practical feasibility, the

auditor should formulate his recommendations. Each of the findings identified should be ranked as per pre-determined criteria. e.g. High, Medium and Low. Such rankings could be based on the risk. The rankings can be further prioritised and discussed with the auditee for accuracy. Feedback from the auditee management has to be obtained for both the findings and recommendations before their inclusion in the final report. The Audit report should include audit scope and objective, description of audit subjects, activities performed during the audit, and finally, conclusions, findings, and recommendations.

Reporting on control weaknesses

The quality of an audit is not measured by the number of findings reported but by the auditor's evaluation of the control system and identification of its weaknesses. Any existing control weaknesses could be detrimental to the quality of the control systems. Hence, evaluation of the quality of the control system is the first priority in an IS audit. The evaluation may take two forms:

i. Review and documentation of the system, whereby the system flow, manual and automated flow is documented in flow chart or narrative form. Points at which control can best be affected whether manual or automated are identified and described. Effectiveness of these control points is evaluated. Weak controls could be documented on a "finding form".
ii. Compliance and Substantive test procedures are performed on IT processes to evaluate the compliance with and the efficacy of the key controls during the audit period.

Reporting Audit Findings

During the preliminary review and verification phases, weaknesses in internal control may have been identified and recorded. These are documented in the finding form. Documented weaknesses form the basis for the auditor's report to the management. Proper preparation of the report is extremely important. Appropriate members of the audit team should be assigned the task of preparing the report. Audit findings during the various audit phases are documented on the findings forms. As each transaction in each phase is completed, the auditor who prepared the finding form should write the comments and recommendations for inclusion in the final audit report.

A typical finding form used to identify control weaknesses is given below: The auditor must identify the condition, causes and effect of the internal control weaknesses.

Sample - Control weakness – Audit finding form

Observation	Servers are not time-synchronized. It was explained that the time synchronization is taken care of manually.
Effect	In case of manual synchronization, there are always possibilities of temporary change of individual system time either intentionally or unintentionally and it's not possible to track such changes. Moreover, If the servers are not time synchronized, their logs may not be accepted as evidence in the courts of law.
Risk Ranking	High
Recommendation	Server should be made time-synchronized by interconnecting with an authentic time server which automatically updates and keeps controls of the time settings.
Management Response	Our band width cannot support additional network traffic right now. However, critical server shall be time-synchronized.

A brief explanation of each of the above terms is given below:

Observation	This section describes the problem, or more specifically the exposure. Evidence that the condition exists should be documented with the number of errors.
Effect	This section is for the description of the extent of impact or loss that has occurred or potential loss. The probability or potential extent of the exposure should be estimated to the extent possible.
Risk Ranking	The auditor's ranking of the risk in terms of the intensity of the observation.
Recommendation	This section describes the possible solution to the problem that the auditor, in discussion with the auditee management, feels is appropriate. The management looks at this section as the value added from the IS auditing exercise. The recommendation should be practicable and should provide the solution to the problem.
Management Response	This section describes the auditee management's response to the audit finding and recommendation

It is important that the auditor must discuss the findings with the management before raising the issues in the final report.

The audit report should state at a minimum the following:

- Audit objectives
- Audit scope
- Period of coverage
- Nature and extent of audit work performed
- Audit Findings
- Audit conclusions and recommendations
- Reservations or qualifications that the auditor may have.

The audit report should also be addressed to the intended recipients and specifically mention restrictions as to circulation of the report. The report should be in lucid language, objective, complete and relevant.

Salient Features of the IS Audit Reports

There cannot be standard audit report formats that could be generically applied to every audit. However, the contents and format of the IS audit report should contain the minimum requirements as per the reporting standards and the information required by the auditee. The IS auditors should consider the specific scope and objectives of the audit while designing the format and structure of the audit report. The report should be complete, accurate, objective, convincing, and as clear and concise as the subject permits. The report should include all significant audit findings.The auditor should provide the explanation in a separate reference and make reference to it in the report.

Some salient features of an audit report are given below:

i. **Report Content and Form**

An IS auditor should provide a report in an appropriate form to the intended recipients upon the completion of the audit work. The report must state the scope, objectives, period of coverage and the nature and extent of the audit work performed. It should also identify the organization, the intended recipients and state restrictions on distribution, if any. The report must include the findings, conclusions and recommendations and any reservations or qualifications that the auditor has with respect to the audit.

ii. **Purpose and Content**

A report is a formal means of communicating the objectives of the audit, the auditing standards used, the audit scope, the methodology and the findings, conclusions and recommendations

iii. **Intended Recipients**

While preparing the report, the auditor should consider the needs of the intended recipients, which may include the auditee, executive management, the Board of Directors, the audit committee and the statutory or regulatory authorities

iv. **Style and content**

The style and content of the report should be appropriate to the intended recipients. It could be in writing, oral or other form. A written report should identify the organisation audited and include a title, a signature and the date.A report on other media may include an appropriate form of authentication instead of a written signature. Reports should be objective, clear, concise, constructive and timely.

v. **Statement of objectives**

The report should include a statement of the objectives of the audit to identify what the audit intended to accomplish. If any audit objectives stated in the report were not met, this fact should be disclosed in the report.

vi. **Scope of audit**

The report should include a statement of the audit scope that describes the nature, timing and extent of audit work performed. The statement of scope should identify the functional audit area, the audit period covered and the information systems, applications or processing environments audited.

The report should identify circumstances when there has been a limitation on the scope of the audit. There is a limitation of scope when the IS auditor's opinion, tests and procedures appropriate for meeting standards could not be completed, or when an auditee imposed restrictions on the audit work.

vii. **Restrictions on distribution**

The report should identify the auditee and indicate the date of issue of the report. The report should also specify that it is solely for the information and use of the intended parties such as the auditee, board of directors, management and any intended parties outside the organisation (e.g. a government agency). Restrictions on its distribution if any should be stated.

viii. **Significant findings**

The report should include all significant audit findings. When a finding required explanation, the IS auditor describe the finding, its cause and its risk. When appropriate, explanations and reference could be included as attachments. The IS Auditor should also identify the organizational,professional and governmental criteria applied.

ix. **Conclusion**
The auditor's evaluation may be stated where appropriate. The conclusion may be an overall evaluation or multiple evaluations related to specific audit objectives**.**

x. **Recommendations**
The report should express recommendations for corrective action where it is possible, and recommendations should be linked to specific findings.

xi. **Reservations or qualifications**
The report should describe any significant reservations or qualifications and the exposure relating to such qualifications should also be mentioned.

xii. **Presentation**
The report should be logically organized and presented. It should contain sufficient and relevant information to be understood by the intended recipients.

xiii. **Timeliness**
The report should be issued in a timely manner to encourage prompt corrective action. When appropriate, the IS auditor should communicate significant findings promptly to concerned persons issuing the report. Prior communication of significant findings should not alter the intent or content of the report.

xiv. **Subsequent events**
Before issuing the final version of the report, the IS auditor should consider establishing any material changes in the organisation or its environment which might affect the reported findings conclusions and recommendations. When such changes are identified, he should alert the recipients about the potential effect of these changes on the reported findings, conclusions and recommendations.

Follow Up

The effectiveness of an Information Systems Audit is realized only if the action points and recommendations committed and agreed to by the auditee management are implemented. Hence, an important task of the auditor is to review the previous audit reports and follow up on the corrective actions and recommendations implemented within the time schedules committed by the auditee management. It is a limited scope review and do not entail going beyond the examination of actions agreed upon by the client to correct deficiencies. Normally, the status of follow up activities is included in a separate Compliance Audit Report which is issued after the completion of follow-up review. IT audit is not effective if audits are performed and reports issued, but no follow-up is conducted to determine if auditee organisation has taken appropriate corrective action. The auditor should have a follow-up program to determine if agreed corrective actions have been implemented. The level of the auditor's follow-

up review will depend upon several factors. In some instances, the auditor may merely need to inquire as to the current status. In other instances, the auditor may have to perform certain audit steps to determine if the corrective action agreed to by the auditee organisation has been implemented

The Institute of Internal Auditor's definition of a follow-up:

"A follow-up is defined as a process by which the internal auditors determine the adequacy, effectiveness and timeliness of actions taken by the management on reported audit findings."

Where agreed action plans are not completely implemented, the auditor asks the following questions:

- What remains to be done?
- By whom and when?
- Have alternatives been implemented that may be more appropriate?
- Has the agreed action plan ceased to be of value?
- If no action was taken, why not?
- What is the issue or concern causing inaction?

The end result should be a brief summary of the status of every action plan agreed upon.

The final summary is reviewed with the person responsible for clearing the audit report before the follow-up report is issued.

Documentation Requirements in Information Systems Audits

As in any other audits, documentation of audit work forms a critical task which the auditor should retain in support of his audit work. Significant amount of information may be generated during the course of the IS auditor's work. The auditor is required to ensure the evidence obtained by him on which he bases his audit opinion is sufficient, reliable, relevant and useful and enables an effective achievement of audit objectives.

The audit documentation generally includes:

- Basic documents relating to the business, technology and control environment.
- Documents relating to laws, regulations and standards applicable.
- Preliminary review and how the audit objectives and scope were evaluated and agreed upon.
- Documents relating to Risk analysis.
- Audit plan and progress against plan, Audit programs.
- Audit procedures as applied to the audit.

- Audit findings, observations, inspection reports, management representations, logs, audit trails and other related evidence.
- Interpretation of audit evidence.
- Audit Report issued.
- Auditee's observations and response to findings and recommendations.
- Reports by third party experts.
- Peer Reviews.

The audit working papers:

- Aid in the planning and performance of the audit.
- Aid in the supervision and review of the audit work.
- Provide the evidence of the audit work performed to support the auditor's opinion

The auditor's work must be documented and organized in a standardised fashion for easy reference in future audits and reference by other auditors. For purposes of easy reference, the documents may be organized as follows:

- Test work papers
- Permanent work papers
- Pending files
- Report files.

Test working papers

The testing work papers, either electronic or otherwise are those prepared or obtained as a result of the compliance and substantive testing procedures performed by the auditor, relevant to the audit engagement. Each working paper should follow a naming convention and numbering convention for naming and numbering of the work papers. The files should also contain a brief description of the content. The compliance test files should contain documentation of:

- Review of the existing internal controls.
- A summary of the tests conducted.
- Documentation of procedures performed and tools, if any used.
- Supporting documentation of detailed tests.

Substantive test files require the same elements as compliance test files except for the review of existing internal controls.

Organisation of audit working papers:

Each document must describe the following:

- Objective – Why the work was done?

- Work done – What was actually done?
- Finding – What issues arose?
- Risk – What are the risks associated with the finding, expressed in terms of impact on business?
- Recommended action – What is being recommended?
- Action – What action was agreed with the management?
- Each working paper should be supported by the evidence of the weaknesses observed

Documentation Controls

Information systems audit documentation is the record of the audit work performed and the audit evidence supporting the IS auditor's findings and conclusions.

- Each working paper (or work paper) should be:

  i. Dated and manually or digitally signed by the person completing the work.
  ii. Referenced with a unique number.

- In case of work papers and the evidence in electronic format, special care must be taken to ensure their recoverability at any subsequent date with sufficient controls to prove the date of creation and ensure protection against any modifications to the content or the state of such documents. This would require the auditor to use necessary technology such as use of appropriate media for storage of electronic evidence and their assured recoverability, use of digital signatures for protecting authenticity of documents, use of encryption techniques to safeguard the confidentiality of such documents.
- The auditor should also take care to ensure the retention of such audit documentation to be retained for sufficient length of period such that it complies with legal, regulatory, professional and organizational requirements.

Use of Sampling in Information Systems Audits

Sampling is used when time and cost considerations preclude a 100 percent verification of all transactions and events in a predefined population. The population consists of the entire group of items that needs to be examined. The subset of population members is called a sample. Sampling is used to infer characteristics of a population, based on the results of examining the characteristics of a sample of the population.

In case of Information systems audit, the knowledge of CAATs can have a significant impact on the auditor's work. Using CAATs, it may be quite possible to examine 100% of the population instead of samples. However, it should also be understood that in case of Information Systems audit, other considerations come into play. For

example, in case of banks using core banking solutions, the entire transaction database of the bank could be centralized. In such case, the entire audit function would be achieved by a small IS audit team using CAATs with capabilities of remote audit of transaction controls. In such an environment, the auditors do not have much transaction audit work at the branches since the computers at the branches are mere nodes connecting to the central database. Using CAATs may also adversely impact on the operational efficiency of the business operations since CAATs could consume enormous IT resources. These are some of the reasons that the audit would need to consider sampling in the IS audits.

The Auditing and Assurance Standard (AAS 15) "Audit Sampling" provides the related standards on the design and selection of an audit sample and the evaluation of the sample results. This AAS applies equally to both statistical and non-statistical sampling methods. Either method, when properly applied, can provide sufficient appropriate audit evidence.

The IS Auditor should consider selection techniques which result in a statistically based representative sample for performing compliance or substantive testing. Four sampling methods are commonly used:

Statistical Sampling Methods

- **Random sampling**: Ensures that all combinations of sampling units in the population have equal chances of selection.
- **Systematic sampling**: Involves selecting sampling units using a fixed interval between selections. The first interval has a random start. Examples include Monetary Unit Sampling or Value weighted selection where each individual monetary value (e.g. Rs.1) in the population is given an equal chance of selection. As the individual monetary unit cannot be ordinarily examined separately, the item, which includes the monetary unit is selected for examination. . Another example includes selecting every nth sampling unit.

Non-Statistical Sampling Methods

- Haphazard sampling : The IS Auditor selects the sample without following a structured technique, but avoiding any conscious bias or predictability. However, analysis of a haphazard sample should not be relied upon to form a conclusion on the population.
- Judgmental Sampling : The IS Auditor places a bias on the sample (e.g. All sampling units over a certain value, all for a specific type of exception, all negatives, all new users, etc.). A judgmental sample is not representative of the population and is not statistically based so the results should not be extrapolated over the population.

The IS Auditor should select sample items in such a way that it is representative of the population. The selected sample should represent all the characteristics of the population being tested. This is done by statistical sampling methods. In order to maintain audit independence, the IS Auditor should ensure the population is complete and control the selection of the sample.

For a sample to be representative of the population, all sampling units in the population should have an equal or known probability of being selected i.e. statistical sampling methods should be used. There are two commonly used selection methods: selection on records, and selection on quantitative fields (e.g. monetary units).

Methods in Use (For selection on records):

- Random Sample (Statistical sample)
- Haphazard Sample (Non statistical)
- Judgmental Sample (Non statistical: high probability to lead to a biased conclusion).

Examples of compliance testing of controls where sampling could be considered include user access rights and authorizations granted, program change control procedures, documentation, follow up on exceptions, review of logs, software license audits etc.

Examples of substantive tests where sampling could be considered include re-performance of complex calculation (e.g. Interest) on a sample of accounts, sample of transactions to vouch to supporting documentation etc.

When using sampling methods either statistical or non-statistical, the IS Auditor should design and select an audit sample, perform audit procedures and evaluate the sample results. Thus, he can obtain sufficient, reliable, relevant and useful audit evidence.

Statistical sampling uses techniques from which mathematically constructed conclusions regarding the population can be drawn. Non-statistical sampling is not statistically based and the results should not be extrapolated over the population, as they may not be representative of the population. When designing the size and structure of an audit sample, the IS auditors should consider the specific audit objectives, the nature of the population, the sampling and the selection methods. The IS auditor should also consider the need to involve appropriate specialists in the design and analysis of samples.

Various aspect in Sampling Audit

i. **Sampling Unit**

The sampling unit depends on the purpose of the sample. For compliance testing of controls, attribute sampling is typically used, where the sampling unit is an event or transaction (e.g. A control such as "to determine invoices that are not duly authorized").

For substantive testing, on the other hand, variable or estimation sampling is frequently used and the sampling unit is often monetary. (e.g. Testing of inventory, debtors etc.).

ii. **Audit objectives**

The IS auditor should consider the specific audit objectives to be achieved and the audit procedures which are most likely to achieve those objectives. In addition, when audit sampling is appropriate, he should consider the nature of the audit evidence sought and possible error conditions.

iii. **Population**

The population is the entire set of the data from which the auditor wishes to sample in order to reach a conclusion on the population. Therefore, the population from which the sample is drawn should be appropriate and verified. Also it must be complete for the specific audit objective.

iv. **Stratification**

Stratification may be necessary for designing the sample efficiently and effectively. Stratification is a process of dividing a population into sub-populations (strata) with similar characteristics explicitly defined so that each sampling unit can belong to only one stratum.

v. **Sample size**

When determining sample size, the IS auditor should consider the sampling risk, the amount of the error that would be acceptable and the extent to which errors are expected.

vi. **Sampling risk**

Sampling risk arises from the possibility that the IS auditor's conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure. There are two types of sampling risks:

The risk of incorrect acceptance: The risk that material misstatement is assessed as unlikely when in fact the population is materially misstated.

The risk of incorrect rejection – The risk that material misstatement is assessed as likely when actually the population is not materially misstated.

The level of sampling risk that the IS auditor is willing to accept affects the sample size.

Sampling risk should also be considered in relation to the audit risk model and its components, inherent risks, control risks and detection risks.

vii. **Tolerable error**
Tolerable error is the maximum error in the population that IS auditors are willing to accept and still conclude that the audit objectives have been achieved. For substantive tests, tolerable error is related to the auditor's judgment about materiality. In compliance tests, it is the maximum rate of deviation from a prescribed control procedure that the IS auditor is willing to accept.

viii. **Expected error**
If the IS auditor expects errors in the population, he selects a larger sample than when no error is expected. This helps to conclude that the actual error in the population is not greater than the planned tolerable error. Similarly, lower sample sizes are justified when the population is expected to be error free. When determining the expected error in a population, the auditor should consider such matters as error levels identified in previous audits, changes in the organisation's procedures and the evidence available from an evaluation of the system of internal control and results from analytical review procedures.

The audit work papers should include sufficient details to clearly describe the sample objective and the sampling process used. The work papers should include the source of the population, the sampling method used, sampling parameters (e.g. random start number or method by which random start was obtained, sampling interval), items selected, details of audit tests performed and conclusions reached.

Having performed appropriate audit procedures on each sample item, he should analyse any possible errors detected in the sample. He can thereby determine whether there are actually errors and their nature and cause and the possible effect of the error on the other phases of the audit. He should consider the qualitative aspects of the errors. The errors should be projected as appropriate to the population, if the sampling method used is statistically based.

Errors caused by the breakdown of an automated process ordinarily have wider implications for error rates than human errors. When the expected audit evidence regarding a specific sample item cannot be obtained, the auditor may be able to

obtain sufficient and appropriate audit evidence by performing alternative procedures on the item selected.

The IS auditor should consider projecting the results of the sample to the population with a method of projection consistent with the method used to select the sampling unit. The projection of the sample may involve estimating probable errors and estimating any undetected errors due to imprecision of the technique together with the qualitative aspects of any errors found.

The IS auditor should consider whether the errors in the population might exceed the tolerance error. While doing so the results of the other audit procedures relevant to the audit objective must be taken into account. If the projected population error exceeds the tolerable error, the IS auditor should reassess the sampling risk. If the risk is unacceptable, he should consider extending the audit procedure or performing alternative audit procedures.

Key steps to construction and selecting samples for an audit test:

- Determine the objectives of the test (e.g. compliance or substantive).
- Define the population to be sampled.
- Determine the appropriate sampling method, such as attribute vs. variable sampling.
- Determine the precision, reliability and tolerance desired.
- Calculate the sample size.
- Select the sample.
- Evaluate the sample from an audit perspective.
- Document the Result.

Design of the Sample

ISA 530 on "Audit Sampling and other selective testing procedures" prescribes the guidelines for designing an audit sample:

When designing an audit sample, the auditor should consider the objectives of the test and the attributes of the population from which the sample will be drawn.

- The auditor first considers the specific objectives to be achieved and the combination of audit procedures which is likely to best achieve those objectives. Consideration of the nature of the audit, evidence sought and possible error conditions or other characteristics relating to that audit evidence will assist the auditor in defining what constitutes an error and what population to use for sampling.
- The auditor considers what conditions constitute an error by reference to the objectives of the test. A clear understanding of what constitutes an error is

important to ensure that all, and only those, conditions that are relevant to the test objectives are included in the projection of errors. For example, in a substantive procedure relating to the existence of accounts receivable, such as confirmation, payments made by the customer before the confirmation data but received shortly after that date by the client are not considered an error. Also, a mis-posting between customer accounts does not affect the total accounts receivable balance. Therefore, it is not appropriate to consider this an error in evaluating the sample results of this particular procedure, even though it may have an important effect on other areas of the audit, such as the assessment of the likelihood of fraud or the adequacy of the allowance for doubtful accounts.

When performing tests of control, the auditor generally makes a preliminary assessment of the rate of error the auditor expects to find in the population to be tested and the level of control risk. This assessment is based on the auditor's prior knowledge or the examination of a small number of items from the population. Similarly, for substantive tests, the auditor generally makes a preliminary assessment of the amount of error in the population. These preliminary assessments are useful for designing an audit sample and in determining sample size. For example, if the expected rate of error is unacceptably high, tests of control will normally not be performed.

However, when performing substantive procedures, if the expected amount of error is high, 100% examination or the use of a large sample size may be appropriate.

Evaluating the Sample Results

The auditor should evaluate the sample results to determine whether the preliminary assessment of the relevant characteristic of the population is confirmed or needs to be revised.

- In the case of a test of controls, an unexpectedly high sample error rate may lead to an increase in the assessed level of control risk, unless further evidence substantiating the initial assessment is obtained. In the case of a substantive procedure, an unexpectedly high error amount in a sample may cause the auditor to believe that an account balance or class of transactions is materially misstated, in the absence of further evidence that no material misstatement exists.
- If the total amount of projected error plus anomalous error is less than but close to that which the auditor deems tolerable, the auditor considers the persuasiveness of the sample results in the light of other audit procedures, and may consider it appropriate to obtain additional audit evidence. The total of projected error plus anomalous error is the auditor's best estimate of error in the

population. However, sampling results are affected by sampling risk. Thus, when the best estimate of error is close to the tolerable error, the auditor recognizes the risk that a different sample would result in a different best estimate that could exceed the tolerable error. Considering the results of other audit procedures helps the auditor to assess this risk, while the risk is reduced if additional audit evidence is obtained.

- If the evaluation of sample results indicates that the preliminary assessment of the relevant characteristic of the population needs to be revised, the auditor may:

  i. Request the management to investigate identified errors and the potential for further errors, and to make any necessary adjustments; and/or
  ii. Modify planned audit procedures. For example, in the case of a test of control, the auditor might extend the sample size, test an alternative control or modify related substantive procedures; and/or
  iii. Consider the effect on the audit report.

Summary

The Chapter discussed the process of IS audit- the different phases have been described. The audit procedures and techniques are explained properly. The chapter starts with defining what is audit and scope and objective to drafting audit mission and charter. It also defines the additional skills and competence required to conduct the IS audit. The systematic approach has been defined while performing IS audit by the auditor.

The chapter discussed various documentation associated with audit and report formats. Finally, Use of sampling in IS audit as well as various aspects of sampling audit is discussed thoroughly.

SELF-ASSESSMENT TEST QUESTIONS

1 What should the audit strategy be?
  a. It should be knowledge-based.
  b. It should be cycle-based.
  c. It should be request-based.
  d. It should be risk-based.

2. An entity's internal control system is built into all of the following basic management processes except:
  a. Planning
  b. Execution
  c. Monitoring
  d. Risk.

3. An information systems (IS) auditor is not concerned with which of the following?
   a. Inherent risk
   b. Country risk
   c. Detection risk
   d. Control risk.

4. The scope of an IS audit affects which of the following?
   a. Audit schedules
   b. Audit objectives
   c. Audit summary
   d. Audit program.

5. Which of the following would not be considered in performing a risk analysis exercise?
   a. System complexity
   b. Results of prior audits
   c. Auditor skills
   d. System changes.

6. Which of the following actions impairs the IS auditor's independence?
   a. The auditor designs controls
   b. The auditor tests controls
   c. The auditor advises on controls
   d. The auditor designs an integrated test facility.

7. The best time to write an audit program is during the:
   a. Planning phase
   b. Substantive testing phase
   c. Survey phase
   d. Compliance testing phase.

8. Which of the following is a proper step in an audit program?
   a. Notification of the audit
   b. Observation of procedures
   c. Definition of audit objectives
   d. Planning for audit reporting.

9. In the implementation of control self-assessment (CSA), which of the following examines a given business process in-depth?
   a. Horizontal sessions
   b. Diagonal sessions
   c. Vertical sessions
   d. Individual sessions.

10. The first step in the IS compliance audit testing is to review which of the following?
    a. Access security controls
    b. Input controls
    c. Processing controls
    d. Output controls.

11. During an audit, an IS auditor found no written procedures for an application system. What should the auditor do?
    a. Cancel the audit immediately since it is hard to do an audit without documentation.
    b. Reschedule the audit when the procedures are written.
    c. Report the issue to the management.
    d. Document the procedures and audit against them.

12. The major purpose of control self-assessment (CSA) is:
    a. Control
    b. Improvement
    c. Documentation
    d. Auditing.

13. The objective of control tests of details of the transactions performed by the IS auditor is to:
    a. Determine the nature, timing and extent of substantive tests to be performed on the IS records and files.
    b. Detect material control weaknesses in the IS operations.
    c. Evaluate whether an IS control policy or procedure is working effectively.
    d. Inquire whether all IS employees have an access card to enter the computer room.

14. In an information technology (IT) environment, which of the following is not a compliance review and/or test?
    a. Determining whether polices are a available.
    b. Performing system storage media analysis
    c. Determining whether system logs are reviewed.
    d. Determining whether system errors are present.

15. During the IS audits, the type of evidence the auditor uses does not include:
    a. Physical evidence
    b. Documentary evidence
    c. Representations
    d. Reporting.

16. In a variables sampling application, which of the following will result when the confidence level is changed from 90 to 95 percent?
    a. Standard error of the mean will not be affected.
    b. Non-sampling error will decrease.
    c. Sample size will increase.
    d. Point estimate of the arithmetic mean will increase.

17. Sample size:
    a. Increase with the use of higher confidence levels.
    b. Decrease with the use of higher confidence levels.
    c. Remains unchanged with changes in confidence levels.
    d. Increases with the use of lower confidence levels.

18. A car rental agency has branches located throughout the world that are essentially small-scale representations of the entire population. What is the appropriate sampling method for determining the average net revenue per vehicle in inventory?
    a. Stratified sampling
    b. Cluster sampling
    c. Attributes sampling
    d. Systematic sampling.

19. Which one of the following statements about sampling is true?
    a. A large sample is always more representative of the underlying population than a smaller sample.
    b. For very large populations, the absolute size of a sample has more impact on the precision of its results than does its size relative to its population.
    c. For a given sample size, a simple random sample always produces the most representative sample.
    d. The limitations of an incomplete sample frame can almost always be overcome by careful sampling techniques.

20. A distinguishing characteristic of random number sample selection is that each:
    a. Item is selected from a stratum having minimum variability.
    b. Item's chance for selection is proportional to its dollar value.
    c. Item in the population has an equal chance of being selected.
    d. Stratum in the population has an equal number of items selected.

21. The primary reason for an auditor to use statistical sampling is to:
    a. Obtain a smaller sample than would be required by non-statistical sampling techniques.
    b. Obtain a sample more representative of the population than would be obtained by non-statistical sampling techniques.

c. Allow the auditor to quantify and, thus, control the risk of making an incorrect decision based on sample evidence.
d. Meet auditing standards.

22. Which of the following is not an audit procedure that is commonly used in conducting the IS tests of controls (compliance reviews and tests)?
    a. Confirmations
    b. Inquiry
    c. Observations
    d. Inspections.

23. Which of the following represents the correct sequence of performing the IS audit procedures?
    a. Substantive tests
    b. Interviews of IS and/or user personnel
    c. Compliance tests
    d. Preliminary evaluation.
        i. 1,2,3. and 4
        ii. 3,4,2, and 1.
        iii. 4,2,3, and 1
        iv. 2,4,3, and 1

24. An IS auditor's primary consideration regarding internal control policies, procedures, and standards available in the IS department is whether they are:
    a. Documented
    b. Distributed
    c. Followed
    d. Approved.

25. The results of analysis of the information gathered during the performance of the IS audit procedures should focus on:
    a. Ensuring the availability of user personnel.
    b. Comparing service level objectives to actual results.
    c. Ensuring the availability of the IS personnel.
    d. Understanding the operating policies and procedures.

26. The major objective in understanding the IS internal control structure is to provide the IS auditor with:
    a. A basis for planning the information systems audit.
    b. A basis for conducting test of controls.
    c. A basis for modifying tests of controls.
    d. A basis for reviewing the IS and user documentation.

27. In an IS audit environment, the likelihood of assessing too low a control risk relates to the:
    a. Efficiency of the audit
    b. Allowance for unforeseen errors and irregularities
    c. Allowance for unforeseen changes
    d. Effectiveness of the audit.

28. The IS auditor primarily uses the information provided by a detailed understanding of the IS controls and final risk assessment to determine the nature, timing, and extent of the:
    a. Substantive tests.
    b. Attribute tests.
    c. Sampling tests.
    d. Tests of controls.

29. In an IT environment, which of the following is not a substantive review and/or test?
    a. Determining whether program changes are approved
    b. Performing system aging analysis
    c. Performing program activity analysis
    d. Performing job activity analysis.

30. For an IS auditor, proper evidence in terms of representations would not include which of the following?
    a. Written policies and procedures
    b. Independence
    c. System flowcharts
    d. Verbal statements

31. Indicate the order in which primary questions must be addressed when an organization is determined to audit for fraud.
    a. How vulnerable is the organization?
    b. How can the organization detect fraud?
    c. How might someone go about defrauding the organization?
    d. What does the organization have that someone would want to defraud?

1. D	2. D	3. B	4. A	5. C	6. A	7. A	8. B	9. C
10. A	11. D	12. B	13. C	14. B	15. D	16.C	17.A	18.B
19.B	20. C	21. C	22. A	23. D	24. C	25. B	26. A	27. D
28. A	29. A	30. B	31. D					

References and Sources:

1. Information Tech environment: why are controls and audit important, Info tech. control and audit, third edition,Sandra senft,Frederick Gallegos,CRC press
2. Wikipedia.org
3. Weber,R.,Information System Control and Audit, 1999
4. ISACA
5. INTOSAI
6. CISA review manual 2007
7. Mcneese.edu
8. Primeacademy.com

2 Information Risk Management

Learning Objectives

- Gain knowledge of an integrated approach to Information Risk Management
- Understand IS Threats, vulnerabilities and risks
- Gain knowledge on IS risk assessment
- Gain knowledge on various categories of controls and their assessment
- Gain knowledge of use of IS risk assessment as key to planning and performing an audit

Information Risk Management

Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization and deciding what actions, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.

The Information Risk Management is a key aspect of modern decision making for all industries. The universal need to make informed, realistic and justifiable decisions in the face of uncertainty is the driver for increased information risk management activities in most of the organizations.

Effective risk management begins by specifying clearly the organization's appetite for risk. It encompasses identifying, analyzing, evaluating, monitoring and communicating the impact of risk on IT processes. Having defined risk appetite and identified risk exposure, the management may develop strategies to avoid, mitigate, transfer, accept or eliminate individual risks.

As discussed in the previous chapter, the basic premise of IS audit is to independently conduct an appraisal of the risk management as regards the risks to business arising from the use of IT. Hence it is significant that the IS Auditor be aware of the nature of IS risks, threats, vulnerabilities and types of security controls to mitigate the risks. Further, auditors should be in a position to evaluate the risk management measures and to identify the residual risks as IS audit has a very important role to play in the entire process of Information Risk Management.

Why is Information Risk Management Important?

The management of risks is a cornerstone of IT governance, ensuring that the strategic objectives of the business are not endangered by IT failures. IT related risks are increasingly a board-level issue as the impact on the business of an IT failure—be it an operational crash, security breach or failed project—can have devastating consequences.

Risk management itself is not a new topic and risk taking is an everyday part of managing an enterprise. However, understanding the risks relating to the use of information technology is still a challenge for business executives who probably do not have an in-depth appreciation of the technical issues. Technical complexity, misunderstanding of risks and a tendency for the media to create hype regarding certain risks can result in some significant risks being overlooked and others receiving possibly too much emphasis. Ultimately, though, risk taking is an essential element of business today and success comes to those organizations that identify and manage risks most effectively. Risk is as much about failing to grasp an opportunity as it is about doing something badly or incorrectly.

Information Risk Management: Process

The process of Information Risk Management typically involves the following steps:

- Identifying and classifying information assets,
- Valuation of the information and information assets as per their criticality
- Identifying threats and vulnerabilities to those assets,
- Measuring or assessing risk
- Developing strategies to manage risk

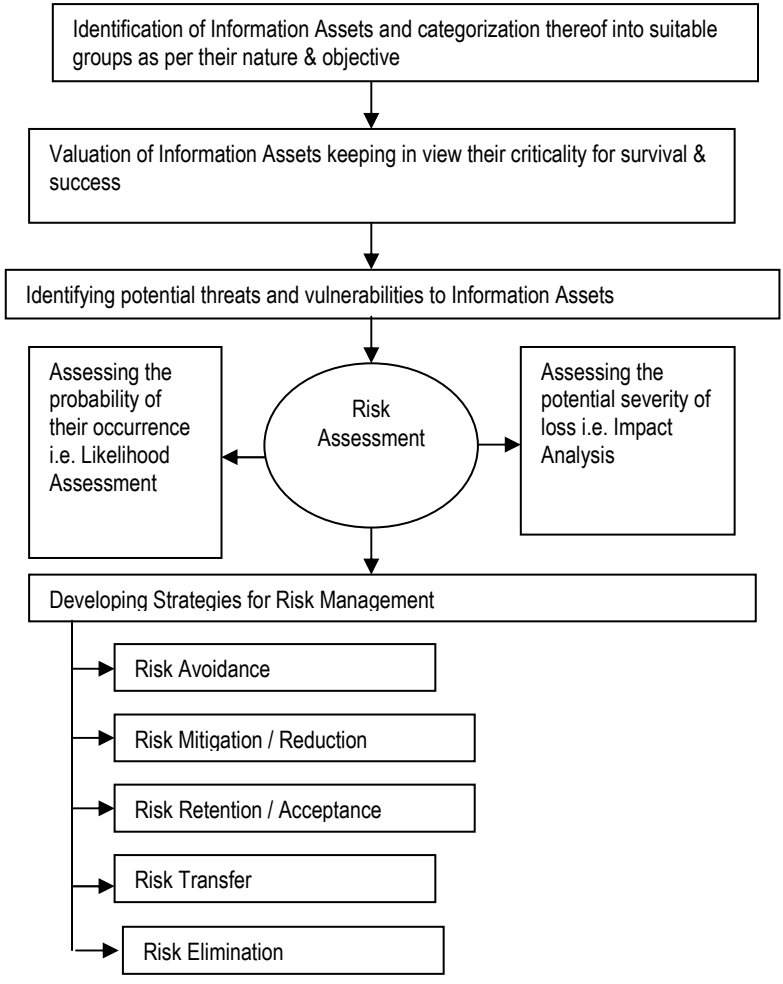


Fig 2.1 Information Risk Management: Process

Step 1: Identification of Information Assets

The first step in the information risk management process is to identify the information assets supporting critical business operations that need to be protected. The assets could fall under different groups which are:

Conceptual / Intangible Assets

- Data and Information: Business and related information contained in various storage devices such as hard disks or in transit may be subject to unauthorized disclosure, copying, theft, corruption or damage.

- Software: Application software (application packages for accounting, payroll, sales etc.) and system software (operating system, utility programs, compiler, communication software, DBMS etc.). Such programs may be susceptible to intentional or unintentional unauthorized modification by persons internal or external to the organization or by faulty technology processes.

Physical / Tangible Assets

- People (e.g. skilled users, analysts, programmers etc.)
- Hardware (e.g. mainframes, minicomputers, microcomputers, storage media, printers)
- Networking devices (e.g. communication lines, concentrators, hubs and switches etc.)
- Facilities: The computing and communication equipments such as servers could require special environment such as air-conditioned, dust free, humidity controlled facilities.
- Documentation (e.g. printed forms, manuals, system and database documentation, IS policies & procedures)

Step 2: Valuation of Information Assets

The information classification process focuses on business risk and data valuation. Not all data has the same value to an organization. Some data is more valuable to the people who are making strategic decisions because it aids them in making long-range or short-range business direction decisions. Some data, such as trade secrets, formulas, and new product information, are so valuable that its loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility.

Information systems resources may require classifying or categorizing according to their sensitivity. This would depend upon the risks affecting such resources and impact resulting from exposure. Such classification makes for administrative convenience of implementing and maintaining access control systems and importantly optimizing the cost of security.

Some information is more critical to a business than others such as production process information, formulas, strategic plans, research information. In the financial services industry, for example, information assets are very close to being financial assets. The loss of such information can jeopardize the existence of the business or create loss of goodwill and trust among stakeholders and loss of brand equity.

Compared to this, the organization may also have information, which is of less consequence in the event of their loss, such as a list of customers, details of

employees' salaries, etc. Thus in order to ensure cost-effective controls, it is beneficial to classify the entire organizational information. This also enables fine tuning of access control mechanisms and avoids the cost of over-protecting and under protecting information. The assets so identified and grouped may be categorized into different classes, which are:

- **Top secret:** This indicates the highest classification wherein the compromise of the confidentiality, integrity and availability can endanger the existence of the organization. Access to such information may be restricted to either a few named individuals in the organization or to a set of identified individuals.
- **Secret:** Information in this category is strategic to the survival of the organization. Unauthorized disclosure could cause severe damage to the organization and stakeholders.
- **Confidential:** Information in this category also needs high levels of protection but unauthorized disclosure may cause significant loss or damage. Such information is highly sensitive and should be well protected.
- **Sensitive:** Such information requires higher classification as compared to unclassified information. Disclosure may cause serious impact.
- **Unclassified:** Information that does not fall in any of the above categories finds place here. This also implies that the nature of the information is such that its unauthorized disclosure would not cause any adverse impact on the organization. Such information may also be made freely available to the public.

Another type of classification, popular in commercial organizations, can be: Public, Sensitive, Private and Confidential.

Data Privacy and Data Protection

Many advanced nations have enacted legislations concerning "Data Privacy". These often take the form of prohibiting release of medical or other information to third parties without a court order. Regulatory bodies also require restriction on dissemination of data collected by certain industries, notably banks and financial services.

The UK's Data Protection Act, 1988, for example, has the following key features and is not limited specifically to data held electronically:

There are strict controls on the processing of 'sensitive personal data' (i.e. race, ethnicity, gender, health), even where it is processed only for research purposes.

The Act also prescribes compliance audits.

The aims of data protection compliance audits go beyond the basic requirements of say Data Security and address wider aspects of data protection including:

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully and on a proper basis.
- Quality Assurance – ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive.
- Retention – appropriate weeding and deletion of information.
- Documentation on authorized use of systems, e.g. codes of practice, guidelines etc.
- Compliance with individual's rights, such as subject access.
- Compliance with the data protection legislation in the context of other pieces of legislation.

Step 3: Identifying the potential threats

Threat can be defined as an event that contributes to the interruption or destruction of any service, product or process. Common classes of threats are:

- Errors
- Malicious damage / attack
- Fraud
- Theft
- Equipment/software failure

Threats occur because of vulnerabilities associated with use of information resources. Vulnerabilities are characteristics of information resources that can be exploited by a threat to cause harm. Examples of vulnerabilities are:

- Lack of user knowledge
- Lack of security functionality
- Poor choice of passwords
- Untested technology
- Transmission over unprotected communication medium

Computer systems are vulnerable to threats that cause damage ranging from the loss of database integrity to the destruction of entire computer facilities. The sources of loss could be manifold from mere technological glitches to hackers, disgruntled or adventurous employees, data entry clerks, etc. These threats could affect the confidentiality, integrity or availability of system information or resources.

Confidentiality

Confidentiality involves the protection of the organization's sensitive information from disclosure to unauthorized persons and processes.

Confidentiality threats in an IT environment include intentional as well as unintentional access to sensitive information. A few examples of exposures are given hereunder:

- Improper application controls in application software may lead to sensitive information being accessed by employees not having any need to access such information e.g. a payroll clerk may get accidental access to confidential records of management employees.
- Unauthorized disclosure arising from the access of confidential data on a system/network by inadvertent broadcast of data across the network, improper disposal of data etc.
- Accidental access to spool files used by printers may compromise sensitive information which may otherwise be protected by stringent access controls.

Integrity

Integrity requires that the business information and related processes should not suffer any intentional or accidental unauthorized modification, which may result in serious consequences to the business.

Integrity violations in an IT environment are also common due to system errors which include corruption of files, power failures leading to unauthorized alteration in the values being transmitted or stored, erroneous program codes leading to alteration of values in data files etc; hence the need to prevent the processes from performing any integrity violations.

A few examples of threats are given hereunder:

- A bank employee not having authority to credit files may tamper with the sanctioned amount of credit facilities by bypassing the application controls and making direct changes to data files or by gaining unauthorized access to the manager's login.
- Computer virus may cause corruption of data / program thereby causing loss of transactions or state of integrity of such transactions.
- Integrity violations in mission critical systems could cause irreparable damage to the business, threats to national security or loss of lives e.g. corruption of tariff data files of Indian Railways, changes in values or parameter files of missile control systems, meteorological warning systems, corruption of program codes of autopilot systems used in flight control etc.

Availability

Availability relates to whether the information and information technology processes are available to the authorized business users when required.

Availability therefore requires safeguarding the information systems and processes that are essential for supporting business processes, so as to ensure that the information systems and processes critical for conduct of business will be available to authorized users as and when required.

A few examples of exposures are given hereunder:

- The most common problems of availability occur due to improper capacity availability such as strangulated bandwidth, low computer resources as against the actual requirements such as processing capacity, storage capacity, number of terminals etc.
- Failure or improper functioning of power systems can lead to the computer systems being dysfunctional and hence not available for service e.g. power failure during banking hours.
- Intentional unavailability can also be created by hackers by launching denial-of-service attacks.

A clear idea of threats in the working environment will enable systems managers to implement the most cost-effective security measures.

Sources and Causes of Threats

Various threats can be grouped into environmental and man-made threats. Man made threats can again be categorized into internal and external threats as depicted in the figure 2.2.

Step 4: Information Risk Assessment

Once the assets and corresponding potential threats have been identified, the systems are reviewed for weaknesses that can be exploited and the likelihood of those being exploited.

Information security professional or IS auditor here audits various systems and processes to find out vulnerabilities or weaknesses that can lead to a threat being materialized.

Vulnerability Assessment

Vulnerability is a condition or weakness in (or the absence of) the safeguards, procedures, technical controls, physical controls or other controls that could be exploited by the threat.

Sometimes the threat viewed in isolation may be misleading unless the vulnerabilities are taken into consideration. In most cases the threats attempt to exploit the vulnerabilities to cause loss or harm to the assets. For example, a hacker would look

for loopholes in the architecture of the firewall to compromise the controls and gain unauthorized access to the networks.

Probability or Likelihood Assessment

Likelihood is the estimation of the frequency, or the chance of a threat happening. A likelihood assessment considers the presence, tenacity and strength of threats, as well as, the effectiveness of safeguards. In general, historical information about many threats is weak, particularly with regard to human threats; hence the judgment and experience in this area is of relevance. Some threats affect data especially threats to physical assets such as fires, floods etc. Care needs to be taken in using any statistical threat data; the source of data otherwise the analysis may be inaccurate or incomplete. In general, the greater the likelihood of a threat occurring, the greater is the risk.

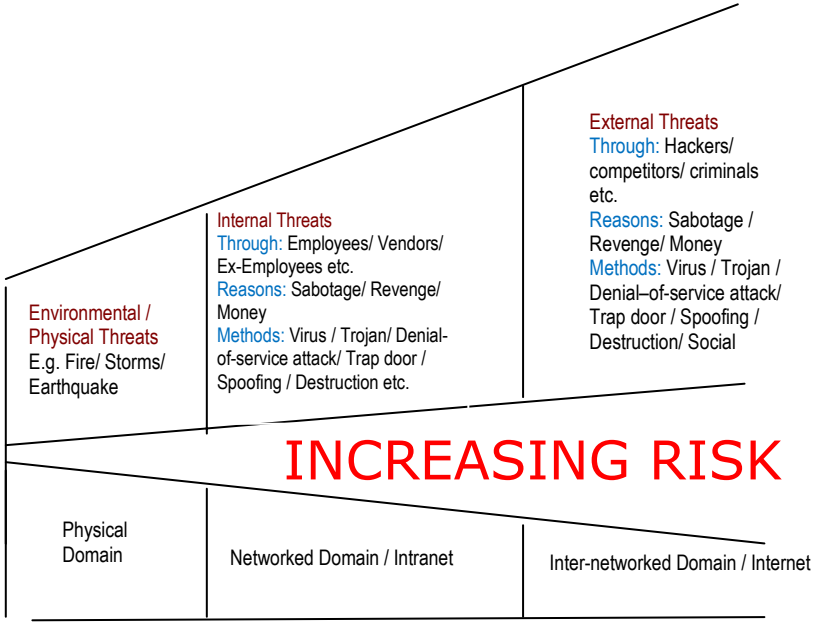


Fig 2.2 Categories of Threats

To some extent, the nature and value of information assets affect the likelihood of occurrence of a threat. If the asset is of high value, e.g. proprietary software packages, it is a prime target for piracy attempts. Thus, the identification and valuation of assets also assists with the identification of threats and their likelihood of occurrence. Periodically, the likelihood of occurrence of a threat needs to be reassessed due to changes occurring in the structure, direction, and environment of an organization.

Impact Analysis

The threat that is successful in causing harm or loss to an asset results in an impact. Impact may be either in terms of direct loss of money or financial impact such as a hacker stealing a sensitive file containing all information about credit card customers that is used by the ATM access control system. Impact need not necessarily be in terms of direct impact of money; but can be, for example, disruption of operations leading to operational loss and delayed and back log processing etc. IT risks can also lead to significant losses in terms of damages (both monetary as well as to the reputation of the organization) such as a hacking attack leading to compromise of sensitive financial information of customers, which may be published by the hacker on the Internet resulting in both legal repercussions and loss of reputation.

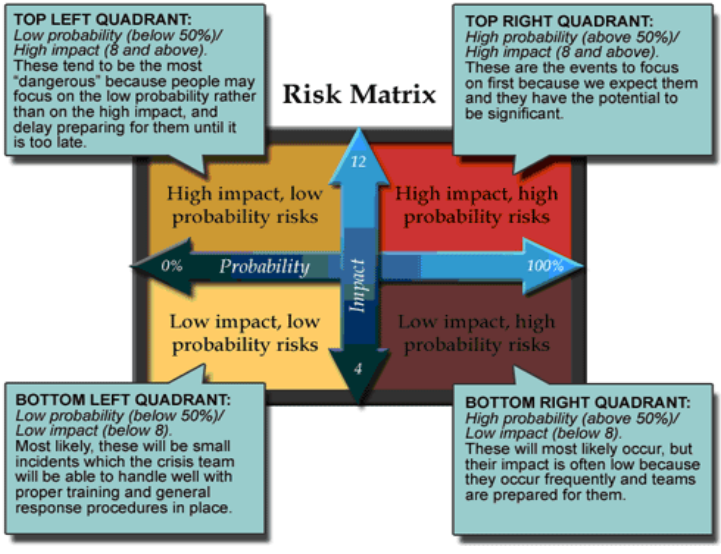


Fig 2.3 Risk Matrix

Step 5: Developing Strategies for Information Risk Management

Once risks have been identified and assessed, appropriate corrections shall be made to the system, if required. Immediate action may not be taken to correct some identified vulnerabilities but the process will at least analyze these vulnerabilities, document and recognize them for risk management decisions.

The strategies to manage the risk fall into one or more of these four major categories:

Risk Avoidance: It means not doing an activity that involves risk. It involves losing out on the potential gain that accepting the risk might have provided. E.g. not using

Internet / public network on a system connected to organization's internal network, instead using a stand-alone PC for Internet usage.

Risk Mitigation / Reduction: It involves implementing controls to protect IT infrastructure and to reduce the severity of the loss or the likelihood of the loss from occurring. E.g. using an effective anti-virus solution to protect against the risk of viruses and updating it on timely basis.

Risk Transfer: It involves causing another party to accept the risk i.e. sharing risk with partners or insurance coverage.

Risk Retention / Acceptance: It means formally acknowledging that the risk exists and monitoring it. In some cases it may not be possible to take immediate action to avoid/mitigate the risk. All risks that are not identified or avoided or transferred are retained by default. These risks are called residual risks. Risk management aims to identify, select and implement the controls that are necessary to reduce residual exposures to acceptable levels.

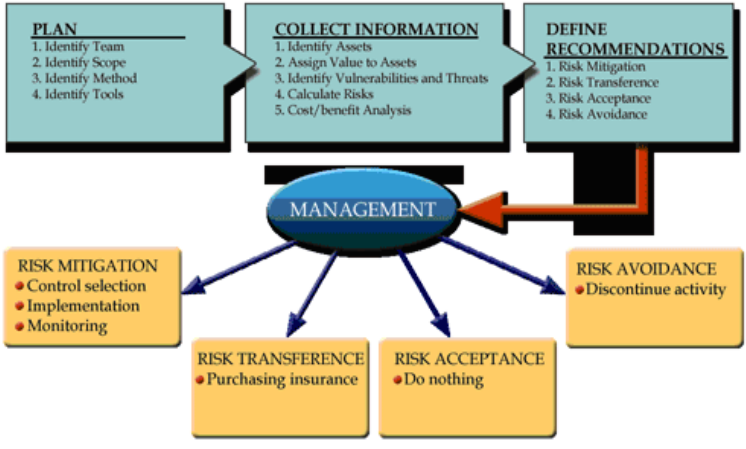


Fig 2.4 Management of Risk

The goals and mission of an organization should be considered in selecting any of these risk management strategies. It may not be practical to address all identified risks, so priority should be given to the risks that have the potential to cause significant mission impact or harm.

In ideal information risk management, a prioritization process is followed whereby the risks with the greatest loss and the greatest probability of occurrence are handled first, and risks with lower probability of occurrence and lower loss are handled later. In practice the process can be very difficult, and balancing between risks with a high

probability of occurrence but lower loss versus a risk with high loss but lower probability of occurrence can often be mishandled.

Understanding the Relationships Between IS Risks and Controls

Risks that threaten the IS cannot be altogether eliminated but, through appropriate decisions and actions can be mitigated. Threats to information system can materialize as an outcome of poor controls or absence of controls. Any threat to the system or its components could result in a loss to the company as a consequence of exploitation of the vulnerabilities.

A control is a check or restraint on a system which is designed to enhance its security. Controls can act to:

- reduce a threat
- reduce vulnerability to a threat
- reduce impact of a threat
- detect an impact
- recover from an impact

The objective of IS controls is to prevent the threats from exploiting the vulnerabilities of the assets or the safeguards. In the event the threats cannot be prevented, the controls should enable timely detection and trigger corrective action. In the event of failure of a control, threats could cause harm to the assets resulting in an actual impact.

IS Auditor should be able to evaluate whether available controls are adequate and appropriate to mitigate the IS risks. In the case of deficiency in controls or existence of newer or uncontrolled risks, the IS auditor should report such weaknesses to the auditee management along with appropriate recommendations. Hence it is important for the IS auditor to understand the relationship between risks and controls. He should also be thorough with the process and procedure of reviewing and evaluating controls.

The auditor should understand that the controls always have a cost, but also come with a benefit. The cost could be in terms of time or investment of money or sometimes even compromising with the performance of systems e.g. anti-virus software or intrusion detection systems consume the resources and might make the system slow. Benefits could be in terms of reduction of risk, or in terms of improving the effectiveness and efficiency of operations. In any organization, it is crucial to balance the cost vs. benefits of controls. The following rules apply in determining the use of new controls:

- If control would reduce risk more than needed, then see whether a less expensive alternative exists.
- If control would cost more than the risk reduction provided, then find something else.
- If control does not reduce risk sufficiently, then look for more controls or a different control.
- If control provides enough risk reduction and is cost-effective also, then use it.

If vulnerabilities exist but with a low probability of occurrence, then it may be wiser and more cost-effective to simply be conscious about the possibility of such losses and their magnitude rather than implement controls, the costs of which may critically impact the profitability of the enterprise. However this is entirely dependent on the risk appetite of the management. Such decisions would be enabled only by a risk assessment exercise which results in identification of the organization's risk profile.

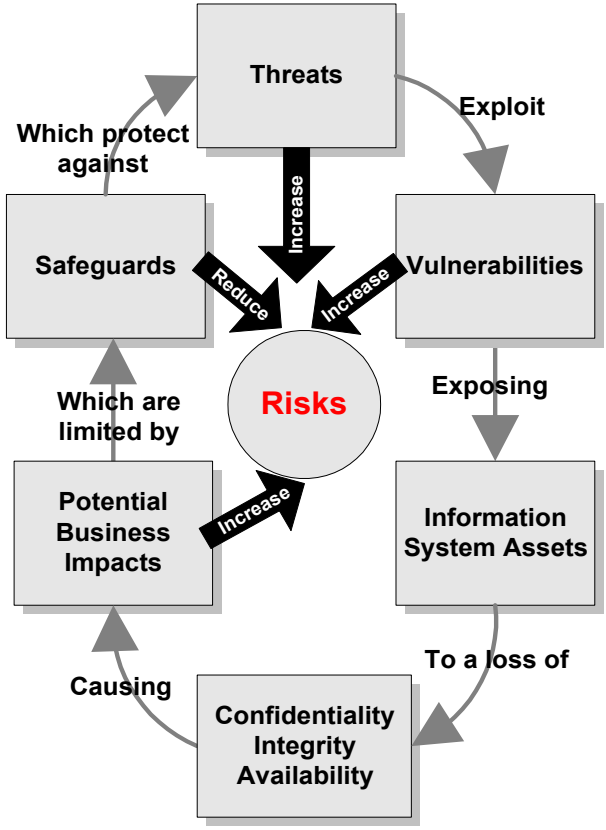


Fig 2.5 Risk Assessment

Acceptable / Residual Risk

Like any other risk, IS Risks cannot be absolutely reduced to nil. Hence the strategy lies in mitigating the risks to an acceptable level. Therefore, it is important for the management, as well as the IS auditor conducting the Risk assessment, to arrive at the Risk profile which would consist of the acceptable risks. A systematic Risk assessment process for identifying, qualifying and quantifying the threat to IS resources is a critical precursor to effective risk management.

Final acceptance of residual risks takes into account:

- Organizational policy
- Risk identification and measurement
- Uncertainty incorporated in the risk assessment approach
- Cost and effectiveness of implementation

To cite an example, fire is a threat that can cause significant harm to the data center of an organisation. The susceptibility of the IS resources such as the facilities, hardware, media etc. is an inherent vulnerability.

The loss that would occur on account of the fire could be termed as risk e.g. destruction of assets, disruption of business, loss of customers etc.

One of the common and simple methods of quantification of risks is as follows:

Risk = Value of Assets X Probability of occurrence of Threat X Vulnerability Factor

In the above given example let us say the value of Computer equipment is Rs.10,00,000 and the probability of occurrence of Fire is 0.75 and the Vulnerability is increased by 1.5 since the data center is constructed using extensive inflammable wooden materials then the risk, in the absence of controls would be

Risk = Rs.10,00,000 X 0.75 X 1.5 = Rs.11,25,000

Controls Assessment

After the risks have been identified, existing controls can be evaluated, or new controls can be designed to ensure that the risk is mitigated to an acceptable level.

Controls are defined as "The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected."

Factors influencing control selection:

- Level of residual risks
- Cost-effectiveness of existing controls
- Acquisition issues –
  - Span of control
  - Lifetime cost
  - Impact on operational efficiency
  - Need for balanced security

In the example given above, the threat of fire cannot be totally eliminated but however the risk of loss from fire can be mitigated by various technical and control measures e.g. prohibiting smoking within the facility, use of fire proof material for construction of the data center facility, etc. Further, the impact of the loss in the event of fire can be reduced by installing smoke detectors and fire suppression systems, fire proof cabinets etc. Further, the company may obtain an insurance for direct loss (such as destruction of IS assets) as well as loss of profits etc. The choices for treatment of the risk from fire available with the organization are either to mitigate, transfer, accept or take the extreme step of not going for the data center. The strategy for risk mitigation would vary from organization to organization, depending on the risk appetite of the organization.

If organization has adequate fire extinguishers, alarms, smoke detectors etc., say the probability is reduced to 0.25, the residual risk would be

Residual Risk = Rs.10,00,000 X 0.25 X 1.5 = Rs. 3,75,000

However it must be appreciated that Risk assessment is an estimation process that involves quantitative and qualitative estimates.

IT Control Objectives

It is the primary responsibility of the management to establish a Risk Management process. Once the acceptable risks have been identified at every process level, it is now the task of the management to define the control objectives so as to ensure that the internal controls to control the IS risks are put in place and remain effective. IT control objectives seek to ensure that IT remains aligned to business strategies and delivers effectively and efficiently to business requirements, and, in particular, that:

- the organization's computing facilities are secure and measures have been taken to ensure continuity of operations
- the environment ensures completeness and accuracy of data processing
- information is accessible only to authorized users – confidentiality, integrity and availability of information is maintained
- effective use of computing resources is made

Defining Control Objectives

Controls are implemented to mitigate risks. Controls always have a cost, but also come with a benefit. In any organization, it is crucial to balance the cost vs. benefits of controls. To do this, it is important that controls should not be implemented merely for sake of controls, but should have a specific purpose. The objective of putting the control in place is termed as control objective. Control Objectives define what is sought to be accomplished by implementing the control and the purpose thereof.

Control Objective is defined as "A statement of the desired result or purpose to be achieved by implementing control procedures in particular IT process or activity". One of the most important steps in an IS audit is to identify the control objectives. The control objectives serve two main purposes:

1. Outline the policies of the organization as laid down by the management
2. A benchmark for evaluating processes and systems

Category of Controls

Controls are classified in a number of ways. Based on the objective with which controls are designed or implemented, controls can be classified as:

Directive Controls: These controls 'direct' an activity towards a desired outcome. Directive controls ensure direction of systems in such a manner as to provide reasonable assurance that the organization's objectives and goals will be achieved. E.g. policies, procedures, guidelines

Preventive Controls: Controls that are designed to prevent an error, omission or malicious act from occurring. For example, use of access control software that

allows only authorized personnel to access sensitive files and processing options.

Detective Controls: Controls that detect an error, omission or malicious act that has occurred and report the occurrence. Detective controls help management identify when preventive controls have broken down and corrective action is needed. For example, an access violation log that contains the details of access that have taken place. Such features are common in most access security systems software.

Corrective Controls: Controls that correct errors, omissions or malicious acts once they are detected. For example, the clean option of an anti-virus program that is programmed to immediately delete malicious codes and scripts once they are detected, before the code can cause damage. Corrective controls also help mitigate the losses where the threats have impacted the assets thus helping in reducing the intensity of the impact.

Existence Controls: Existence controls ensure the continuity of business in the event of a disaster / disruption. E.g. BCP/DRP

Control Category	Examples
Directive Controls	• Security policies, standards, guidelines and procedures • Business Continuity Plan and Disaster Recovery Plan
Preventive Controls	• Security awareness and technical training • Employ qualified personnel • Segregation of duties • Pre-employment background screening and checks • Fences • Security guards • Locks and keys • Badge systems • Biometric access controls • Double door systems • Fire extinguishers • System Documentation • Access control software • Anti-virus software

	• Firewalls • Library control systems • Passwords / PINs • Proximity cards / Smart cards • Encryption • Digital Signatures • Dial-up access control and callback systems • Supervision & monitoring • User registration process for access to IPF • Restriction on use of camera phones, USB drives, CDs etc. in critical IPF • Restriction on eatables or smoking in IPF
Detective Controls	• Motion detectors • Smoke and fire detectors • Video surveillance cameras • Closed-circuit television monitors • Sensors and alarms • Audit Trails • Intrusion Detection Systems • Security reviews and audits • Performance Monitoring • Mandatory Leave / Rotation of duties • Post employment background investigations
Corrective Controls	• Automatic load restoration after diagnosis of power system voltage collapse situations, following large disturbances and/or load increases • Roll-back / roll-forward controls in database • Auto clean feature in anti-virus software
Existence Controls	• Data and software backups • Business Continuity and Disaster recovery arrangements • Power Backup Arrangements

Information Systems Control Framework

The risks coupled with the use of IT need to be effectively managed. However managing the business risks arising from use of technology is often more complex than what it appears. An organization's effective IT Risk Management is not merely putting up firewalls or other sophisticated technologies but is a complex combination of both technical and human controls in the right proportion. Controls, if too complex and involving, can result into competition risk e.g. enforcing an Internet banking user to change his PIN number every 30 days. Security that has significant overhead on functionality can impact business adversely. At the same time lack of poor controls and lack of education of customers on security practices can also lead, for example, to increased credit card frauds, which again will result into loss of business and reputation.

Hence taking the IT control and security of the enterprise as a whole would require an orchestrated set of security technologies, control policies, procedures and practices to be put in place throughout the organization. Evolving an Information Systems Control Framework is effective only with a systematic and structured approach to Information Security, primarily driven by the Information Risk Management process.

A few of the critical requirements for evolving an Information Systems Control Framework includes:

1. Top Management's understanding and support for Information Security as a prime business concern
2. Top Management to allocate adequate budgets for Information Security both in terms of money and human resource
3. Organization wide awareness and understanding of Information as a key business resource that must be protected.
4. Inventorying and classifying information assets.
5. Establishing an effective Risk Management Process aligned with business strategy, as a continuing effort
6. Identify technologies and related enabling resources in use from a risk perspective and the control objectives, including but not limited to:

    a. Personnel Security
    b. Physical and Environmental Security
    c. Management of networks and related communication technologies
    d. Identity Management and Access Control
    e. Controls over Systems Development and Maintenance
    f. Business Continuity Planning

7. Establishing an Organization Structure and fixing accountability for Information Assets
8. Appointing a top level, highly representative governing forum with centralized responsibility for all strategic IS security initiatives and operations
9. Enhancing enterprise wide IS security awareness and training staff on a continuing basis
10. Independent monitoring mechanism for Information Risk Management

The result of the above should translate into an effective Control Environment, usually through the Enterprise wide Security Policy.

Information Systems Risks & Controls – Implications for Financial Auditor

The wide spread use and ongoing development of information systems has enabled the organizations to improve the efficiency of their operations tremendously. On the other hand, it has also introduced enormous amount of risk that needs to be addressed by the management and assessed by the auditor while planning and conducting their audit.

Use of IT does not give rise to new audit objectives nor does it change the same. Though, it essentially forces the auditors to review their audit processes and procedures in the light of changes brought by IT in the ways of doing business and resultant risks. It requires auditors to upgrade their professional skills with the adequate knowledge of Information Systems to apprehend their impact on client's business and audit process in its right spirit.

From the audit point of view, IT brings two vital changes in the organization:

a. New risks introduced or changed level of risks coupled with the use of Information systems, causing organization to deploy appropriate additional controls and
b. New form of records- electronic records, resulting in evaporation of paper trail of transactions

In an IT environment, business events are identified, captured, measured, categorized, aggregated and recorded without any paper documentation. It is the duty of the management to assure their increasingly learned stakeholders and auditors that their electronic records which lead to the generation of financial statements are reliable. In this process they need to convince the auditors that the controls over the information systems being used for processing transactions and generating records are appropriate to the value of the records.

The auditors, in turn, are expected to evaluate various controls in the course of gathering sufficient, reliable and appropriate audit evidence before forming the audit

opinion which calls for a heightened understanding of environment in which the business operates.

As per Auditing and Assurance Standard -5 'Risk Assessments and Internal Controls':"The auditor should obtain an understanding of accounting and internal control systems sufficient to plan the audit and develop an effective audit approach. The auditor should use professional judgment to assess audit risk and to design audit procedures to ensure that it is reduced to an acceptably low level."

It further states that "audit risk" means the risk that the auditor gives an inappropriate audit opinion when the financial statements are materially misstated.

In an IT environment, audit risk is intensified because of the following threats coupled with the use of highly sophisticated electronic systems:

Faded accountability:

Electronic records do not contain any physical marks for the identification of the person making or authorizing the transactions. As a result, individual users cannot be held responsible for such transactions and resultant records. The very nature of e-records raises the possibility of unauthorized transactions.

Moreover, it is very difficult for the auditor to identify and segregate unauthorized transactions and assess their overall impact on the profitability and financial position of the entity. Such unauthorized transactions may be an indication of a fraud already committed or to be committed in near future and are, therefore, to be considered carefully while planning and conducting the audit.

Vulnerability to amendment:

Electronic records are innately easy to amend and amendment is, by default, invisible, as it does not leave any trace of amendment. It results in the auditors being unable to rely on authenticity of records.

Ease of duplication:

It is very easy to duplicate data and files and extremely difficult to differentiate the duplicate from the original. In case of financial transactions, it becomes very important to apply controls in the form of sequence numbers, unique IDs etc. for the prevention and detection of duplicate records, as duplicity may directly result in financial losses.

Evaporated paper trail of transactions:

Information systems process transactions in an invisible form. Only input and output can be available for auditing. The invisible form of transaction processing makes it

vulnerable to unauthorized amendments during processing itself, without leaving any trace of the amendments.

It becomes more risky when organization uses electronic interface with the key suppliers, distributors, banks and other outside agencies and the transaction is processed at two or more ends, because it is very difficult to place assurance on the controls employed by the other partner especially when transaction takes place on untrusted networks.

Remote access:

Internet, by its very nature, is vulnerable to attack as it is open for access to the world at large. Use of Internet further increases the risks.

Placing reliance on outsourced processes:

When any business process is outsourced by the client, it becomes very difficult for the auditor to ensure compliance of security and control standards. It becomes more risky in case of open networks, where it is impossible for one to assess the identity and extent of the involvement of third parties.

Security Controls and Audit Implications:

Many auditors now believe that the audit methodology that was appropriate for the industrial age is not sufficient for the information age.

It is because the responsibility of the auditor with regard to the detection of misstatement arising from fraud and error remains the same irrespective of the added risk of information technology and non-availability of paper evidence. In the IT environment, it is the security concern which becomes worthy of special consideration and causes auditor to re-define the audit procedures to meet responsibilities. Security has three main dimensions: Confidentiality, Integrity and Availability, which have been discussed in previous modules.

Integrity and continued availability of information resources to authorized users can be ensured and confidentiality of sensitive information can be preserved by implementing appropriate security features which have been discussed in the previous chapters.

An auditor should familiarize himself with the type and level of various controls employed by the client and check if these controls are appropriate to the value of information resources. He should thoroughly analyse the security policy with reference to the use of various security measures such as firewalls, encryption, user IDs, passwords, smart cards, digital signatures and certificates to ensure their adequacy and appropriateness for securing critical data.

In addition, the auditor should apply procedures to ensure use of integrity checks, control totals and check digits as detective and corrective controls to protect the organization against unauthorized amendments to data. He should also ensure that a system of generating sequence numbers and randomly generated unique codes is in place to ensure uniqueness of the transactions and to provide a safeguard against duplicity specially in case of monetary transactions.

Auditor should also use audit trail effectively to follow the history of transactions. The review and analysis of audit trail becomes more critical in case of transactions processed in open networks.

The sophisticated IT environment, resultant risks and their implications for auditors can be understood simply with the help of the case study enumerated below.

CASE STUDY

Consider the case of a domestic airlines company say E-Fly Ltd. The company uses e-commerce systems to enable its customers to book air tickets on-line.

E-Fly Ltd. offers three ways of booking e-tickets depending upon the type of its customers:

1. One time customers

Anybody can access the website and book e-tickets by simply giving the details of passengers and making payment through credit card. The e-tickets, so booked, can be printed and used for travel.

In such a case, user can reschedule the flights by entering ticket form serial no. and PNR, a randomly generated 6-digit unique alpha code printed on e-ticket.

2. Registered Users

a. Frequent Fliers

The customer can register themselves as frequent fliers. They are allotted a ten digit unique number called E-Flyer privilege number (EFP no.).

The customer can use EFP no. with their password to login into the system and do the transactions i.e. enquire, book, view, reschedule and cancel the e-tickets. The customers are required to make instant payments through credit card while booking an e-ticket.

The customers gain the advantage of a reward program run by the company which allows customer to have 1 point for every Rs.100 spent on booking e-tickets.

b. Privileged Fliers

The customers in this category are shifted from frequent flier category, when they accumulate 10000 reward points. The privileged fliers are allowed a credit of fifteen days for booking e-tickets up to the specified limit of Rs.100000. They continue to be the part of reward program in the same manner.

Nature of transactions, both financial as well as non-financial, associated risks and respective controls to ensure integrity of the transactions:

a. Booking ticket

One time customers: No logical access controls applicable as no identification of the customer is needed so far as passengers' details are valid, credit card details are verified and payment is secured.

Frequent flier: Though in the case of frequent fliers also, payment is secured at the time of booking tickets, they get the advantage of reward program. Therefore, the identification and authentication becomes essential. User should be asked to enter EFP no. and password.

Privileged Fliers: In addition to the risk with frequent flier transactions, the risk of booking tickets up to Rs. 100000 on credit also exists which may cause immediate financial loss to the company.

Therefore, in addition to the control required in the form of entering EFP no. and password, at the time of booking e-ticket on credit, system may enforce the user to supply some secret information which was asked for at the time of creating EFP account like mother's maiden name, name of first school etc. and to supply credit card no. which can be debited on expiry of fifteen days.

b. Rescheduling flights, no financial adjustment

One time customers: The controls in the form of entering PNR and ticket form serial no. should be in place and work effectively for rescheduling the flights.

Registered users: In addition to the above controls, logical access controls exist in the form of EFP no. and password which protect unauthorized modifications to flight schedule.

c. Canceling e-ticket

One time customers: The controls in the form of entering PNR and ticket form serial no. should be in place and work effectively for affecting cancellation also.

Moreover, auditor should ensure that no cash refunds are allowed and the amount is credited to the same credit card account.

Registered users: In addition to the above controls, logical access controls protect against unauthorized cancellations.

d. Requesting public information e.g. a flight schedule:

The information is not specific to a customer; hence there is no need of identification and authentication. In case, a non-registered user requests company to send schedule by post, though name & address is required, no verification is needed, information desired being open for public.

e. Creating EFP A/c:

The form for creating EFP a/c should incorporate essential field validations like completeness check, range check, limit check, reasonableness check, field interdependency check etc.

The risk of one person having multiple accounts also exists which should be mitigated by unique sequence no. or ID like EFP no.

f. Requesting personal information e.g. monthly activity statement

One time customers: Not applicable

Registered Users: Identification and authentication required. To ensure accountability, integrity and confidentiality of personal information, user should be asked to log-in using his EFP no. and password. It is also essential to log the logging time, nature of request made, logout time etc.

g. Updating personal information

One time customers: Not applicable

Registered Users: The risk of security breach exists by unauthorized user viewing, printing or incorrectly amending personal details, therefore, identification and authentication should be insisted upon. All changes made should also be incorporated into the audit trail.

h. Redeeming / en-cashing award points:

One time customers: Not applicable.

Register Users: The risk of unauthorized user en-cashing / redeeming reward points exists, which may result in loss of customer faith, reputation and even business.

Therefore, strong logical access controls enforcing customer to log-in using his EFP No. and password, are required before the user is allowed to deal with the reward points.

i. Correspondence - enquiry, feedback, complaints etc.

All correspondence should be recorded and made part of audit trail. It should consist of the nature of correspondence, the reply given in case of enquiries and complaints, user ID of the staff member who handled the correspondence, date & time of all correspondences and identity of the user/person who initiated / made correspondence.

An auditor should thoroughly review all customer correspondences particularly complaints as they may provide auditor an insight into the efficiency or otherwise of the controls.

The auditor should also ensure that all critical transactions, financial or non-financial, by or with registered users are intimated to them via e-mail which can work as a detective measure.

QUESTIONS

1. Which of the following is the correct sequence?
   a. Vulnerabilities lead to Threats which, in turn, lead to Risks.
   b. Risks lead to Threats which, in turn, lead to Vulnerabilities.
   c. Vulnerabilities lead to Risks which, in turn, lead to Threats.
   d. Threats lead to Vulnerabilities which, in turn, lead to Risks.

2. Which of the following provides both integrity and confidentiality services for data and messages?
   a. Digital signatures
   b. Encryption
   c. Cryptographic checksums
   d. Granular access control

3. Denial of service attacks compromise which of the following properties of information systems?
   a. Integrity
   b. Availability
   c. Confidentiality
   d. Reliability

4. From a risk management viewpoint, which of the following options is not acceptable?
   a. Accept the risk
   b. Assign the risk
   c. Avoid the risk
   d. Defer the risk

5. Which of the following techniques that organizations are utilizing to help cut costs and improve basic services, are also factors that increase security threats and vulnerabilities?
   a. Access privileges, security rules, policies, and procedures
   b. Interconnected systems, data accessibility, and paperless processing
   c. Security monitoring, reports, and alerts
   d. Security plans, procedures, and standards

6. Which of the following items is most important in controlling the risks of operating a computer-based information system?
   a. A vulnerability inducing a threat
   b. Asset valuation
   c. Threat identification
   d. Vulnerability analysis

7. Risk is the possibility of something adverse happening to an organization. Which of the following steps is the most difficult to accomplish in a risk management process?
   a. Risk identification
   b. Risk assessment
   c. Risk mitigation
   d. Risk maintenance

8. Before assessing a risk, you must first _____.
   a. Identify the risk response action
   b. Identify the risk
   c. Manage the risk
   d. Calculate the risk

9. In addition to protecting important assets, security rules and procedures should _____.
   a. Be cost-effective
   b. Be justified by risk analysis
   c. Support the organizational mission
   d. Apply to everyone in the organization

10. Integrity is protection of data from all of the following except _____.
    a. Unauthorized changes
    b. Accidental changes
    c. Data analysis
    d. Intentional manipulation

11. Risk management is commonly understood as all of the following except _____.
    a. Analyzing and assessing risk
    b. Identifying risk
    c. Accepting or mitigating risk
    d. Likelihood of a risk occurring

12. The absence of a fire-suppression system would be best characterized as a(n) _____.
    a. Exposure
    b. Threat
    c. Vulnerability
    d. Risk

13. When should a risk be avoided?
    a. When the risk event has a low probability of occurrence and low impact
    b. When the risk event is unacceptable – generally one with a very high probability of occurrence and high impact
    c. When it can be transferred by purchasing insurance
    d. A risk event can never be avoided

14. Risk is accepted when _____.
    a. You develop a contingency plan to execute should the risk event occur
    b. You accept the consequences of the risk
    c. You transfer the risk to another party
    d. You reduce the probability of the risk event occurring

15. In Project Risk Management, risk response may include actions to _____.
    a. Reduce the probability of risk events
    b. Change the scope, budget, schedule, or quality specifications of the project
    c. Reduce the consequences or severity of impacts of a potential risk event
    d. All of the above

16. Risk management is defined as the art and science of _____ risk factors throughout the life cycle of a project.
    a. Researching, reviewing, and acting on
    b. Identifying, analyzing, and responding to
    c. Reviewing, monitoring, and managing
    d. Identifying, reviewing, and avoiding

17. The three factors that characterize project risk are _____.
    a. Severity of impact, duration of impact, and cost of impact
    b. Identification, type of risk category, and probability of impact

c. Risk event, risk probability, and the amount at stake
d. Occurrence, frequency, and cost

18. The probability of failure for a project element is often called exposure to risk, or risk exposure. This exposure may be mitigated by taking measures to avoid a particular approach or use of specific technologies. When the risk exposure cannot be reduced through selection of another alternative, the project manager should _____.
    a. Conduct further studies and analyses until a more attractive alternative is found
    b. Disregard the exposure to risk because nothing can be done
    c. Not perform the activities with risk exposure and save the money that would have been spent on them
    d. Establish a contingency plan to overcome any adverse activity, which may include a contingency allowance

19. The project manager may realize that some terms of the contract and project objectives will not be met. It would be costly and time consuming to meet some specifications. The project has a high degree of exposure to risk at this point. Negotiation with the customer to reduce the risk exposure is a means that _____.
    a. Could eliminate all risk to the project and customer at no cost to either party
    b. Could redefine the risk exposure to one of opportunities for both the project and customer
    c. Could result in reduced scope for the project and an improved product for the customer
    d. All of the above

20. Using a firewall to protect the organization's internal network is an example of _____.
    a. Avoiding risk
    b. Mitigating risk
    c. Transferring risk
    d. Accepting risk

21. _____ ensure the continuity of business in the event of a disaster.
    a. Existence controls
    b. Corrective controls
    c. Directive controls
    d. Detective controls

22. In an IT environment, audit risk is intensified because of all of the following except _____.
    a. Faded accountability
    b. Ease of duplication
    c. Difficulty in amendment of records
    d. Evaporated paper trail of transactions

23. If a control reduces a risk more than needed, what should the auditor do?
    a. See whether a less expensive alternative control exists. If no alternative exists, use it.
    b. Find something else.
    c. Use it.
    d. Look for more controls.

24. If value of software is Rs. 5,00,000 and the probability of its being stolen is 0.80, then the risk, in the absence of controls, is _____.
    a. Rs. 4,00,000
    b. Rs. 6,25,000
    c. Rs. 5,00,000
    d. Risk cannot be calculated from the given data.

25. Sensors and alarms are examples of _____ controls.
    a. Directive
    b. Detective
    c. Corrective
    d. Preventive

26. Elimination of all risks is usually _____.
    a. Impractical or impossible
    b. Easy to achieve
    c. Vital to the survival of the company
    d. Recommended by law

27. The risk assessment process involves all of the following except _____.
    a. Take steps to reduce risk to an acceptable level
    b. Assess probability of occurrence of threats
    c. Identify the IT resources
    d. Ascertain the risk profile

28. The risk assessment approach should ensure formal agreement on residual risk. The most critical factor on which this depends is _____.
    a. Risk identification and measurement
    b. Corporate policy
    c. Adopting risk assessment approach of that of the competitor
    d. Cost effectiveness of implementing safeguards and controls

29. Which of the following is a detective control?
    a. Physical access controls
    b. Segregation of duties
    c. Back-up procedures
    d. Audit trails

30. To address the risk of operations staff's failure to perform the daily backup, management requires that the systems administrator sign off on the daily backup. This is an example of risk _____.
    a. Avoidance
    b. Transference
    c. Mitigation
    d. Acceptance

31. A poor choice of passwords and transmission over unprotected communication lines are examples of _____.
    a. Vulnerabilities
    b. Threats
    c. Probabilities
    d. Impacts

32. Which of the following is a detective control in a LAN environment?
    a. File recovery
    b. Contingency plan
    c. Electronic surveillance
    d. Locks and keys

33. Which of the following types of control would an IS auditor look for when a weakness in a system of control is discovered?
    a. Directive
    b. Preventive
    c. Corrective
    d. Detective

34. Which statement best describes the difference between a detective control and a corrective control?
    a. Neither control stops errors from occurring. One control type is applied sooner than the other.
    b. One control is used to keep errors from resulting in loss, and the other is used to warn of danger.
    c. One is used as a reasonableness check, and the other is used to make management aware that an error has occurred.
    d. One control is used to identify that an error has occurred and the other fixes the problems before a loss occurs.

35. Vulnerability of an asset is _____.
    a. Is a weakness that can be accidentally triggered
    b. Is a weakness which can be intentionally triggered
    c. Is a weakness which can be triggered both accidentally or intentionally
    d. Is a weakness of the asset

36. A program check that ensures data entered by a data-entry operator is complete is an example of a _____ control.
    a. Detective
    b. Corrective
    c. Preventive
    d. Redundancy

ANSWERS

1. A	2. B	3. B	4. D	5. B	6. A
7. B	8. B	9. B	10. C	11. B	12. C
13. B	14. B	15. D	16. B	17. C	18. D
19. D	20. B	21. A	22. C	23. A	24. D
25. B	26. A	27. A	28. D	29. D	30. C
31. A	32. C	33. C	34. D	35. C	36. A

Reference Sources

1. CISA Review Manual 2007 by ISACA
2. Information Systems Control and Audit by Ron Weber
3. Information risk management: Defining the scope, methodology and tools by Shon Harris
4. Risk Management Guide for Information Technology Systems
5. Recommendations of the National Institute of Standards and Technology by Gary Stoneburner, Alice Goguen, and Alexis Feringa
6. IT Audit Training for INTOSAI, IT Security Student Notes, March 2007
7. CISA Examination Textbooks Volume 2: Practice Third Edition
8. The CISSP® Prep Guide: Mastering the Ten Domains of Computer Security by Ronald L. Krutz, Russell Dean Vines
9. Information System Audit and Assurance by D.P. Dube and V.P. Gulati
10. The CISA Prep Guide by John Kramer
11. http://www.isaca.org
12. http://en.wikipedia.org/wiki/Risk_management
13. http://www.microsoft.com/events/series/security360octlist.mspx
14. www.apm.org.uk/RiskCertificate.asp
15. http://www.fsa.go.jp/en/ refer/manual/hoken_e/h20.pdf
16. http://www.yancy.org/research/project_management/risk_sample_questions.html

3 IS Audit Techniques & Computer Assisted Audit Techniques

Learning Objectives

To gain knowledge about available audit methods and techniques and reasons for selection of auditing in a computerized information system environment while being aware of the advantages and disadvantages of using CAATs.

- To gain a thorough understanding of the IT controls and security and the impact of IT environment in selecting the appropriate audit methodology.
- To gain knowledge of the various methods, techniques and types of tools for auditing in a computerized environment and IT audits.
- To understand auditing in a continuous audit environment..

Introduction

Today every organization continue to rely on computer to perform the task in effective manner. Initially, conversion from manual system to automatic transaction processing made companies more productive and decrease in cost. CAAT is needed to evaluate the adequacy of automated information system to meet processing needs to evaluate the adequacy of internal controls, and to ensure that assets controlled by those systems are adequately safeguard.This chapter introduces the various audit methodologies adopted by the auditor for auditing Information Systems in a computerized environment. Various auditing standard has been discussed in respect to audit in computerized environment.

1. IT Environment Impact on Audit Methodology

The impact on auditing can be twofold:

a The traditional audit techniques invariably fail to achieve the traditional audit objectives whether it be external financial audits or internal audits. The cost of audits and the time required would be unjustifiably higher. This can be also referred to as Auditing in a computerized environment.

b The emergence of newer risks due to introduction of Information Technology and the very inherent nature of risks that IT suffers from, has also introduced the

need for assurance on related security and controls. This can be referred to as conducting an IT Audits.

While the former is more oriented towards testing the transactions, the latter is more oriented towards controls over the Information Technology and IT environment. Depending on the audit objective, the auditor would have to carefully ascertain the audit methodology and the tools and techniques that would enable the effective and efficient achievement of the audit objectives.

1.1 Auditing in a computerized Information Systems Environment

Information technology has impacted the very manner in which auditing objectiveness is achieved in a computerized environment. In a Computerized Information Systems (CIS) environment , there is significant impact on financial information and the related systems. The manner in which the internal controls affect the financial and related information will vary significantly and it is required of the auditor to gain a good understanding of the manner and the effectiveness with which the controls are applied in such an environment.

Audit test procedures should be so designed as to be effective and at the same time efficient to ensure a timely and cost effective audit. It is important for the audit function entrusted with such an objective to take into consideration the **Auditing and Assurance Standard 29** on "Auditing in a Computerized Information Systems environment, issued by the council of the Institute of the Chartered Accountants of India.

In this regard, the **AAS 29** states:

"The overall objective and scope of an audit does not change in a CIS environment. However, the use of a computer changes the processing, storage, retrieval and communication of financial information and may affect the accounting and internal control systems employed by the entity. Accordingly, a CIS environment may affect:

i. The procedures followed by the auditor in obtaining a sufficient understanding of the accounting and internal control system.
ii. The auditor's evaluation of inherent risk and control risk through which the auditor assesses the audit risk.
iii. The auditor's design and performance of tests of control and substantive procedures appropriate to meet the audit objective.

For the purposes of this AAS, a CIS environment exists when one or more computer(s) of any type or size is (are) involved in the processing of financial information, including quantitative data, of significance to the audit, whether those computers are operated by the entity or by a third party.

The **AAS 29** specifically requires the auditor to consider the effect of a

CIS environment on the audit and requires that:

"The auditor should evaluate, inter alia, the following factors to determine the effect of CIS environment on the audit:

a. The extent to which the CIS environment is used to record, compile and analyse accounting information;
b. The system of internal control in existence in the entity with regard to:
   i. flow of authorised, correct and complete data to the processing center;
   ii. processing, analysis and reporting tasks undertaken in the installation; and
c. The impact of computer based accounting system on the audit trail that could otherwise be expected to exist in an entirely manual system."

1.1.1 Skills and Competence

AAS 29 also stipulates the skills and competence requirements as regards auditing in a CIS environment:

"The auditor should have sufficient knowledge of the computer information systems to plan, direct, supervise, control and review the work performed. The sufficiency of knowledge would depend on the nature and extent of the CIS environment. The auditor should consider whether any specialised CIS skills are needed in the conduct of the audit. Specialised skills may be needed, inter alia, to:

i. obtain sufficient understanding of the effect of the CIS environment on accounting and internal control systems;
ii. determine the effect of the CIS environment on the assessment of overall audit risk and of risk at the account balance and class of transactions level;
iii. and design and perform appropriate tests of control and substantive procedures."

The objective and scope of audit differs with the type of audit i.e. tax audit, statutory audit, internal audit, operational audit etc. Thus, the methodology of audit may vary depending on extent of automation of the audit subject area and related information, and the IT environment at the client's place.

The deployment of IT resources for a specific environment consists of different information technology resources such as information technology facilities, technology (hardware, operating system software, telecommunication software, networking software, multimedia software), application software and business process and organisational structure. As result, numerous types of information technology architectures are possible depending on the extent of automation and combination of information technologies deployed. Hence, there cannot be any standard software for auditing of computerised environments that would enable

achieving all the audit objectives. There are however generalized audit software products that can be used for a significant part of the audit procedures, however it would be the call of the auditor to ascertain the extent of use of such software in his audit work.

Irrespective of the IT environment, the auditor must have certain key competency areas:

a. Althrough understanding of the fundamental concepts of Information Technology.
b. Its key components and
c. Functionality and limitations of such components
d. Risks to the audit subject and controls thereof.

The auditor should gain relevant knowledge about computer hardware, operating systems, networking, database, application software, risks and controls of a computerized environment and office automation software. These should be understood in terms of their impact on functionality, contribution, limitations and risks as regards the work of the auditor. Such knowledge would be a basic requirement before the auditor ventures into auditing in a computerized environment. If the auditor finds himself handicapped with requirement of advanced knowledge requirements as regards IS technologies and controls, it is possible for the auditor to rely on the services of an expert from the auditee oranisation or more preferably an external expert.

1.1.2 Audit of IT Controls and Security

The IT environment also presents with a new set of risks that directly or indirectly impact the business risks. Information Technology suffers from inherent risks that can critically impact the business processes and activities in a significant manner. These risks could result from the lack of various controls that include:

a. Lack of an IS Security Policy Framework, procedures and controls
b. Approach for Control over IT and related resources
c. Risks of outsourcing of IT processes
d. Physical and Environmental Security of IT equipments and related assets
e. Poor controls over Communication and Networking technology and infrastructure
f. Poor controls over systems parameter settings and critical systems files
g. Risks from viruses, hackers and malicious code
h. Poor Access Controls over network access, operating systems access, Application access, monitoring
i. Poor Controls over Software Development Life Cycle
j. Poor Business Continuity Planning

Performing IT audits requires a significantly higher level of knowledge of Information Technology and related controls. More importantly, the auditor should be in a position to appreciate the technology risks and controls with regards to the existing and emerging technologies and the related impacts on the business controls. Performing such audits would require the auditor to use various techniques including both traditional audit procedures such as inquiry and observation and sophisticated IT tools to achieve his audit procedures. The use of tools in such audits needs significant care by the auditor to assure and ensure against any possibilities of any integrity risks to the client's environment.

Technical audits such as network penetration testing would require indepth knowledge of networking technologies, methods of attack and knowledge of tools that are safe and that can be used for achieving the testing objectives. The auditor should also be aware of the protocols to be followed in such cases before commencing the testing and after completion of testing.

2. IS Audit Approach

2.1 Auditing around the Computer- Black Box Approach

Also known as the black box approach, audit around the computer refers to the concept of ignoring what is happening inside the computer and conducting the audit using the inputs and outputs as in manual audit. The objective of the auditor in this case is to understand and gain an assurance as to whether the IT systems, as regards his audit subject, are achieving the required controls or not. This is done by examining the inputs to the computer system(s) and analyzing the outputs from such system. If the output meets the predetermined process and internal control requirements, then the auditor may conclude that the computer system does meet the required control expectations.

While using the black box approach the auditor verifies the existing systems and controls, not the processing of the computer applications. This enables the auditor to gain confidence as regards:

a. Availability of correct and complete data for processing.
b. Error detection and correction.
c. Restart of compilation interrupted by power, mechanical or processing failures without duplicating the entries and records.
d. Checks and controls for accuracy and completeness.
e. Adequate data security against wrong processing, fraud, fire and other calamities.
f. Prevention of unauthorized/invalid amendments, corrections and processing instructions (programs) operating instructions as sequences.
g. Custody of the data files.

However the black box approach also suffers from significant disadvantages:

a. The auditor can only gain reasonable satisfaction as regards a limited set of control objectives.
b. Cannot be used where the audit subject involves complex logic and controls
c. Cannot be used in a highly complex integrated controls environment such as an ERP.

2.2 Auditing through the computer - Whitebox approach

With the introduction of computerisation, traditional audit trails have disappeared. It is possible that the entire processing cycle occurs within the computer systems, with a single transaction that spans across organizational boundaries (such as vendors, agents etc). is completed by a complex set of networked computing systems.

It thus becomes necessary for the auditor to examine the logic and internal controls embedded in the application and related software. The auditor may also need to verify the technical accuracy of the systems, checks, controls, error detection and data security procedures. This would often require the auditor to use Information technology to achieve the auditing objectives effectively in such an environment;

For e.g. to examine the purchase cycle in an ERP environment, the auditor would need to use various computer assisted audit techniques such as extracting, analysing and querying on the transaction data to ascertain the effectiveness of controls, examining the parameter settings etc.

In such a situation, examination and testing of computer implemented controls becomes mandatory for an auditor. In some cases, the high volume and complexity of transactions might necessitate the use of powerful IT tools.

The auditor performs various kinds of test on data stored in the system. They are:

a. varifying extensions
b. examinations of data and records that ensure quality, completeness, consistency and correctness
c. data comparision
d. summerizing and regrouping of data
e. audit sample checking and selection
f. printing the request

Computerised auditing techniques refers to the approach of reviewing the internal controls in the computerised environment, which usually involves the use of Computer Assisted Audit Techniques (CAATs). An understanding of the IT environment, its components and their operations is thus necessary. The objective is

to understand the system and the processes and identify the risks and controls at the system or process level itself. It is also essential to know the implications of how the controls are set up in the computerised environment at the various levels of hardware, operating system software, database, application software and access to these by the staff as per authorizations.

3. Computer Assisted Audit Techniques

CAAT is a significant tool for auditors to gather evidences independently. It provide a mean to gain access and to analyse data for a predetermined audit objective, and report the audit findings with evidences. It helps the auditor to obtain evidence directly on the quality of records produced and maintained in the system.The quality of the evidence collected gives reassurance on the quality of the system processing such transactional evidences.

Depending on the audit objective and approach to audit, the auditor would need to decide on the extent of computer assisted audit techniques.The CAATs generally involve running the auditor's software under a controlled environment to verify the quality of data and controls in the computing environment. The auditor can potentially perform different kinds of tests, both addressing the compliance and substantive testing objectives, with the use of CAATs if the client's data is available to the auditor or the access to client's networks and IT resources are made available to the auditor. Hence CAATs are helpful in collection of valuable audit evidence, analysis of client data to identify weaknesses and for reporting. Thereby the CAATs also enable the auditor to better manage his audit efficiently and qualitatively.

3.1 Needs for CAAT

During the course of the audit an IS auditor should obtain sufficient, relevant and useful evidence to effectively achieve the audit objectives. The audit findings and conclusions have to be supported by appropriate analysis and interpretation of this evidence. Computerised information processing environments pose a challenge to the IS auditor to collect sufficient, relevant and useful evidence, since the evidence exists on magnetic media and can be examined only by using CAATs. With systems having different hardware and software environments, different data structure, record formats, processing functions, etc., it is almost impossible for the auditors to collect evidence and analyse the records without a software tool. Owing to resource constraints and the ever changing audit objectives, it is almost impossible to quickly develop audit capabilities, without using audit software like CAATs.

The ICAI Guidance note on CAAT describes CAATs as important tools for the auditor in performing audits. CAATs may be used in performing various auditing procedures including the following:

a. Tests of details of transactions and balances, for example, the use of audit software for recalculated interest or the extraction of invoices over a certain value from the computer records.
b. Analytical procedures, for example, identifying inconsistencies or significant fluctuations.
c. Tests of general controls, for example testing the setup or configuations of the operating system or access procedures to the program libraries or by using code comparison software to check that the version of the program in use is the version approved by management.
d. Sampling programs to extract data for audit testing
e. Tests of application controls, for example, testing the functionality of a programmed control
f. Reperforming calculations performed by the entity's accounting system.

However the auditor, while selecting the CAAT is faced with certain critical decisions that he may be required to make, while balancing on the quality and cost of audit:

a. Use the audit software developed by the client
b. Design and develop his own audit software
c. Use a standard Off the shelf Generalised Audit Software

The first two options require the auditor to be technically competent in programming and its methodology, which may not be his area of expertise. Computer audit software, also known as Generalised Audit

Programs (GAS) which are readily available. The auditor do not require much expertise knowledge to be able to use for auditing purpose

3.2 Types of CAATs

The various types of CAATs can be categorized as follows:

i. Generalised Audit Software
ii. Specialised Audit Software
iii. Utlity Software

A brief description of the types of software is given below:

i. Generalised Audit Software (GAS)

Computer audit software may be defined as: "The processing of a client's live files by the auditor's computer programs". Computer audit software may be used either in compliance or substantive tests. Generalised Audit software refers to generalized computer programs designed to perform data processing functions such as reading data, selecting and analyzing information, performing calculations, creating data files

and reporting in a format specified by the auditor. The use of Generalised Audit Software is perhaps the most widely known computer assisted audit technique. GAS has standard packages developed by software companies exclusively for auditing data stored on computers. These are economical and extensively used by auditors the world over. Available off the shelf, GAS can be used for a wide range of hardware, operating systems, operating environments and database. GAS generally achieves the most common data testing requirements which are common irrepective of the type of business or the kind of IT environment e.g. identifying cash payments in excess of the limits stipulated in the Income Tax Act, identification of pending receivables over 180 days, identifying ghost employees in payroll, identifying duplicate payments for supplier invoices, identifying employees with more than one login id etc. of the above, the Generalised Audit Software are the most widely used for transaction audits and also for testing some systems controls. With their capabilities for achieving the traditional manual audit procedures

in a highly effective and efficient manner, GAS products are an essential tool for every Chartered Accountant desiring to conduct a transaction or business controls audit. Hence it is important for the auditor to have detailed knowledge about the features, selection, functionality, limitations and audit approach with the use of GAS.

Typical Operations Using GAS

Generalised Audit Software (GAS) refers to standard software, which can directly read and access data from various database platforms, flat file systems and ASCII formats. This software has all the features of mathematical computations, stratification, statistical analysis, sequence check, duplicate check, recomputations, etc. Auditors can thus directly access the data stored in a computer and undertake various types of mathematical computations and statistical analysis. GAS cannot perform the audit but can facilitate selection and processing the information as per the clients' requirements. The two most commonly used GAS are ACL (Audit Command Language) and IDEA (Interactive Data Extraction Analysis). Information about these packages can be accessed at **www.acl.com** and **www.idea.com**.

Typical operations using GAS include :

a. Sampling Items are selected following a value based or random sampling plan.
b. Extraction Items that meet the selection criteria are reported individually.
c. Totalling The total value and number of items meeting selection criteria are reported.
d. Ageing Data is aged by reference to a base date
e. Calculation Input data is manipulated prior to applying selection criteria

Advantages of using CAATs

Independence of Data

The packages are independent of the data they retrieve and analyse. The user merely needs to define the data structures and specify simple selection criteria.

Portability of GAS and data

GAS can be installed on a PC or laptop and then used to run on live data on the computing environment of the client, by using the PC/Laptop as a dedicated audit terminal. It can be deployed for analysis on any personal computer. This feature facilitates easy extraction and analysis on any platform.

Analysis of data

The main purpose of such packages is to allow testing and analysis of data to achieve the control or audit objectives, with minimum knowledge of IT and specialised programming techniques. GAS usually have a GUI and very user friendly with menu driven command structure.

Certain functions are automated to the extent that one command can carry out a fairly complex task—for example, the calculation of averages, means and other meaningful values. Fairly complex applications can be written, even to the extent of simulation of the processing of a particular business application running live, to enable the auditor or control professional to verify accuracy and completeness of the data processing and related controls.

Statistical Sampling

GAS is most commonly used in the selection of statistical samples for substantive testing. Various statistical functions and selection routines are automated and simple even for a non specialist.

ii. Specialised Audit Software(SAS):

Specialised Audit software, unlike GAS, is written for special audit puroses or targeting specialized IT environments. The objective of these software to achieve special audit procedures which may be specific to the type of business, transaction or IT environment e.g. testing for NPAs, testing for UNIX controls, testing for overnight deals in a Forex Application software etc. Such software may be either developed by the auditee or embedded as part of the client's mission critical application software. Such software may also be developed by the auditor independently. Before using the entity's specialized audit software, the auditor should take care to get an assurance on the integrity and security of the software developed by the client..

iii. Utility Software:

Utility software or utilities, though not developed or sold specifically for audit are often extremely useful and handy for conducting audits. These utilities usually come as part of office automation software, operating systems, database management systems or may even come separately. Utilities are useful in performing specific system command sequences and are also useful in performing common data analysis functions such as searching, sorting, appending, joining, analysis etc. Utilities are extensively used in design, development, testing and auditing of application software, operating systems parameters, security software parameters, security testing, debugging etc.

a. File comparison - A current version of a file for example, is compared with the previous year's version, or an input file is compared with a processed file.
b. Production of circularisation letters.

3.3 Functionalaties of CAATs

CAATs facilitate auditors to use high level problem solving software to invoke functions to be performed on data files. Typical functions of GAS which facilitate CAAT are :

a. File Access - helps to read different record formats and file structures.
b. File Re-organisation - enables indexing, sorting, merging, linking with another file, etc.
c. Data Selection - Facilitates global filtration conditions, selection cri- teria, etc.
d. Statistical functions - Allows sampling, stratification, frequency analysis, etc.
e. Arithmetical functions - Facilitates arithmetic operators and functions.

Typical Steps in using GAS

i. Define the audit objectives
ii. Identify the tests that the package can undertake to meet the objectives.
iii. Make out the package input forms for the tests identified.
iv. Compile the package on the computer, clearing reported edit errors.
v. If a programmer has been adding coded routines to the package to fill out the input forms or to advise, the programmer's work must be tested.
vi. Obtain copies of the application filed to be tested.
vii. Attend the execution of the package against these copy files.
viii. Maintain security of the copy files and output until the tests have been fully checked out.
ix. Check the test results and draw audit conclusions.
x. Interface the test results with whatever subsequent manual audit work to be done.

3.4 Selecting, implementing and using CAATs

Computer Assisted Audit Techniques (CAATs) are a significant tool for auditors to gather evidence independently. CAATs provide a means to gain access and analyse data for a predetermined audit objective and to report audit findings with evidence. They help the auditor to obtain evidence directly on the quality of the records produced and maintained in the system. The quality of the evidence collected confirms the quality of the system processing.

CAAT Usages

CAATs could be used for various types of audit, which involve direct access, analysis and interrogation of data. Usage of CAATs can be broadly categorised as:

i. Test of details of transactions and balances
ii. Analytical review of procedures.
iii. Compliance test of IS general controls
iv. Compliance test of application controls
v. Penetration testing.

CAATs - Effective usage methodology

The usage of CAATs will be effective if the following methodology is

a. adopted
b. Walk through the system and identify the areas off weakness.
c. Perform compliance tests and evaluate the results.
d. If the results necessitate substantive testing, use CAATs to get evidence.

Guidelines on decision factors for using CAATS

When planning the audit, the IS auditor should consider an appropriate combination of manual techniques and CAATs.The factor to be considered includes

a. Computer knowledge, expertise, and experience of the IS auditor
b. Availability of suitable CAATs and IS facilities
c. Efficiency and effectiveness of using CAATs over manual techniques
d. Time constraints
e. Integrity of the information system and IT environment
f. Level of audit risk.

Steps for effective use of CAATs

Normally, audit conclusions and recommendations are based on the evidence collected by auditors. Audit conclusions based on incorrect and/or inappropriate evidences will reduce the credibility of the audit itself. Hence some of the steps

associated with effective use of CAATs include:

i. Set the audit objectives of the CAATs
ii. Determine accessibility and availability of organisation's IS facilities programs/systems and data.
iii. Define the transaction types to be tested
iv. Define procedures to be undertaken (e.g. statistical sampling, recalculation, confirmation etc).
v. Define output requirements
vi. Determine resource requirements, i.e., personnel, computers, CAATs, processing environment (Organisation's IS facilities or audit IS facilities)

    a. Obtain access to the organisation's IS facilities, programs/systems, and data, including file definitions.
    b. Refine the estimates of costs and benefits
    c. Ensure that the use of the CAAT is properly controlled and documented.
    d. Arrange the administrative activities activities, including the necessary skills and computer facilities.
    e. Execute the CAAT application
    f. Evaluate the result.

vii. Document CAATs to be used, including objectives, high level flow charts, and run instructions.

Performance Steps

a. Obtain written read only access to IS facilities, systems and data
b. Obtain file/table definition/structure
c. Perform audit procedures using CAATs
d. Review results obtained from CAATs to verify
e. Perform reconciliation of data
f. Check reasonableness of output
g. Confirm logic, parameters and characteristics of data
h. Document the steps undertaken

Cautions of use of CAATs. Ensure integrity, reliability and security of the CAATs before selecting.

a. Assure integrity of information Systems and security environment
b. Assure the confidentiality and security of data as required by the client's
c. Take into confidence client's IS staff of for usage of CAATs.

Use of Spreadsheets as an audit tool Spreadsheets are an effective and easy to use tool for the auditor to achieve audit and analytical procedures. Spreadsheets enable querying

on a set of data based on the criteria and filters set by the auditor. Spreadsheets offer features which can assist the auditor in efficient achievement of audit procedures. Many of the audit procedures for querying of transactions or for analyzing data relating to testing of controls require the auditor to define criteria. The subject data is tested against defined criteria. Some of these features include the following:

- **Join:** The data to be tested for a specified criteria may arise from more than one database. Hence this may require joining of files extracted from two or more different databases. Spreadsheets offer various features to joining and linking data files into single files.
- **Sort:** Sorting of subject data based on one or more data fields is often a requirement as part of various procedures to analyse trends,determine exceptions . Spreadsheets provide dialog boxes for simple to complex sorting functions
- **Filter:** Most spreadsheets provide for simple to very complex filtering of data based on multiple conditions or criteria, which is often useful in achieving searches based on complex audit criteria.
- **Summarise:** While working on large data files and working sheets, spreadsheets enable the summarizing of voluminous findings, relevant and useful for purposes of presentation.
- **Graphs and Charts:** Representation of findings using graphs and charts is extremely useful in conveying complex issues in a simple manner. Most spreadsheets provide a range of features that enable creating various types of graphs and charts, which can be linked to representative data.
- **Pivot Tables:** Pivot Tables are works sheets Erroneous Overwriting of worksheets one of the most useful tools for data analysis since they allow multi-dimensional analysis of data.
- **Macros:** Where a series of spreadsheet menu based command and instruction structures are required, macros enable repeated execution of long and complex instruction routines to be easily achieved using macro functions.

Risks associated with use of spreadsheets

The auditor should also be aware of the risks of using spreadsheets for analytical procedures and use of evidence arrived therefrom, e.g.:

- Errors in Input values leading to erroneous results
- Errors in logic and formulae leading to erroneous results
- Incorrect reference and range
- Problems associated with complex worksheets
- Improper or incorrect linking of works sheets required for evidence

The auditor should institute adequate controls to safeguard his work against the above risks.

The following are some examples of CAATs, which can be used to collect evidence :

- ACL, IDEA etc.
- Utility Software such as Find, Search, flowcharting utilities
- Spreadsheets such as Excel
- SQL Commands, OS commands
- Third party access control software
- Application systems
- Options and reports built in as part of the application/systems software
- Performance monitoring tools
- Network management tools, OS utilities
- High end CAATs
- RSAREF, DES, PGP
- TCP Wrapper, SOCKS, TIS Toolkit
- COPS, Tripwire, Tiger
- ISS, SATAN, etc.

4. Other Computer Assisted Audit Techniques

4.1 CAATs used in SDLC

i. Flowcharting Software

The processing logic of the programs may also be understood by examining the program flowcharts. This tool also calls for expertise in data processing. When writing a computer program, the programmer usually constructs a logic chart that is also useful, once the program is written, to assist in an appreciation of how the system works. This process can also help in identifying control procedures and system changes. Flowcharts are also useful in designing of audit software.

ii. Test Data (test packs)

The use of audit test data (test packs) may be defined as: "The controlled application of an auditor's test data (live or dummy) to client application program procedures". The expression "test pack" is however, normally, reserved for situations where conventional testing is not practical (for example, where there is a loss of audit trail). A small sample of data is processed through the computer and the output is compared with manually generated output using the same data. It requires little computer expertise, at least for simple batch systems. The auditor should take adequate care in designing the test pack and should be designed with the objective of making the application software fail.

iii. Test Data generator

When test data or test packs are required to be generated, this may require a set of numerous data that tests a range within each parameter value. This requires a significant effort, if done manually. Test data generators are software packages which can be used either to construct data to be tested or to create dummy master files. The users describe the characteristics of the data required and the software generates a file of appropriate set of data and produces a listing. The data so generated can then be used as a "test pack". Test data generators are cost effective especially, when large volumes of test data are needed for testing.

iv. Program Comparison

This tool compares two different versions of the same program to ensure that they are identical. Software is available for this purpose has both source code and the object code.

- A program implemented with one testing of the software and than accepted by the user.
- Programs installed at different locations. Recompiling the source code and comparing them with the installed version.
- The presently installed version with a copy of the auditor's previously tested version.

v. Program Code Analysis

Program code analysis also known, as program listing review is another tool, which can be used for analysis software code. A listing of the program code is obtained and reviewed for logic. Though not strictly a computer assisted technique, program code analysis involves looking at the original instructions to the computer (the source program listing) to verify whether particular program procedures exist. Such findings are than corroborated using the test data. The technique is complex and requires a high level of technical skill for effective application.

vi. Tracers

Tracing Software and utilities are extremely useful in understanding the trail of controls as they are executed by the various program lines in the application. Using a predetermined or preidentified set of input data, the tester or auditor can trace through the action of various instruction sets on the memory variable(s) marked for tracing.

vii. Program (Parallel) Simulation

This consists of a separate computer application that performs the same functions as those used by the installed program. It uses the same data and files

and the results are similar to those produced by the installed program. Conceptually, it is akin to auditing around the computer. Parallel simulations may be done in any programming language. Using GAS nontechnical persons can create parallel programs with little effort. Speed of execution is not a criterion, as the parallel simulation is done only on a one off basis not as a regular production run. The objective is to test the adequacy of underlying controls that are expected to be embedded in the live computing environment. Parallel simulation is useful where the auditor may not have access to the live environment of the auditee.

4.2 CAATs used for systems testing

i Utility Program

Most hardware manufactures provide software, known as "Utility programs". They are designed to perform common tasks such as copying or sorting files or printing details of records for visual inspection. These programs may be useful in compliance or substantive tests. They may for instance, be employed to produce copies of data files required for interrogation purposes or to print out internal file labels, which can determine whether the correct file has been obtained.

ii. Operating Systems and DBMS utilities

Auditors can also review the features of the operating systems and DBMS used so as to understand and use the powerful utilities to meet the requirements of auditors. In recent years, auditors have discovered that the powerful fourth generation languages contain many functions found in the GAS packages. Besides, they make it possible to download the needed data on to a microcomputer for further processing.

iii. Statistical Techniques

Auditors may also consider using statistical procedures both for sampling items from a single database or shared databases. Some spread sheet software contains a limited amount of statistical capability, but an auditor desirous of carrying out extensive statistical analysis may need software or an utility to do so.

5. Continuous Auditing Approach

Continuous auditing is a process through which an auditor evaluates the particular system(s) and thereby generates audit reports on real time basis. Continuous auditing approach may be required to be used in various environments. Such environments usually involve systems that are 24*7 mission critical systems.

Enabling continuous auditing enables an independently developed or embedded set of audit software that continuously audits the transactions. The reports from such

software provide real time detection of audit criteria and are capable of initiating or triggering corrective action before the risk gets out of control.

In the traditional method, the scope for market influence on the information contained in the audit report is less due to

1. The time gap between the audit and reporting
2. The deficiencies identified in the control systems can be rectified even by the management during the time gap.

5.1 Difference between continuous monitoring and continuous auditing

Continuous monitoring systems (CMS) enable organizations to monitor and obtain the information relating to systems, data types and process performance. For instance, the CMS developed to evaluate the accounts payable activities enables detection of double payments and details of such transactions by querying on invoice and related files

CMS is different from continuous auditing in the following manner:

1. Audit report: it does not generate any audit report.
2. Evidence: The opinion expressed in the report must be backed by substantive evidence and should be obtained from direct observation. The information gathered through CMS is indirect, as it is not obtained from direct observation. However, monitoring and testing the processes and systems by an IS auditor result in direct and independent monitoring under the control of the auditor.

5.2 Feasibility of Continuous Auditing

Continuous Auditing is generally not popular due certain problems associated with the implementation and management of continuous auditing techniques and tools:

- Risks of continuous auditing tools interfering with the integrity of application software running in live environment
- Continuous Auditing software may consume significant IT resources of the organisation thereby affecting the performance of IT for routine business functions, the impact of which may be felt by the customer ultimately
- Technological complexity associated with using such technologies.
- Cost of implementation of such techniques vs. the benefit

However feasibility of implementing continuous auditing systems would depend on the business risk that the auditee faces due to continuous process systems wherein an error or crime could get of control if not detected in a timely manner. Examples: an airline ticketing system may be applying significantly incorrect tariff to reservations, or, results of actions of hackers in online trading systems to defeat the controls of the systems for gains

5.3 Techniques for Continuous Auditing

i. Snapshot

Most applications follow a standard procedure whereby, after taking in the user input they process it to generate the corresponding output. Snapshots are digital pictures of procedures of the console that are saved and stored in the memory. Procedures of the console refer to the application procedures that take input from the console i.e. from the keyboard or the mouse. These procedures serve as references for subsequent output generations in the future.

Typically, snapshots are implemented for tracing application software and mapping it. The user provides inputs through the console for processing the data. Snapshots are means through which each step of data processing (after the user gives the input through) is stored and recalled.

Let us consider, for example, a banking transaction. Numerous transactions are effected and processed by various application systems in a banking environment. While all applications are tested before being deployed, in an integrated computing environment, a cash withdrawal at the ATM may be processing by more than one software working in a integrated manner. In the event of some errors in transactions being detected or suspected, snapshot software installed as part of the production environment would continuously take pictures of transactions passing a particular control point e.g. instruction set executed in the memory of the ATM machine for processing withdrawal. Hence the error in code/ instruction can be pinpointed and identified by the snapshot software.

Implementation

Specifically designed snapshot software applications or audit tools (incorporating snapshot software) are used for tracking the results of application of all or specified steps in the application process. The snapshot software takes a "digital image" of the user input and the corresponding intermediate state of results or output. Subsequently, digital images or snapshots taken by the snapshot software are stored in a separate file to be retrieved later. The digital images may also be distributed to selected servers and client systems for further processing. Snapshots may either be triggered manually by the User/Auditor by specifying the transactions in respect of which the snapshot needs to be taken or may be programmed to be triggered based on time or a occurrence of a particular event.

Snapshots are employed in the following:

- They are used for analysing and tracking down the flow of data in an application program, so as to know the underlying logic of the data

processing software.

- For documenting the logic, input/output controls (or conditions) of the application program and the sequence of processing.

Snapshots are generally deployed for tracking down the reasons for any disruption in the functioning of application or system software like operating system or database system.

ii. Integrated Test Facility (ITF)

Integrated Test Facility (ITF) is a system in which a test pack is pushed through the production system affecting "dummy" entities. Hence this requires dummy entities to be created in the production software. For example, the auditor would introduce test transactions that affect targeting dummy customer accounts and dummy items created earlier for this testing purpose. The approach could also involve setting a separate dummy entity using the application software in the live environment. ITF is useful in identifying errors and problems that occur in the live environment and that cannot be traced in the test environment. However the disadvantage in using ITF is that the dummy transactions also append to the live database and hence will impact the results and reports drawn from the live database. It will therefore, be necessary to delete the test transaction from the system once the test is performed. As with all test packs, the output produced is compared with predicted results. This helps to determine whether the programmed procedures being tested are operating correctly.

iii. System Activity File Interrogation

Most computer operating systems provide the capability of producing a log of every event occurring in the system, both user and computer initiated. This information is usually written to a file and can be printed out periodically. As part of audit testing of general controls, it may be useful for the auditor to review the computer logs generated at various points to build an audit trail. Wherever possible, unauthorised or anomalous activity would need to be identified for further investigation. Where a suitable system activity file is retained on magnetic media, one can select and report exceptional items of possible audit interest such as unauthorised access attempts, unsuccessful login attempts, changes to master records and the like.

Similar implementation is also possible by embedding special audit software in application software that maintains continuous transaction logs at various points in the application software. This technique is also referred to as the Systems Control Audit Review File. The files can be further analyzed to determine deviations and improper transactions.

iv. Embedded Audit Facilities

Embedded audit facilities consist of program audit procedures, which are inserted into the client's application programs and executed simultaneously. The technique helps review transactions as they are processed and select items according to audit criteria specified in the resident code, and automatically write details of these items to an output file for subsequent audit examination.

This technique generally uses one or more specially designed modules embedded in the computer application system to select and record data for subsequent analysis and evaluation. The data collection modules are inserted in the application system or program at points predetermined by the auditor. The auditor also determines the criteria for selection and recording. Automated or manual methods may be used to analyse the data later. This is intended to highlight unusual transactions, which can be later taken up for scrutiny.

v. Continuous and Intermittent Simulation

With significant advancements in technologies, business systems are increasingly driven by client-server systems with distributed computing and databases. The components of such systems are networked generally over geographically disparate locations. This has resulted in the need for auditing systems that not only enable continuous auditing of transactions but also have a low overhead on the IT resources of the auditee but without compromising on the independence of such systems. This has resulted in the use of continuous auditing techniques that the client-server environment to enable independent simulation of "suspect" transactions independently by the simulation audit software under the control of the auditor but using the online data of the auditee awaiting to be written to the database.

6. Annexure 1: ICAI Guidance Note on Computer Assisted

Audit Techniques (CAATs)

6.1 Introduction

i. The overall objectives and scope of an audit do not change when an audit is conducted in a computer information systems (CIS) environment. The application of auditing procedures may, however, require the auditor to consider techniques known as Computer Assisted Audit Techniques (CAATs) that use the computer as an audit tool for enhancing the effectiveness and efficiency of audit procedures. CAATs are computer programs and data that the auditor uses as part of the audit procedures to process data of audit significance, contained in an entity's information systems.

ii. The purpose of this Guidance Note is to provide guidance in the use of CAATs. This Guidance Note describes computer assisted audit techniques including computer tools, collectively referred to as CAATs. This Guidance Note applies to all uses of CAATs when a computer of any type or size is involved whether that computer is operated by the entity or by a third party.

6.2 Description of Computer Assisted Audit Techniques (CAATs)

i. Computer Assisted Audit Techniques (CAATs) are important tools for the auditor in performing audits. CAATs may be used in performing various auditing procedures, including the following:

- tests of details of transactions and balances, for example, the use of audit software for recalculating interest or the extraction of invoices over a certain value from computer records;
- analytical procedures, for example, identifying inconsistencies or significant fluctuations;
- tests of general controls, for example testing the setup or configuration of the operating system or access procedures to the program libraries or by using code comparison software to check that the version of the program in use is the version approved by management;
- sampling programs to extract data for audit testing;
- tests of application controls, for example, testing the functioning of a programmed control; and
- reperforming calculations performed by the entity's accounting systems.

ii. CAATs allow the auditor to give access to data without dependence on the client, test the reliability of client software, and perform audit tests more efficiently. CAATs are computer programs and data that the auditor uses as part of the audit procedures to process data of audit significance contained in an entity's information systems. CAATs may consist of package programs, purpose written programs, utility programs or system management programs. Regardless of the origin of the programs, the auditor substantiates their appropriateness and validity for audit purposes before using them. A brief description of the programs commonly used is given below.

- **Package Programs** are generalized computer programs designed to perform data processing functions, such as reading data, selecting and analyzing information, performing calculations, creating data files and reporting in a format specified by the auditor.
- **Purpose Written Programs** perform audit tasks in specific circumstances. These programs may be developed by the auditor, the

entity being audited or an outside programmer hired by the auditor. In some cases, the auditor may use an entity's existing programs in their original or modified state because it may be more efficient than developing independent programs.

- **Utility Programs** are used by an entity to perform common data processing functions, such as sorting, creating and printing files. These programs are generally not designed for audit purposes, and therefore may not contain features such as automatic record counts or control totals.
- **System Management Programs** are enhanced productivity tools that are typically part of a sophisticated operating systems environment, for example, data retrieval software or code comparison software. As with utility programs these tools are not specifically designed for auditing use and their use requires additional care.

Details of some of the techniques used are mentioned in the Appendix.

6.3 Considerations in the Use of CAATs

i. When planning an audit, the auditor may consider an appropriate combination of manual and computer assisted audit techniques. In determining whether to use CAATs, the factors to consider include:

- the IT knowledge, expertise and experience of the audit team;
- the availability of CAATs and suitable computer facilities and data;
- the impracticability of manual tests;
- effectiveness and efficiency; and
- time constraints.

Before using CAATs the auditor considers the controls incorporated in the design of the entity's computer systems to which CAAT would be applied in order to determine whether, and if so, how, CAATs should be used.

6.4 IT Knowledge, Expertise and Experience of the Audit Team

i. Auditing and Assurance Standard (AAS) 29, "Auditing in a Computer Information Systems Environment" deals with the level of skill and competence the audit team needs to conduct an audit in a CIS environment. It provides guidance when an auditor delegates work to assistants with CIS skills or when the auditor uses work performed by other auditors or experts with such skills. Specifically, the audit team should have sufficient knowledge to plan, execute and use the results of the particular CAAT adopted. The level of knowledge required depends on "availability of CAATs" and "suitable computer facilities".

6.5 Availability of CAATs and Suitable Computer Facilities

i. The auditor considers the availability of CAATs, suitable computer facilities and the necessary computer based information systems and data. The auditor may plan to use other computer facilities when the use of CAATs on an entity's computer is uneconomical or impractical, for example, because of an incompatibility between the auditor's package program and entity's computer. Additionally, the auditor may elect to use their own facilities, such as PCs or laptops.

ii. The cooperation of the entity's personnel may be required to provide processing facilities at a convenient time, to assist with activities such as loading and running of CAAT on the entity's system, and to provide copies of data files in the format required by the auditor.

6.6 Impracticability of Manual Tests

i. Some audit procedures may not be possible to perform manually because they rely on complex processing (for example, advanced statistical analysis) or involve amounts of data that would overwhelm any manual procedure. In addition, many computer information systems perform tasks for which no hard copy evidence is available and, therefore, it may be impracticable for the auditor to perform tests manually. The lack of hard copy evidence may occur at different stages in the business cycle.

- Source information may be initiated electronically, such as by voice activation, electronic data imaging, or point of sale electronic funds transfer. In addition, some transactions, such as discounts and interest calculations, may be generated directly by computer programs with no specific authorization of individual transactions.
- A system may not produce a visible audit trail providing assurance as to the completeness and accuracy of transactions processed. For example, a computer program might match delivery notes and suppliers' invoices.
- In addition, programmed controlled procedures, such as check ing customer credit limits, may provide hard copy evidence only on an exception basis.
- A system may not produce hard copy reports. In addition, a printed report may contain only summary totals while computer files retain the supporting details.

6.7 Effectiveness and Efficiency

i. The effectiveness and efficiency of auditing procedures may be improved by using CAATs to obtain and evaluate audit evidence. CAATs are often an

efficient means of testing a large number of transactions or controls over large populations by:

- analyzing and selecting samples from a large volume of transactions;
- applying analytical procedures; and
- performing substantive procedures.

ii. Matters relating to efficiency that an auditor might consider include:

- the time taken to plan, design, execute and evaluate CAAT;
- technical review and assistance hours;
- designing and printing of forms (for example, confirmations); and
- availability of computer resources

iii. In evaluating the effectiveness and efficiency of CAAT, the auditor considers the continuing use of CAAT application. The initial planning, design and development of CAAT will usually benefit audits in subsequent periods.

6.8 Time Constraints

i. Certain data, such as transaction details, are often kept for a short time and may not be available in machine readable form by the time auditor wants them. Thus, the auditor will need to make arrangements for the retention of data required, or may need to alter the timing of the work that requires such data.

ii. Where the time available to perform an audit is limited, the auditor may plan to use CAAT because its use will meet the auditor's time requirement better than other possible procedures.

6.9 Using CAATs

i. The major steps to be undertaken by the auditor in the application of CAAT are to:

a. set the objective of CAAT application;
b. determine the content and accessibility of the entity's files; (c) identify the specific files or databases to be examined;
c. understand the relationship between the data tables where a database is to be examined;
d. define the specific tests or procedures and related transactions and balances affected;
e. define the output requirements;
f. arrange with the user and IT departments, if appropriate, for copies of the relevant files or database tables to be made at the appropriate cut off date and time;

g. identify the personnel who may participate in the design and application of CAAT;
h. refine the estimates of costs and benefits;
i. ensure that the use of CAAT is properly controlled;
j. arrange the administrative activities, including the necessary skills and computer facilities;
k. reconcile data to be used for CAAT with the accounting and other records;
l. execute CAAT application;
m. evaluate the results;
n. document CAATs to be used including objectives, high level flowcharts and run instructions; and
o. assess the effect of changes to the programs/system on the use of CAAT.

6.10 Testing CAAT

i. The auditor should obtain reasonable assurance of the integrity, reliability, usefulness, and security of CAAT through appropriate planning, design, testing, processing and review of documentation. This should be done before reliance is placed upon CAAT. The nature, timing and extent of testing is dependent on the commercial availability and stability of CAAT.

6.11 Controlling CAAT Application

i. The specific procedures necessary to control the use of CAAT dfepend on the particular application. In establishing control, the auditor considers the need to:
   a. approve specifications and conduct a review of the work to be performed by CAAT;
   b. review the entity's general controls that may contribute to the integrity of CAAT, for example, controls over program changes and access to computer files. When such controls cannot be relied on to ensure the integrity of CAAT, the auditor may consider processing CAAT application at another suitable computer facility; and
   c. ensure appropriate integration of the output by the auditor into the audit process.

ii. Procedures carried out by the auditor to control CAATs applications may include:

   a. participating in the design and testing of CAAT;
   b. checking, if applicable, the coding of the program to ensure that it conforms with the detailed program specifications;

c. asking the entity's staff to review the operating system instructions to ensure that the software will run in the entity's computer installation;
d. running the audit software on small test files before running it on the main data files;
e. checking whether the correct files were used, for example, by checking external evidence, such as control totals maintained by the user, and that those files were complete;
f. obtaining evidence that the audit software functioned as planned, for example, by reviewing output and control information; and
g. establishing appropriate security measures to safeguard the integrity and confidentiality of the data.

When the auditor intends to perform audit procedures concurrently with online processing, the auditor reviews those procedures with appropriate client personnel and obtains approval before conducting the tests to help avoid the inadvertent corruption of client records.

iii. To ensure appropriate control procedures, the presence of the auditor is not necessarily required at the computer facility during the running of CAAT. It may, however, provide practical advantages, such as being able to control distribution of the output and ensuring the timely correction of errors, for example, if the wrong input file were to be used.

iv. Audit procedures to control test data applications may include:

- controlling the sequence of submissions of test data where it spans several processing cycles;
- performing test runs containing small amounts of test data before submitting the main audit test data;
- predicting the results of the test data and comparing it with the actual test data output, for the individual transactions and in total;
- confirming that the current version of the programs was used to process the test data; and
- testing whether the programs used to process the test data were the programs the entity used throughout the applicable audit period.

v. When using CAAT, the auditor may require the cooperation of entity staff with extensive knowledge of the computer installation. In such circumstances, the auditor considers whether the staff improperly influenced the results of CAAT.

vi. Audit procedures to control the use of audit enabling software may include:

- verifying the completeness, accuracy and availability of the relevant data, for example, historical data may be required to build a financial model;
- reviewing the reasonableness of assumptions used in the application of the tool set, particularly, when using modeling software;
- verifying availability of resources skilled in the use and control of the selected tools; and
- confirming the appropriateness of the tool set to the audit objective, for example, the use of industry specific systems may be necessary for the design of audit programs for unique business cycles.

6.12 Documentation

i. The various stages of application of CAATs should be sufficiently documented to provide adequate audit evidence.

ii. The audit working papers should contain sufficient documentation to describe CAAT application, including the details set out in the sections below.

(a) Planning

CAAT objectives;

- CAAT to be used;
- Staffing, timing and cost.
- Controls to be exercised; and

(b) Execution

- CAAT preparation and testing procedures and controls;
- Details of the tests performed by CAAT;
- Details of inputs (e.g., data used, file layouts), processing (e.g., CAATs high level flowcharts, logic) and outputs (e.g., log files, reports);
- Listing of relevant parameters or source code; and
- Relevant technical information about the entity's accounting system, such as file layouts.

(c) Audit Evidence

- Output provided;
- Description of the audit work performed on the output;
- Audit findings; and
- Audit conclusions;

(d) Other
- Recommendations to the entity management; and
- In addition, it may be useful to document suggestions for using CAAT in future years.

6.13 Arrangements with the Entity

i. The auditor may make arrangements for the retention of the data files, such as detailed transaction files, covering the appropriate audit time frame.

ii. In order to minimize the effect on the organization's production environment, access to the organisation's information system facilities, programs/systems and data should be arranged well in advance of the needed time period

iii. The auditor should also consider the effect of these changes on the integrity and usefulness of CAAT, as well as the integrity of the programs/system and data used by the auditor.

6.14 Using CAATs in Small Entities

i. Although the general principles outlined in this Guidance Note apply in small entity IT environments, the following points need special consideration:

a. The level of general controls may be such that the auditor will place less reliance on the system of internal control. This will result in greater emphasis on tests of details of transactions and balances and analytical review procedures, which may increase the effectiveness of certain CAATs, particularly, audit software.
b. Where smaller volumes of data are processed, manual methods may be more cost effective.
c. A small entity may not be able to provide adequate technical assistance to the auditor, making the use of CAATs impracticable.
d. Certain audit package programs may not operate on small computers, thus restricting the auditor's choice of CAATs. The entity's data files may, however, be copied and processed on another suitable computer.

Appendix to the Guidance Note

Examples of Computer Assisted Audit Techniques

Techniques	*Description*	*Advantages*	*Disadvantages*
Audit Automation	Expert Systems Tools to evaluate a client's risk management procedures Electronic working papers, which provide for the direct	These techniques are more useful when auditors are using laptops which can be directly linked with	Not applicable in the case of mainframe computers.

	extraction of data from clients computer records • Corporate and financial modeling programs for use as predictive audit test	the entity's system.	
Audit Software	Software used by the auditor to read data on client's files, to provide information for the audit and/or to reperform procedures carried out by the client's programs.	• Performs a wide variety of audit tasks • Long term economies • Reads actual records • Capable of dealing with large volumes of transactions	• Requires a reasonable degree of skill to use • Initial set up costs can be high • Adaptation often needed from machine to machine
Core Image Comparison	Software used by the auditor to compare the executable version of a program with a secure master copy	• Provides a high degree of comfort concerning the executable version of the program • Particularly useful where only executable versions are distributed	• Requires a high degree of skill to set up and to interpret the results • Where programs have been recompiled the comparison may be invalidated as the program records everything as a difference • Printouts are hard to interpret and the actual changes made are difficult to establish • Availability restricted to certain machine types
Database Analysers	Software used by the auditor to examine the rights associated with terminals and the ability of users to access information on a database	• Provides detailed information concerning the operation of the database • Enhances the auditor's understanding of the database management system	• Requires a high degree of skill to set up and to interpret the results • Restricted availability both as regards machine types and database management systems • Specific and limited audit applicability
Embedded Code	Software used by the auditor to examine transactions passing through the system by placing his own program in the suite of programs used for processing	• Performs a wide variety of audit tasks • Examines each transaction as it passes through the sys tem • Operates continuously	• There is a processing overhead involved because of the extra programs • Definition of what constitutes an unusual transaction needs to be very precise • Precautions need to be

		Capable of identifying unusual transactions passing through the system	taken over the output from the programs to ensure is security Precautions need to be taken to ensure that the program cannot be suppressed or tampered with Requires some degree of skill to use and to interpret the results
Log Analysers	Software used by the auditor to read and analyse records of machine activity	Provides detailed information on machine usage Long term economies Effective when testing integrity controls	Requires a high degree of skill to use and to interpret the results Limited availability as regards machine types High volume of records restricts extent of test
Mapping	Software used by the auditor to list unused program instructions	Identifies program code which may be there for fraudulent reasons	Very specific objective Requires a high degree of skill to use and to interpret the results Adaptation needed from machine to machine
Modelling	A variety of software, usually associated with a microcomputer, enabling the auditor to carry out analytical reviews of client's results, to alter conditions so as to identify amounts for provisions or claims, or to project results and compare actual results with those expected	Can be a very powerful analytical tool Can enable the auditor to examine provisions on a number of different bases Very flexible in use Can provide the auditor with useful information on trends and patterns	A high volume of data may need to be entered initially Results require careful interpretation
Online Testing	Techniques whereby the auditor arranges or manipulates data either real or fictitious, in order to see that a specific program or screen edit test is doing its work	Very widely applicable Easy to use Can be targetted for specific functions carried out by programs	Each use satisfies only one particular objective Care must be taken to ensure that "live" data does not impact actual results
Program	An examination by the	Gives a reasonable	The auditor must

Code Analysis	auditor of the source code of a particular program with a view to following the logic of the program so as to satisfy himself that it will perform according to his understanding	degree of comfort about the program logic ▯ The auditor can examine every function of the program code	understand the program language ▯ The auditor needs to check that the source code represents the version in the source library, and that this version equates to the executable version
Program Library Analysers	Software used by the auditor to examine dates of changes made to the executable library and the use of utilities to amend programs	▯ Provides the auditor with useful information concerning the program library ▯ Identifies abnormal changes to the library ▯ Useful when testing program security	▯ Requires a high degree of skill to use and to interpret the results ▯ Availability restricted to certain machine types ▯ Only relevant when testing integrity controls
Snapshots	Software used by the auditor to take a "picture" of a file of data or a transaction passing through the system at a particular point in time	▯ Permits the auditor to examine processing at a specific point in time to carry out tests, or to confirm the way a particular aspect of the system operates	▯ Can be expensive to set up
Source Comparison	Software used by the auditor to compare the source version of a program with a secure master copy	▯ Compares source code line by line and identifies all differences ▯ Useful when testing integrity controls or particularly important program procedures	▯ Other procedures are necessary to ensure that the executable version reflects the source code examined ▯ Requires some degree of skill to use and to interpret the results ▯ Availability restricted to certain machine types
Test Data - "Live", "Dead", Integrated Test Facility or Base Case System	Fictitious data applied against the client's programs either whilst they are running or in an entirely separate operation. The results of processing the fictitious data are compared	▯ Performs a wide variety of tasks ▯ Gives considerable comfort about the operation of programs ▯ Can be precisely targetted for specific procedures within	▯ "Dead" test data requires additional work for the auditor to satisfy himself the right programs were used ▯ Care must be taken to ensure that "live" data does not impact actual results ▯ Technique can be expensive

Evaluation	with the expected results based on the auditor's understanding of the programs involved	programs Long term economies	to set up and cumbersome to use Adequate for detection of major error but less likely to detect deepseated fraud
Tracing	Software used by the auditor to identify which instructions were used in a program and in what order	Helps to analyse the way in which a program operates	There may be less costly ways to achieve the same objectives, although not in the same detail Requires a high degree of skill to use and to interpret the results Adaptation needed from machine to machine

7. Annexure 2: Sample Results of Using CAAT

Report on review of RDBMS data using SQL

As a part of our audit procedure, we have used SQL to directly access and analyse the data stored in the tables. Our observations and the related analysis are given below. These observations relate to the data stored, which could impact financial accounts. So we have submitted this information to statutory auditors and user department of ABC requesting them to verify these SQL results and confirm the impact on the financial statements. The detailed SQL statements can be obtained from the IT department of ABC. We have given a copy of this draft report to ABC for confirmation of facts. Our observations with implications, comments and our risk assessment are given below:

i. Observation - High

Users available with invalid employee codes e.g. employee Code 15.

There are two user IDs with user ID 15, which is still being used. Used by live users these transactions will not establish user accountability.

Implications

Since the employer code is invalid, it will be difficult to establish accountability for transactions entered using the ID in case of errors or frauds.

IT Depatment's feedback and agreed action

This User ID was created during the time of data conversion. It has been disabled so that transactions cannot be entered using this.

ii. Observation - High

a. Past Employees having Id in access Table 19 users to have user IDs. Their employee Id and name are given so that a final list may be prepared with actual users who are expected to have access to the system.

b. No. of transactions entered by each employee from the inception. This table has the number of transactions entered by each employee. Some users have entered only 4 transactions while some others have entered more than 30,000 transactions. This needs to be analyzed. Implications

The number of user accounts in the system is much more than the actual users. This is because past and temporary users have not been disabled.

IT Department's feedback and agreed action

The number of users will correspond to the actual users. All other users will be disabled.

iii. Observation - High

Transactions with amount as null Transactions with null amount are listed day wise. There are 181 transactions, which need to be analyzed.

Implications

This results in dummy transactions, which may not have any value, or genuine transactions might have been stored without values.

IT Department's feedback and agreed action

Such action is taken in cases where DD charges are deducted from the loan amount for obtaining DD but the loan account is debited with the total amount including DD charges. This does not have any financial impact. The feedback derived from the IT department leads to agreed action.

iv.. Observation - Low

UNITS HAVING REBATE AS 3% IN LOAN COMTABLE OF HO.

There are 69 accounts with a total rebate of Rs.4,12,132. These need to be confirmed.

Implication

There could be excess rebate granted for loan accounts.

IT Department's feedback and agreed action

All the listings are of genuine accounts where the rebate is 3%

v. Observation - HIGH

Total number of accounts where penal interest is more than 2.5%

a. There are a number of accounts with penal interest ranging from 2% to 23.5%. The number of transactions as per interest rate is given elsewhere. Detailed account wise transactions were extracted, verified and confirmed. There are 34 categories of interest computations, which were given separately to the users.
b. Accounts having penal rates as '0' as on 10-Mar-2000.

There are 196 transactions listed unit wise with zero panel interest rate.

Implication

The interest computation is wrong in that there are errors in the panel interests. Also there is no control on modification to these rates.

IT department's feedback and agreed action Incorrect past data is being rectified and further controls are being incorporated in the programs to ensure that all modifications to such master tables are captured and also authorised. These will also be printed as exception report.

vi. Observation - HIGH

Voucher No. is Null

In a few cases the voucher number is null date Voucher No.

22 April 2000	31
23 June 2000	67
14 July 2000	18

Implication

The transaction may not be picked up for processing as the voucher number is provided by the system. Such errors could have occurred due to program bugs.

IT department's feedback and agreed action.

Voucher numbers are not used for generating any reports. However, they will be investigated and rectified.

vii. Observation - Low

Sanction Amount is Zero

The sanction amount for 26 cases is zero.

Implication

The past data has not been captured and invalid data is printed in the statement of accounts.

IT department's feedback and agreed action.

These are being identif ied and rectif ied as one time measures.

Appropriate controls will be built into the program.

viii. Observation - HIGH

Account with loan balance and principal balances is zero but interest balance and other debits is not zero.

There are genuine cases where unit has been taken over and the amount realised is credited towards principals. Only if there is a balance of loan left is it transferred to interest and other debits.

Implication

There may be errors on account of data entry because of invalid data and incorrect statement of accounts.

IT department's feedback and agreed action

All cases, which are not genuine are being identified and rectified as one time measures. Appropriate controls will be built in the program to consider them as a separate account type.

Summary

Audit in a computerized environment could require either audit of transactions and records or audit of IT and general controls IT Environment impact on Audit Methodology. The auditor should gain good understanding of the technology environment and the state of related controls before designing his audit procedures. Traditional techniques of auditing may not be effective in achieving even the conventional audit objectives in a computerized environment. Hence it is pertinent that the auditor should take into consideration the risks in the computerized environment and choose the appropriate audit approach, computer assisted audit techniques and methods for accomplishing his audit objectives. This requires a good understanding on the part of the auditor in understanding the various types, advantages and risks of using general and special audit tools and techniques and should possess the necessary skill and competence to audit in a computerized environment. Where the auditor encounters continuous computer processing environments, the auditor should evaluate the audit objective requirements taking into consideration the nature of automated processing and apply the most appropriate

continuous auditing technique. Hence auditor uses his knowledge and expertise in assessing the risks in the computerized environment, and possess expertise in choosing the appropriate audit approach and audit techniques for effective completion of audit.

Self Assessment Test Question

Q.1 Under which approach internal control are reviewed and testing is done in the same manner as in non – EDP system.

a. Audit around the Computer
b. Audit through the computer
c. Audit using computer
d. None of the above

Q.2 The condition where audit around the computer can be performed in absence of which of the following parameter.

a. The documents are available in non machine language.
b. Proper filing of the document.
c. Output with sufficient details about individual transaction.
d. *All of the above*

Q.3 In audit around the computer, A auditor verifies

a. Computer H/W
b. Computer S/W
c. Systems and Control
d. None of the above

Q.4 What is the Auditor's Primary concern?

a. System of controls
b. Examination and testing of controls
c. Both (a) & (b)
d. Non of the above

Q.5 To verify the clients data recorded in the computer, what kind of test a auditor can perform.

a. Examining records for quality, completeness, consistency and correctness
b. Comparing data on separate files
c. Selecting audit samples
d. All of the above

Q.6 Which one is the generalized audit programs designed to perform data processing functions that includes reading computer files, selecting information, performing calculation and etc.
- *a. Package program*
- *b. Purpose written program*
- *c. Utility program*
- *d. None of the above*

Q.7 Which one is not the example of CAAT used in collecting evidences.
- *a. Application system*
- *b. Performance Monitoring tool*
- *c. Network Management tool*
- *d. Enterprise Resource System*

Q.8 Online Password and data access controls are example of
- *a. System Data Access*
- *b. Integrated Test Facilities*
- *c. Test Data*
- *d. None of the above*

Q.9 The uses of CAAT comprises of
- *a. Compliance test of General EDP controls*
- *b. Compliance test of EDP application control*
- *c. Both (a) & (b)*
- *d. None of the above*

Q.10 The factors that determines the use of CAAT which describe the effectiveness and efficiency of auditing procedure.
- *a. Timing*
- *b. Availability of CAAT*
- *c. Impracticability of manual test*
- *d. None of the above*

Q.11 Which are is not a part of the GAP.
- *a. Sampling*
- *b. Extraction*
- *c. Totaling*
- *d. None of the above*

Q.12 The techniques uses as a part of substantive approach to test the validity and accuracy of input data processes through a system is known as
- *a. Simulation*
- *b. Audit trail*

c. *Embedded audit facilities*
d. *None of the above*

Q.13 The controlled application of auditors test data (live or dummy) to client application program procedures is known as
a. *Test packs*
b. *Integrated Test Facility*
c. *Program code analysis*
d. *None of the above*

Q.14 In online, real time banking system what kind of test data techniques is used for auditing.
a. *System activity files interrogation*
b. *Integrated Test Facility*
c. *Data file Interrogation*
d. *None of the above*

Q.15 Which one of is the advantages of Data File Interrogation ?
a. *Faster and Accurate*
b. *reviewing voluminous data*
c. *both (a) & (b)*
d. *None of the above*

16. For an IS auditor, the procedures used to gather audit evidence do not include which of the following?
a. *Manual audit procedures*
b. *Computer assisted audit techniques (CAAT)*
c. *CAAT procedures first and manual audit procedures later*
d. *A combination of manual and CAAT audit procedures*

17. What is the least important consideration in obtaining a computerized audit tool or technique?
a. *Platform independence*
b. *Technical support*
c. *Information technology usage levels*
d. *Application independence*

18. Which of the following is not a feature of a generalized audit software package?
a. *Data retrieval*
b. *Data stratification*
c. *Data validation during processing*
d. *Data summarization*

19. Identify the need for controls and auditing in a computerized environment.
    a. *Absence of input documents*
    b. *Lack of visible transaction trail*
    c. *Accessibility of data and computer programs*
    d. *All of the above*

20. Identify the audit technique that examines each transactions as it passes through the system.
    a. *Embedded code*
    b. *Program code*
    c. *Database Analyzers*
    d. *Database code*

21. The technique used by an auditor to list unused program instructions is….
    a. *Modeling*
    b. *Analyzing*
    c. *Mapping*
    d. *Tracing*

22. The sample data created and used for the purpose of testing the application system is called….
    a. *Test data*
    b. *Table data*
    c. *Item data*
    d. *Record data*

23. The test data (dummy unit) implemented in the normal processing of the system over a period of time is known as…
    a. *Integrated Test Facility*
    b. *Black box Test Facility*
    c. *Graph testing*
    d. *Whitebox testing*

24. The capability of the generalized audit software to read different data coding schemes, different record formats and different file structures is …
    a. *File size*
    b. *File data*
    c. *File access*
    d. *File reorganization*

25. The audit software capability of frequency analysis is to….
    a. *Sort and merge files*
    b. *Samples nth item*

c. Formatting output
d. *Classify data on a criteria*

26. The purpose written audit program are used for …..
    a. Sorting, creating, and printing files
    b. Data retrieval, code comparison
    c. Reading data, selecting and analyzing information
    d. Specific tasks with original or modified programs

27. Identify the functional limitation of a generalized audit software that enables evidence collection only on the state of an application system after the fact.
    a. Ex Post Auditing only
    b. Analytical review only
    c. Limited ability to determine Propensity for Error
    d. Limited ability to Verify Processing logic

Answer :

1. a	2. d	3. d	4. c	5. d	6. a	7. d	8. d	9. c
10. d	11. d	12. c	13. a	14. b	15. c	16.c	17.c	18.c
19.d	20. a	21. c	22. a	23. a	24. c	25. d	26. d	27. a

4 Overview of Information Systems Audit Regulations and Standards

Learning Objectives

- To provide an understanding of national and international Audit standards
- To provide an understanding of the IS certifications and regulatory developments

Introduction

Every profession has a unique repository of knowledge, which lends credence to its specialization. This knowledge often forms the basis to define commonly accepted practices. Very often the technical competencies and skills of professionals are assessed against these practices. So the first step towards becoming a specialized professional is to gain a thorough understanding of these matters. The IS auditing standards provide audit professionals a clear idea of the minimum level of acceptable performance essential to discharge their responsibilities effectively. They define mandatory requirements for the IS auditing and reporting.

Audit Standards

The Auditing and Assurance Standards issued by ICAI

At the time of planning and carrying out his audit, a chartered accountant should take into consideration the auditing and assurance standards (AAS) issued by the Institute of Chartered Accountants of India to the extent applicable.

AAS 29 “Auditing in a Computer Information Systems Environment” established standards on procedures to be followed when an audit relating to accounting information is conducted in a computer information systems (CIS) environment. The pronouncement outlines the procedures that an auditor entrusted with financial, operational and other conventional audit objectives relating to

accounting information should carry out while auditing in a computerized environment.

Professional ethics and Code of Conduct prescribed by ICAI

Professional ethics and Code of Conduct prescribed by ICAI shall apply to the Information Systems audit as well.

IT Audit and Assurance Standards, Guidelines, Tools and Techniques by ISACA

Information Systems Audit and Control Association (ISACA) has issued standards, guidelines, tools and techniques for IT audit and assurance. These provide mandatory requirements, guidance and procedures for the IS auditing. IT audit and assurance professionals should use their professional judgment when applying the standards, and provide justification (if any) for any departure from the standards.

IT Audit and Assurance Standards

S1 Audit Charter
S2 Independence
S3 Professional Ethics and Standards
S4 Competence
S5 Planning
S6 Performance of Audit Work
S7 Reporting
S8 Follow-Up Activities
S9 Irregularities and Illegal Acts
S10 IT Governance
S11 Use of Risk Assessment in Audit Planning
S12 Audit Materiality
S13 Using the Work of Other Experts
S14 Audit Evidence
S15 IT Controls
S16 e - Commerce

IT Audit and Assurance Guidelines

G1 Using the Work of Other Auditors
G2 Audit Evidence Requirement
G3 Use of Computer Assisted Audit Techniques (CAATs)
G4 Outsourcing of the IS Activities to Other Organizations
G5 Audit Charter
G6 Materiality Concepts for Auditing Information Systems

G7 Due Professional Care
G8 Audit Documentation
G9 Audit Considerations for Irregularities and Illegal Acts
G10 Audit Sampling
G11 Effect of Pervasive IS Controls
G12 Organizational Relationship and Independence
G13 Use of Risk Assessment in Audit Planning
G14 Application Systems Review
G15 Planning Revised
G16 Effect of Third Parties on an Organization's IT Controls
G17 Effect of Non-audit Role on the IT Audit and Assurance Professional's Independence
G18 IT Governance
G19 Irregularities and Illegal Acts (withdrawn on 1 Sep 2008)
G20 Reporting
G21 Enterprise Resource Planning (ERP) Systems Review
G22 Business-to-consumer (B2C) E-commerce Review
G23 System Development Life Cycle (SDLC) Review Reviews
G24 Internet Banking
G25 Review of Virtual Private Networks
G26 Business Process Reengineering (BPR) Project Reviews
G27 Mobile Computing
G28 Computer Forensics
G29 Post-implementation Review
G30 Competence
G31 Privacy
G32 Business Continuity Plan (BCP) Review From It Perspective
G33 General Considerations on the Use of the Internet
G34 Responsibility, Authority and Accountability
G35 Follow-up Activities
G36 Biometric Controls
G37 Configuration Management Process
G38 Access Controls
G39 IT Organization
G40 Review of Security Management Practices

IT Audit and Assurance Tools and Techniques

P1 The IS Risk Assessment
P2 Digital Signatures
P3 Intrusion Detection

P4 Viruses and other Malicious Code
P5 Control Risk Self-assessment
P6 Firewalls
P7 Irregularities and Illegal Acts
P8 Security Assessment–Penetration Testing and Vulnerability Analysis
P9 Evaluation of Management Controls Over Encryption Methodologies
P10 Business Application Change Control
P11 Electronic Funds Transfer (EFT).

Cobit – IT Governance Model

Objective

COBIT (Control Objectives for Information and related Technology) is a one-stop reference point of current preferred practices for IS control practitioners. It is a collection of, generally, accepted auditing practices (control objectives for an IT environment). 36 Sources were used to develop COBIT, making it the most comprehensive standard.

COBIT defines control as "the policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected." Control objective is defined as "A statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity." COBIT focuses on business processes. For each business process, COBIT has a listing of control objectives, controls that can be used to achieve these objectives, and audit procedures that can be used to determine whether the controls are in place and operating reliably. COBIT also provides an Audit Guideline for each of the control objectives to match the review of the organization's existing IT processes against the recommended detailed control objectives to provide the management assurance and/or advice for improvement.

COBIT is used as a benchmark by the IS control specialists to assess how an activity is practiced or implemented. Auditors have to provide the management and business process owners of the organization a reasonable assurance that relevant control objectives are being met; identify where there are significant weaknesses in those controls; substantiate the risk that may be associated with such weaknesses; and finally, advise these executives on the corrective actions that should be taken.

COBIT also supports a generic IT assurance/audit process, which could be summarized as:

- Obtaining an understanding of business requirements, related risks and relevant control measures;
- Evaluating the appropriateness of stated controls;
- Assessing compliance by testing whether the stated controls are working as prescribed, consistently and continuously;
- Substantiating the risk of control objectives not being met.

Audience

COBIT is a multi-purpose tool, which has been jointly developed by the Information Systems Audit and Control Foundation, several major sponsors and technology consultants. It can be used by:

1. The management, to balance risk and control IT investment and to benchmark the existing and future IT environment;
2. Users, to obtain assurance on the security and control of products and services they acquire;
3. Auditors, to substantiate their opinions to the management on internal controls and to advise on the necessary minimum controls.

Open Standard

COBIT is an open standard that can be downloaded on a complimentary basis from the IT Governance Institute in affiliation with the **Information Systems Audit and Control Association (ISACA)** at www.isaca.org. It is the outcome of years of research and cooperation among global IT and business experts. It provides an authoritative, globally accepted set of IT practices for business managers and auditors. COBIT is accepted and used worldwide as the breakthrough IT governance tool that helps in understanding and managing IT - related risks.

COBIT is based on the Information Systems Audit and Control Foundation's (ISACF) control objectives. It has been enhanced to meet existing and emerging international technical, professional, regulatory and industry-specific standards. The resulting control objectives have been developed for application in organization-wide enterprise information systems. COBIT's best practices (consensus of experts) help in optimizing information investment, but better still it helps in proactively assessing and managing risks.

Tool Kit

COBIT consists of the following components each with its own objective:

1. The executive summary is designed to provide key concepts in IT governance.

2. The framework is a conceptual model linking control objectives to business objectives.
3. The control objectives provide the landscape of the IT Environment.
4. The audit guidelines make it easy for the auditor to navigate through any IS environment.
5. The implementation tool set makes it easy to get started on the audit.
6. Management guidelines provide the tools for benchmarking processes.

The COBIT Framework

The COBIT Framework consists of high-level control objectives and an overall structure for their classification. It addresses the issue of control from three vantage points, or dimensions:

1. **Business Objectives** – To satisfy business objectives, information must conform to certain criteria that COBIT refers to as business requirements for information. The criteria are divided into seven categories: effectiveness, efficiency, confidentiality, integrity, availability, compliance with legal requirements, and reliability.

2. **IT resources** – IT resources include people, applications systems, technology, facilities, and data.

3. **IT processes** – IT processes are broken into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring. Definitions of these four domains are as below:

    - **Planning and Organization –** This domain covers strategy and tactics. It is concerned about finding the way in which IT can best contribute to the achievement of the business objectives.

    - **Acquisition and Implementation –** To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are also covered by this domain.

    - **Delivery and Support** – This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. In order to deliver services, the necessary support services must be set up.

    - **Monitoring** – All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses the management's oversight of the organization's

control process and independent assurance provided by internal and external audit or obtained from alternative sources.

Application of COBIT for IS Audit

COBIT has four domains with 34 IT processes and 318 specific and detailed control objectives. The detailed control objectives can be used to evaluate the available controls in an organization. The IS auditor can base his audit approach, findings and recommendations on COBIT.

It provides a macro business perspective, and then focuses on the need for deploying IT, aligning IT and business objectives, ensuring IT governance and the methodology for management, users and auditors.

Control objectives are the most important aspect of an IS audit as they provide the minimum level of controls required. These objectives have to be developed keeping in mind the requirements of various business and technical environment. Generally, control objectives are meant for the management and staff of the IT, control and audit functions. More importantly, it's for the business process owners. Control objectives provide precise and clear definitions of a minimum set of controls. This ensures effectiveness, efficiency and economy in utilizing resources before commencing the audit. For each IT process to be audited, detailed control objectives are to be identified as the minimum set of controls which need to be in place. Existing controls in the audited environment can then be assessed to verify their sufficiency.

Other Global Standards on IS Assurance and Audit

A. The information security standards: BS7799 & ISO 27001

BS7799 was developed by the British Standards Institute (BSI) in 1995 as an international standard to guide the development and implementation of an Information Security Management System, commonly known as an ISMS. BS7799 provides a comprehensive set of controls that consist of the best practices in information security. It helps identify, manage and minimize the range of threats to which information is regularly subjected. BS7799 was conceived as an industry independent, technology independent, management system which assures the management that its information security measures and arrangements were effective, if it is properly implemented.

BS7799 focuses on protecting the availability, confidentiality and integrity of organizational information. Using it well will result in:

- Reduced operational risk
- Increased business efficiency

- Assurance that information security is being rationally applied

Initially, BS7799 was just a single standard which was envisaged to be followed as a code of practice. It was not developed in a manner to provide specifications for external verification and certification. With the increase in information security awareness all over the globe, the demand for a certification scheme emerged which led to the development of a second part to the standard, in the form of a specification. It was known as BS7799-2 or BS7799 Part 2.

Today, the Code of Practice is recognized under the dual numbers of ISO17799 and BS7799-1 or BS7799 Part 1. The most recent version of the Code of Practice, which is in use today, is ISO/IEC 17799:2005.

BS7799:1995 was revised in 2002 and later in November 2005, it was withdrawn and replaced by ISO/IEC 27001:2005, commonly known as ISO 27001.

Hence, today the two parts in force are:

ISO/IEC 17799:2005 - which serves as a Code of Practice for Information Security Management System;

ISO/IEC 27001:2005 - which provides specification for certification of Information Security Management Systems.

The relationship between ISO/IEC 17799:2005 (Code of Practice) and ISO/IEC 27001:2005(specification)

An organization can develop its ISMS in line with ISO 17799. The good practices identified in this Code of Practice are universally applicable. However, because it was not designed to be the basis of a certification, it doesn't specify the system requirements with which an ISMS must be compliant if it is to be so certified. ISO 27001 contain those specifications. It means that an organization that is using ISO 17799 on its own can conform to the compliance of the Code of Practice but it cannot get an external certification body to verify that it is complying with the standard. An organization that is using ISO 27001 and ISO 17799 in conjunction with one another can design an ISMS that complies with the specification and also follows the guidance of the Code of Practice and which is, therefore, capable of achieving external IS0 27001 certification.

ISO 17799 is intended to provide a single reference point for the wide range of controls required for most situations where IT is used in industry, commerce and communication.

Table 1 lists the standard containing 11 security control clauses collectively containing a total of 39 main security categories and one introductory clause on Risk Assessment and Treatment.

S.No	Security Clauses	No. of Security Control Categories under each clause
1	Information Security Policy	1
2	Organizing Information Security	2
3	Asset Management	2
4	Human Resource Security	3
5	Physical and Environmental Security	2
6	Communications & Operations Management	10
7	Access Control	7
8	Information Systems Acquisition, Development and Maintenance	6
9	Information Security Incident Management	2
10	Business Continuity Management	1
11	Compliance	3
		39

Table 1: The Standards and their Security Controls

B. SAS 70 - Statement on Auditing Standards (SAS) No. 70, Service Organizations (AICPA)

In the present global business environment, outsourcing of business processes or activities is an increasingly common practice. Therefore, service organizations must also be able to assure on the adequacy of controls and safeguards when they host or process the data belonging to their customers. The services could be any services such as data processing, sales or payroll processing, applications and claims processing, IT management, data center operations and management, application service providers, etc.

Statement on Auditing Standards (SAS) No. 70 for Service Organizations is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).

SAS 70 audit involves an in-depth audit of the service organization's control activities, which generally, include controls over information technology and related processes. SAS 70 also specifies a standard format of report, which

signifies that the auditor has examined the service organization's control objectives and control activities. The auditors conducting the examination and issuing the report are referred to as the service auditors. The service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting.

SAS 70 provides for two types of reports called Type I and Type II re- ports. A Type I report describes the service organization's description of controls at a specific point in time, whereas a Type II report not only includes the service organization's description of controls, but also includes detailed testing of the service organization's controls over a period of time.

SAS 70 is an auditing standard, which enables an independent auditor to evaluate a service organization's controls. The audit report (i.e. the Service Auditor's Report) contains the auditor's opinion, a description of the controls in place, and a description of the auditor's tests of operation effectiveness. It is issued to the service organization at the conclusion of an SAS 70 examination. It helps a service organization build trust with its user organizations (i.e. customers). Without a current Service Auditor's Report, a service organization may have to entertain multiple audit requests from its customers and their respective auditors. This report ensures that all user organizations and their auditors have access to the same information.

In an SAS 70 audit, the service organization is responsible for describing its control objectives and control activities that might be of interest to auditors in user organizations. If an organization does not have a security policy covering a particular area, or has one that allows ineffective security, the SAS 70 audit report would contain a favorable opinion because the control activities (none) matched the stated control objectives (none).

SAS 70 is, generally, applicable when an auditor (user auditor) is auditing the financial statements of an entity (user organization) that obtains services from another organization (service organization).

If the report is of Type II, then it can be shared with the user organizations and user auditors. The service organization is responsible for describing its control objectives and activities that are relevant to user organizations and their auditors.

C. SysTrust

The SysTrust service is an assurance service that has been jointly developed by the **American Institute of Certified Public Accountants (AICPA)** and the **Canadian Institute of Chartered Accountants (CICA)**.

It is designed to increase the comfort level of management, customers, and business partners with systems that support a business or a particular activity. SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system. In a SysTrust engagement, the practitioner evaluates and tests whether or not a specific system is reliable when measured against four essential principles - availability, security, integrity and maintainability. Here is a brief explanation of the four key SysTrust principles:

1. Availability: The system is available for operation and use at times set forth in service-level statements or agreements.
2. Security: The system is protected against unauthorized physical and logical access.
3. Integrity: The system processing is complete, accurate, timely, and authorized.
4. Maintainability: The system can be updated when required without adversely affecting its availability, security and integrity.

   A detailed criterion exists for each of the above principles. The SysTrust criteria are posted on both the AICPA and CICA web sites.

   At the completion of a SysTrust engagement, the practitioner renders an opinion on the management's assertion (or the actual subject matter) that effective controls have been maintained. The practitioner can report on all four SysTrust principles together or on each principle separately. Because the SysTrust principles and criteria are established and available to any user, the practitioner's report does not have to be restricted to specific parties.

D. IT Infrastructure Library (ITIL)

With organizations increasingly dependent on information technology for running their businesses, there is a need for high quality of IT services. Hence, the process underlying IT services and IT Service Management (ITSM) has come into focus. ITIL is a series of documents that provides a framework for implementation of IT Service Management. This framework defines how Service Management is applied within specific organizations.

ITIL was originally created by CCTA, a UK Government agency. It has come to be recognized as the de facto standard for best practice in the provision of IT service. ITIL aids a framework based approach to the structured IT service management, which can be customized by organizations to suit their needs. ITIL provides through a series of documents, a cohesive set of best practices

further supported by a comprehensive qualifications scheme, accredited training organizations, and implementation and assessment tools, thus enabling benchmarking of IT Service Management maturity across organizations and against standards. It is published in a series of books, each of which covers an IT management topic. It is composed of five volumes – Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. ITIL enables an organization to get certified against the Standard for IT Service Management i.e. ISO 20000.

ITIL deals with a detailed understanding of the IT service management processes, IT service support processes and IT service delivery processes. Some of the topics covered as part of ITIL are:

- IT Service support processes;
- Incident Management;
- Problem Management;
- Configuration Management;
- Change Management;
- Release Management;
- IT Service Delivery processes;
- Service Level Management;
- Help Desk Management;
- Disaster Recovery Planning/IT Service Continuity Management;
- Capacity Management;
- Financial Management;
- Availability Management;
- Security Management.

ITIL covers a number of areas, but one of its main focuses is IT Service Management. IT Service Management in turn consists of two key areas, Service Support and Service Delivery. It is these two key areas (consisting of 10 disciplines) that are responsible for the provision and management of effective IT services.

ITIL provides a systematic and professional approach to the management of IT service provision. Adopting its guidance offers users a huge range of benefits that include:

- Reduced costs;
- Improved IT services through the use of proven best practice processes;
- Improved customer satisfaction through a more professional approach to service delivery;

- Standards and guidance;
- Improved productivity;
- Improved use of skills and experience;
- Improved delivery of third party services through the specification of ITIL or ISO 20000 as the standard for service delivery in services procurements.

Toolkit

ITIL toolkit is comprised of the following components to help simplify, explain and manage ITIL and the ITIL process:

- The ITIL Guide is a detailed and comprehensive introduction to ITIL.
- The ITIL Management Presentation explains how, what and why of ITIL and service management through a series of PowerPoint slides.
- The ITIL Fact Sheets is a two page unique reference kit covering each of the main ITIL disciplines.
- The ITIL Compliance Assessment Kit is a comprehensive Excel based questionnaire set, designed to help assess the compliance position with ITIL and identify the areas which need attention.
- The ITIL Presentation Template is designed to help interpret compliance assessment scoring and create a presentation from the results.
- ITSM Reference Guides are intended to introduce a range of other ITSM related frameworks and approaches.

ISO 20000

The ISO 20000 standard has been derived from BS 15000, a product of British Standards Institute. It is a universally accepted reference standard for all organizations (regardless of sector, size and type of organization) that provide IT services to internal and/or external customers.

This standard is closely synchronized with the IT Infrastructure Library (ITIL) as the Best Practice recommendation for Service Support and Service Delivery.

ISO 20000 has two parts:

ISO 20000-Part 1

It provides specification for IT service management. It defines the requirements of an organization and the management system for delivering managed services at a level of quality acceptable to the customer. This part gives clear specifications and information as to how an organization must align itself in regard to ISO 20000, an internationally accepted certification.

The requirements/specifications cover:

- Requirements for a management system;
- Planning and implementing service management;
- Planning and implementing new or changed services;
- Service delivery processes;
- Relationship processes;
- Resolution processes;
- Control processes;
- Release processes.

ISO 20000- Part 2

It portrays the code of practice for IT service management. This section interprets ISO 20000 for implementation purposes. It describes an integrated set of Service Management processes that is aligned towards the process approach defined in ITIL and that supplements these.

Conceptually, the two ISO 20000 standards and their relationship with ITIL, are best described with the aid of Fig.1 shown below.

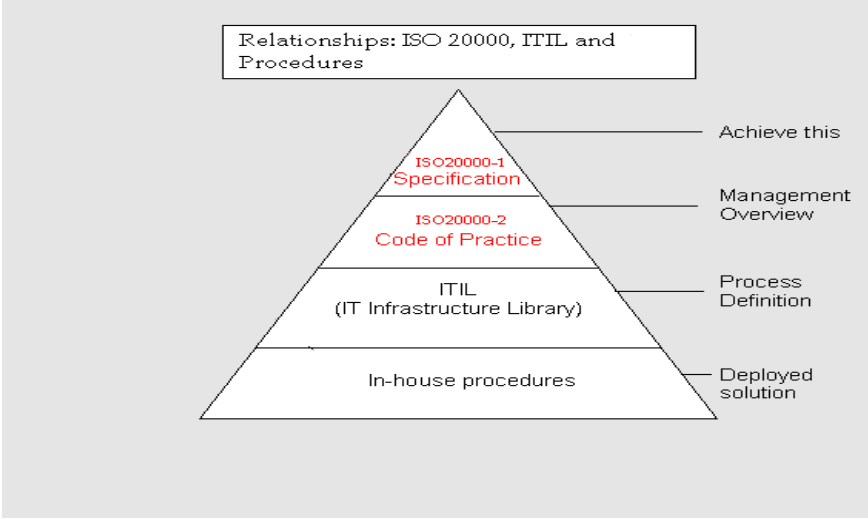


Fig. 1 : The Two ISO 20000 standards and their relationship with ITIL

Overview of Regulatory Developments Impacting Controls in a Computerized Environment

A. Information Technology Act, 2000 of Government of India

The Information Technology Act (the IT Act or the Act) was enacted on 7th June

2000, to provide legal recognition for the transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as e-Commerce and to promote efficient delivery of Government services by means of reliable electronic records (commonly referred to as e-governance). The IT Act is modeled on the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law, which brings uniformity to the law applicable to alternatives to paper-based methods of communication and storage of information.

Objectives of the Act are:

- To grant legal recognition for electronic transactions and electronic communication;
- To give legal recognition to Digital signatures for authentication of any information or matter;
- To facilitate electronic filing of documents with Government departments;
- To facilitate electronic storage of data;
- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions;
- To give legal recognition for keeping of books of accounts by bankers in electronic form;
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

The Act consists of 94 sections spread over thirteen chapters, and four schedules to the Act. The Schedules to the Act contain related amendments made in other acts as outlined in the above paragraph.

The Act shall not apply to the following:

- a negotiable instrument as defined in section 13 of the Negotiable Instruments Act, 1881;
- a power-of-attorney defined in section 1A of the Powers-of-Attorney Act, 1882;
- a trust as defined in section 3 of the Indian Trusts Act, 1882;
- a will as defined in Section 2 (h) of the Indian Succession Act, 1925, including any other testamentary disposition by whatever name called;
- any contract for the sale or conveyance of immovable property or any interest in such property;
- any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

Some of the salient aspects covered under the Act include:

- definitions of various terms relating to electronic means of processing, communication, storage and security. Some of these include electronic form, information, data, computer, computer network, computer system, computer resource, secure system, access, digital signature, private and public key, asymmetric cryptosystem, affixing of a digital signature;
- method of authentication of electronic records using digital signature and its verification;
- legal recognition of electronic records and digital signatures and their use in Government and its agencies;
- attribution, time and place of dispatch and acknowledgment of receipt of electronic records;
- security procedure for securing electronic records and digital signatures;
- method of retention of electronic records and their retrieval;
- empowers the Government to make necessary rules by Central Government, regulation of certifying authorities;
- enabling the legal administrative structure to support the administration of the Act, including licensing, regulation and audit of certifying authorities, setting up of Cyber Regulations Appellate Tribunal;
- Digital Signature Certificates, their certification, revocation and management and duties of subscribers.

The Act also specifies the acts that invite penalty, which may include any of the following:

- Unauthorized accessing or securing access to such computer, computer system or computer network;
- Unauthorized downloading, copying or extracting any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- Introducing or causing to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- Damaging or causing to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system or computer network;
- Disrupting any computer, computer system or computer network;
- Denying or causing the denial of access to any person authorized to access any computer, computer system of computer network by any means;
- Providing any assistance to any person to facilitate access to any

computer, computer system or computer network in contravention of any provisions of the Act, rules or regulations made thereunder;
- Charging the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network.

Besides this, the Act also provides for penalty on the failure to furnish any document or return or report to the Controller or the Certifying Authority, failure to maintain books of accounts or records.

The Act also provides for offences that are liable on conviction to imprisonment or fine up to Rupees Two Lakhs or both. Such offences include

- tampering with computer source documents;
- hacking with computer system;
- publishing of information which is obscene in electronic form;
- breach of confidentiality and privacy of electronic records, books, information, etc. without the consent of the person to whom they belong;
- publishing Digital Signature Certificate for unlawful or fraudulent purposes.

B. The UNCITRAL Code

The **United Nations Commission on International Trade Law (UNCITRAL)** Code adopted in 1996, is based on the resolution of the General Assembly of the United Nations. The resolution noted that an increasing number of transactions in international trade are carried out by means of electronic data interchange and other means of communication, commonly referred to as "electronic commerce". Such means of conducting trade involve the use of alternatives to paper based methods of communication and storage of information. With a view to bring in uniformity of the law applicable to alternatives of paper-based methods of communication and storage of information, the resolution recommended that all States should give favorable consideration to the UNCITRAL Model Law when they enact or revise their laws.

Some of the objectives of the Model Law include:

- Offer national legislators, a set of internationally accepted rules on removal of traditional legal obstacles to e-Commerce and thus help in creating a more secure legal environment.
- Remedy the disadvantages caused by inadequate legislations at the national level that hinder smooth trade using electronic means of doing business.
- Enabling or facilitating the use of electronic commerce and providing equal

treatment to users of paper-based documentation and to users of computer-based information.

Accordingly the Information Technology Bill, 1999 was also drawn up taking into consideration the UNCITRAL Code.

The UNCITRAL Model Law on Electronic Commerce, as per the general provisions, applies to any kind of information in the form of a data message used in the context of commercial activities. In this regard, besides defining certain terminologies for the purpose of law, it contains the following:

- Legal recognition of data messages, admissibility and evidential weight of data messages;
- Addresses the requirement of message being "in writing" and identification of original;
- Recognizes and requires authentication of data messages through specified methods;
- Requirement relating to retention of data messages;
- Formation and validity of electronic contracts;
- Attribution of data messages, time and place of dispatch and receipt and acknowledgement of receipt;
- Provisions relating to specific areas of electronic commerce.

C. Sarbanes - Oxley Act 2002

Sarbanes-Oxley was a reactive legislative measure to the series of corporate failures involving some of the world's giant corporations such as Enron, WorldCom. The giant failures brought to light the stark failures of corporate governance and exposed the ineffective disclosure and reporting practices.

Sarbanes-Oxley or more popularly known as SOX was formally adopted as the law in 2002 and, generally, focused on publicly held companies. The legislation seeks to regulate the following:

- To enhance the requirements as regards quality and transparency of financial reporting and disclosure, and related internal controls;
- To require that independent accounting firms conducting the assurance assignments shall not have any other consulting or other relationship with the auditee organization;
- To formally endorse the accounting standards and practices. As a result the Public Company Accounting Oversight Board (PCAOB) was formed;
- To increase the corporate responsibility and accountability.

SOX contains eleven titles containing several sections, which describe specific mandates and requirements for financial reporting:

1. Public Company Accounting Oversight Board (PCAOB)
2. Auditor Independence
3. Corporate Responsibility
4. Enhanced Financial Disclosures
5. Analyst Conflicts of Interest
6. Commission Resources and Authority
7. Studies and Reports
8. Corporate and Criminal Fraud Accountability
9. White Collar Crime Penalty Enhancement
10. Corporate Tax Returns
11. Corporate Fraud Accountability.

The requirements are primarily driven by two sections viz. section 302 and 404 of the SOX, which specifically require public companies to establish, implement and evaluate their internal controls relating to financial reporting, operating integrity and disclosure.

Section 302: Corporate Responsibility for Financial Reports

The section requires that the CEO and CFO of each issuer shall prepare a statement to accompany the audit report to certify the "appropriateness of the financial statements and disclosures contained in the periodic report, and that those financial statements and disclosures fairly present, in all material respect, the operations and financial condition of the issuer." The statement must also certify that the signing officers are responsible for internal controls and have evaluated the same within previous ninety days and have reported on their findings. A violation of this section must be knowing and intentional to give rise to liability.

Section 404: Management Assessment of Internal Controls

Requires each annual report of an issuer to contain an "internal control report", which shall:

(1) State the responsibility of the management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
(2) Contain an assessment, as of the end of the most recent fiscal year of the company, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Each issuer's auditor shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this section shall be in accordance with standards for attestation engagements issued or adopted by

the Board. An attestation engagement shall not be the subject of a separate engagement.

Internal Control & COSO

Integrated Framework was prepared in response to recommendations of the National Commission on Fraudulent Financial Reporting. **Committee of Sponsoring Organizations (COSO)** of the Treadway Commission was formed to support implementation of the Treadway Commission's recommendations and published the completed Internal Control Integrated Framework. Internal Control Integrated Framework states that internal control is a process established by an entity's Board of Directors, the management, and other personnel designed to provide reasonable assurance regarding the achievement of stated objectives. COSO has released an Enterprise Risk Management (ERM) Framework for public comment that details essential components and concepts of enterprise risk management for all organizations, regardless of size. The Framework also identifies the interrelationships between enterprise risk management and internal control. SEC (Securities and Exchange Commission) recognizes the COSO Framework.

COSO report states that "The core of any business is its people – their individual attributes, including integrity, ethical values and competence – and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests."

According to COSO, the three primary objectives of an internal control system are to ensure (1) efficient and effective operations, (2) accurate and reliable financial reporting, and (3) compliance with applicable laws and regulations. The report also outlines five essential components of an effective internal control system:

- **Control Environment** – It establishes the foundation for the internal control system by providing fundamental discipline and structure.
- **Risk Assessment** – It involves the identification and analysis of relevant risks to achieving predetermined objectives.
- **Control Activities** – They are the policies and procedures that ensure that the management objectives are achieved and risk mitigation strategies are carried out.
- **Information and Communication** – It supports all other control components by communicating control responsibilities to employees and by providing information in a form and time frame that allows personnel to discharge their duties effectively.
- **Monitoring** – It covers the external oversight of internal controls by the

management or other parties outside the process; or the application of independent methodologies, like customized procedures or standard checklists, by employees within a process; to ensure that the controls operate reliably over time.

These five components are simply the actions necessary to achieve the three objectives.

Criminal Penalties and Protection

The law creates tough penalties for those who destroy records, commit securities fraud and fail to report fraud.

- Failure to Maintain Workpapers. It is now a felony with penalties of up to 10 years to willfully fail to maintain "all audit or review work- papers" for at least five years. The SEC will establish a rule covering the retention of audit records and the Board will issue standards that compel auditors to keep other documentation for seven years.
- Document Destruction. It is a felony with penalties of up to 20 years to destroy documents in a federal or bankruptcy investigation.
- Securities Fraud. Criminal penalties for securities fraud have been increased to 25 years.
- Fraud Discovery. The statute of limitations for the discovery of fraud is extended to two years from the date of discovery and five years after the act. It was previously one year from discovery and three from the act.
- Other Provisions. Other provisions protect corporate whistleblowers, ban personal loans to executives, and prohibit insider trading during blackout periods.

SOX and IT Controls

SOX has brought into focus the requirements as regards operational integrity and effectiveness of internal controls as regards financial reporting and disclosure requirements. With most organisations now critically dependent on information technology to achieve their information requirements, adequate and effective internal controls need to be implemented through information systems and general controls.

Amendments to Clause 49 of the SEBI Listing Agreement

To fall in line with the global legislative and regulatory developments on Corporate Governance, the recent amendments to Clause 49 of the Listing Agreement (proposed to be effective from December 2005) now include several stringent stipulations requiring assurance as to the accuracy of financial reporting and regarding the design and accuracy of internal controls. Such

stipulations cast significant responsibilities on the Board, Audit Committee, CEO and CFO for ensuring the adequacy and effectiveness of internal controls.

As a part of the internal control requirements relating to financial reporting controls, among other risk management provisions, the amendment requires CEO and CFO to certify that the financial statements and the information contained therein "do not contain any materially untrue statement or omit any material fact and that such statements are not misleading; present a true and fair view of the company's affairs and are in compliance with the existing standards, laws and regulations". They should also certify that no fraudulent or illegal transactions have been entered into by the company during the year.

The provision also requires the CEO and CFO to:

- Take responsibility and make themselves accountable for design of internal controls and procedures;
- To state that they have evaluated the effectiveness of the company's internal controls and procedures;
- Requires them to disclose to the company's auditors/audit committee, all significant deficiencies in design or operation of internal controls relating to financial disclosures;
- Identify and report to the auditors:
    - Any significant fraud, whether material or not, and the involvement, if any, of the management or employees having significant role in the company's internal control system.
    - Significant changes in internal controls and related factors and corrective actions as regards significant deficiencies or material weaknesses.
    - Significant changes in accounting policies during the year.

The amendments to clause 49 of the listing agreement, now make corporate executives take explicit responsibility for establishing a system of internal controls over financial reporting and evaluating and monitoring the effectiveness of such internal controls. With most organizations entirely or significantly dependent on Information Technology for the collation of financial information and financial reporting, controls over IT have become an inherent part of internal control requirement. This creates a challenge in terms of accountability of the management with regard to quality and integrity of financial information generated using information technology. Hence, as a part of internal controls requirements, many concerns, requirements and responsibilities arise in terms of IT control requirements, some of these include:

- Understanding the internal controls relating to financial reporting from IT perspective;
- Identification of risks arising from the use of IT for financial reporting depending on the complexity and nature of such implementations;
- Identification of software applications and other technology components that deliver to financial reporting objectives, whether directly or indirectly;
- Evaluation of internal control framework with regard to design of IT controls, risk management and monitoring;
- Evaluation of adequacy and efficacy of internal controls and related IT controls.

D. Basel II Framework for Risk Management

A significant global development that is set to critically impact the

Banking Sector is the revision of the framework of standards for establishing minimum capital requirements for banking organisation or more commonly referred to as the Basel II Framework, prepared by the Basel Committee on Banking Supervision. The objective of the new framework is to encourage financial firms to be more proactive and forward looking in their financial activities.

Basel II seeks to further regulate the minimum capital requirements for banks, which serves as the foundation for a bank's future business and a fall back in case of unexpected losses. What is the minimum capital for a bank is often a highly dicey and technical issue, which is determined by a score of factors.

A revision to the earlier Basel Framework was necessitated by the significant advances in banking industry worldwide and the much needed changes in risk management practices, use of technology and changing banking markets.

Good risk management and supervision practices are a key component of the success of a banking organization. Realizing the need for appropriate and sophisticated risk management practices, the Basel II provides for the state of such practices being reflected in the capital regulations.

This promotes and encourages improved risk management practices further strengthening the stability of the financial system.

As against the single financial oriental basis provided by earlier Basel Accord, Basel II has introduced 3 pillars, each complementing and supplementing the others and enables banks to enhance the quality of their internal processes. Such pillars focus on minimum capital requirements, supervisory review and market discipline. It is also essential, as a part of the bank's management process, to provide for adequate capital to protect against overall risks, which

besides credit and market risks, to a significant extent includes operational risks.

Operational risks are risks that result from inadequate or failed internal processes, people and systems from external events. Use of sophisticated systems like CBS has introduced the need for real-time monitoring so that suitable supervisory actions can be triggered on a timely basis.

Adequate controls need to be in place to ensure that all transactions are captured, processed and recorded safely, accurately and confidentially. Measurement and management of operational risks as per Basel II requires suitable systems for identification, capture, storage, analysis, retrieval and dynamic reporting of the data relating to operational risk.

Summary

This chapter gives us an overview of the Information Systems Audit Regulations and standards. COBIT- IT Governance Model is discussed in detail with some other global standards of IS Assurance and Audit standards – BS 7799 & ISO 27001, SAS 70, SysTrust. Overview of Regulatory developments like ITA 2000, Govt. Of India, the UNCITRAL Code, Sarbanes – Oxley Act etc., which are the impacting controls on a computerized environment were highlighted.

Questions

1. Enhanced risk awareness and more emphasis on the importance of good risk measurement and management and properly ensured appropriate capital reserve requirements is a requirement of _____.
   a. SysTrust
   b. Basel II Capital Accord
   c. COBIT
   d. ISO/IES 17799:2005

2. IT audit and assurance standards _____.
   a. Specify the manner in which an IT audit and assurance should be carried out
   b. Provide recommendations on improvement of audit performance
   c. Provide IT audit and assurance professionals with a clear idea of the minimum level of acceptable performance
   d. Provide guidance to professionals on performing IT audit and assurance in specified environments

3. CIS under AAS 29 of ICAI refers to _____.
   a. Continuous and Systematic Information

b. Continuous and Intermittent Simulation
c. Computerized Information Systems
d. Computerized Information Sources

4. COBIT is _____.
   a. A standard to be followed by IS auditors while conducting IS Audit
   b. A comprehensive standard for IT Governance
   c. A multi-purpose audit tool for testing application controls
   d. A standard for Corporate Governance

5. An organization seeks to get its Information Security Management Systems certified by an independent certifying agency. Which of the following standards would be useful in this regard?
   a. COBIT
   b. SAS 70
   c. BS7799
   d. ITIL

6. IT Infrastructure Library (ITIL) deals with _____.
   a. Information technology controls for organizations requiring secure implementation
   b. Best practices for quality of IT services and their management
   c. A governance model for management of IT
   d. Internal controls in Information Technology for integrity of financial reporting

7. The Information Technology Act _____.
   a. Defines the method of authentication of an electronic record
   b. Provides for authentication of all electronic records using digital signature
   c. Encourages the use of digital signatures for all Government transactions
   d. Requires the use of electronic signatures using symmetric cryptography

8. The Information Technology Act does not apply to all of the following, except _____.
   a. An e-banking mechanism used instead of a cheque
   b. A will
   c. Electronic contract for sale of building
   d. Notification of documents in the Government Gazette through electronic means

9. Which of the following is not an offence under the IT Act, 2000?
   a. Introducing a virus into the network of an organization
   b. Providing assistance to any person to facilitate unauthorized access to any computer system
   c. Creating a software to cause denial-of-service attack
   d. Damaging the computer system by changing an operating system parameter with a view to cause disruption to business

10. Which of the following would qualify to be a requirement under the IT Act, 2000?
   a. Requiring signatures on all documents generated
   b. Controls over time and date stamping of data messages
   c. Controls over physical security of computer equipment
   d. Use of standard software for firewalls

11. Sarbanes-Oxley Act 2002 seeks to regulate _____.
   a. Control requirements relating to Information Technology governance and controls, especially those relating to financial disclosure controls
   b. To enhance requirements as regards quality and transparency of financial reporting and disclosure and related internal controls and corporate responsibility thereof
   c. To empower audit committees
   d. To check the rate of growing computer crime

12. An IT audit and assurance professional issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The professional has failed to exercise _____.
   a. Professional independence
   b. Organizational independence
   c. Technical competence
   d. Professional competence

13. According to the Committee of Sponsoring Organizations (COSO), the internal control framework consists of which of the following?
   a. Processes, people, objectives
   b. Profits, products, processes
   c. Costs, revenues, margins
   d. Return on investment, earnings per share, market share

14. According to the COSO report, the correct sequence is_____.
   a. Risks, objectives, actions

b. Actions, objectives, risks
c. Objectives, risks, actions
d. Objectives, actions, risks

15. According to the COSO report, the core of an organization is which of the following?
a. Products
b. Processes
c. People
d. Profits

16. According to the COBIT, control includes all of the following except ___.
a. Policies
b. Procedures
c. Programs
d. Practices

17. COBIT is the model for _____.
a. IT planning
b. IT governance
c. IT standards
d. IT infrastructure

18. According to COBIT, IT resources do not specifically refer to which of the following?
a. Capital
b. Data
c. Technology
d. Facilities

19. According to COBIT, control objectives are defined in a _____ manner.
a. Product-oriented
b. Policy-oriented
c. Process-oriented
d. Control-oriented

20. Which of the following can serve as an educational tool and provide for flexibility?
a. Policies
b. Guidelines
c. Standards
d. Principles

21. "Assess the adequacy of internal control" appears under which domain of COBIT:
    a. Planning and Organization
    b. Acquisition and Implementation
    c. Delivery and Support
    d. Monitoring

22. According to COBIT, an IS auditor's role in acquiring and maintaining application software is to _____.
    a. Evaluate and support
    b. Evaluate
    c. Support
    d. Assess

23. The four-prong approach of audit, devised by COBIT is _____.
    a. Obtaining, evaluating, assessing, and substantiating
    b. Evaluating, assessing, monitoring, and substantiating
    c. Assessing, evaluating, substantiating, and reporting
    d. Evaluating, assessing, monitoring, and substantiating

24. According to section 404 of Sarbanes-Oxley Act, the management of a company must accept responsibility for the effectiveness of the company's internal control over its financial reporting. Which of the following is not also a responsibility of the management?
    a. Must provide a written plan each year for updating the internal control over the financial reporting
    b. Must evaluate the actual effectiveness of internal control over the financial reporting
    c. Must support the evaluation of internal control over the financial reporting with sufficient documented evidence
    d. Must prepare a written assessment of internal control over the financial reporting

25. The Planning and Organization domain of the COBIT model includes all of the following except _____.
    a. Project management standards
    b. Architecture planning process
    c. Strategic planning process
    d. Operational readiness process

26. The main theme of COBIT is _____.
    a. Control orientation
    b. Audit orientation

c. Technical orientation
d. Business orientation

27. All of the following are SysTrust's principles except _____.
a. Integrity
b. Confidentiality
c. Availability
d. Security

28. Which of these is an objective of UNCITRAL Model Law?
a. To give certification to an ISMS
b. To increase corporate responsibility and accountability
c. To bring in uniformity of the law applicable to alternatives of paper-based methods of communication
d. To standardize IT service management process

29. An ISMS that ____can be given an external ISO 27001 certification.
a. Complies with the specification given in ISO 27001
b. Follows the practices identified in ISO 17799 Code of Practice
c. Both A and B
d. Neither A nor B

30. SAS 70 was developed by _____.
a. AICPA
b. BSI
c. CCTA
d. ISACF

31. Which of these is not specified in ISO 20000-Part 1?
a. Relationship processes
b. Risk management processes
c. Control processes
d. Release processes

Answers

1 b	2 c	3 c	4 b	5 c	6 b	7 a	8 a	9 c
10 d	11 b	12 a	13 a	14 c	15 c	16 c	17 b	18 a
19 c	20 b	21 d	22 a	23 a	24 a	25 c	26 d	27 b
28 c	29 c	30 a	31 b					