

ISO 27001 – (BS7799 : Part II) – Information Security Management Standard

The requirements of information security system as described by standard are stated below. An organisation must take a clear view on these issues before trying to implement an Information Security Management Systems (ISMS).

General: Organisation shall establish and maintain documented ISMS addressing assets to be protected, organisations approach to risk management, control objectives and control, and degree of assurance required.

Establishing Management Framework :

This would include

- Define information security policy;
- Define scope of ISMS including functional, asset, technical, and locational boundaries;
- Make appropriate risk assessment ;
- Identify areas of risk to be managed and degree of assurance required;
- Select appropriate controls;
- Prepare Statement of Applicability,

Implementation : Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.

Documentation : The documentation shall consist of evidence of action undertaken under establishment of the following

- Management control
- Management framework summary, security policy, control objective, and implemented
- control given in prepare Statement of Applicability
- Procedure adopted to implement control under Implementation clause
- ISMS management procedure
- Document Control: The issues focused under this clause would be
 - Ready availability
 - Periodic review
 - Maintain version control;
 - Withdrawal when obsolete
 - Preservation for legal purpose
- Records : The issues involved in record maintenance are as follows:
 - Maintain to evidence compliance to Part 2 of BS7799.;
 - Procedure for identifying, maintaining, retaining, & disposing of such evidence;
 - Records to be legible, identifiable and traceable to activity involved.
 - Storage to augment retrieval, and protection against damage.

Areas of focus of ISMS :

There are ten areas of focus of ISMS. These are described in the following paragraphs:

- (i) **Security Policy :** This activity involves a thorough understanding of the organization business goals and its dependence on information security. It should be implement able, easy to understand and must balance the level of protection with productivity.

The policy should cover

- a definition of information security
- a statement of management intention supporting the goals and principles of information security
- allocation of responsibilities for every aspect of implementation
- an explanation of specific applicable proprietary and general, principles, standards and compliance requirements.
- an explanation of the process for reporting of suspected security incidents
- a defined review process for maintaining the policy document
- means for assessing the effectiveness of the policy embracing cost and technological changes
- nomination of the policy owner

The detailed **control and objectives** are as follows:

- *Information Security Policy:* To provide management direction and support for information security
- *Information System Infrastructure:* To manage information security within the organisation
- *Security of third party access:* To maintain the security of organisational information processing facilities and information assets accessed by third parties.
- *Outsourcing:* To maintain the security of information when the responsibility for information processing has been outsourced to another organisation

- (ii) **Organisational Security :**

A management framework needs to be established to initiate, implement and control information security within the organization. This needs proper procedures for approval of the information security policy, assigning of the security roles and coordination of security across the organization.

The detailed **control and objectives** are as follows :

- *Information System Infrastructure :* To manage information security within the organisation.
- *Security of third party access :* To maintain the security of organisational information processing facilities and information assets accessed by third parties.
- *Outsourcing :* To maintain the security of information when the responsibility for information processing has been outsourced to another organisation.

- (iii) **Asset Classification and Control** : One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, which is appropriate for copy, store, transmit or destruction of the information asset.

An Information Asset Register (IAR) should be created. detailing every information asset within the organisation. For example:

- Databases
- Personnel records
- Scale models
- Prototypes
- Test samples
- Contracts
- Software licenses
- Publicity material

The Information Asset Register (IAR) should also describe who is responsible for each information asset and whether there is any special requirement for confidentiality, integrity or availability. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. 'Media Register' will detail the stock of software and its licenses.

The detailed **control and objectives** thereof are as follows :

- *Accountability for assets* : To maintain appropriate protection of organisational assets
- *Information Classification* : To ensure that information assets receive an appropriate level of protection

- (iv) **Personnel Security** : Human errors, negligence and greed are responsible for most thefts, frauds or misuse of facilities. Various proactive measures that should be taken are, to make personnel screening policies, confidentiality agreements, terms and conditions of employment, and information security education and training. Alert and well-trained employees who are aware of what to look for can prevent future security breaches.

Appropriate personnel security ensures that :

- Employment contracts and staff handbooks have agreed, clear wording
- Ancillary workers, temporary staff, contractors and third parties are covered
- Anyone else with legitimate access to business information or systems is covered.

Staff training is an important feature of personnel security to ensure the Information Security Management System (ISMS) continues to be effective. Periodically, refreshers on less frequently used parts of the Information Security Management System (ISMS), such as its role in disaster recovery plans, can make a major difference when there is a need to put the theory into practice. Disaster management is a team effort and not the responsibility of a single department or person.

The detailed control and objectives thereof are as follows:

- *Security in Job definition and Resourcing* : To reduce the risks of human error, theft, fraud, or misuse of facilities .
- *User Training* : To ensure that users are aware of information security threats and concerns, and are equipped to support organisational security policy in course of their normal work
- *Responding to security incidents and malfunctions* : To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents

- (v) **Physical and Environmental Security** : Designing a secure physical environment to prevent unauthorized access, damage and interference to business premises and information is usually the beginning point of any security plan. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risks ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables are some of the activities.

The detailed **control and objectives** thereof are as follows:

- *Secure areas*: To prevent unauthorized access, damage and interference to business premises and information
- *Equipment Security*: To prevent loss, damage or compromise of assets and interruption to business activities
- *General Controls*: To prevent compromise or theft of information and information processing facilities

- (vi) **Communications and Operations Management** :

- Properly documented procedures for the management and operation of all information processing facilities should be established. This includes detailed operating instructions and incident response procedures.
- Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks.
- Special controls may also be required to maintain the availability of the network services.

- Exchange of information and software between external organizations should be controlled, and should be compliant with any relevant legislation.
- There should be proper information and software exchange agreements, the media in transit need to be secure and should not be vulnerable to unauthorized access, misuse or corruption.
- Electronic commerce involves electronic data interchange, electronic mail and online transactions across public networks such as Internet.

The detailed **control and objectives** thereof are as follows :

- *Operational procedures and responsibilities* : To ensure correct and secure operation of information processing facility
- *System planning and acceptance* : To minimise risks of system failure
- *Protection against malicious software* : To protect the integrity of software and info
- *Housekeeping* : To maintain the integrity and availability of information processing and communication services
- *Network Management* : To ensure the safeguarding of information in networks and the protection of the supporting infrastructure
- *Media handling and security* : Prevent damage to assets and interruptions to business activity
- *Exchanges of information and software* : To prevent loss, modification or misuse of information exchanged between organisations

(vii) Access Control : Access to information and business processes should be controlled on the business and security requirements. This will include

- defining access control policy and rules, user access management, user registration, privilege management, user password use and management, review of user access rights, network access controls, enforcing path from user terminal to computer, user authentication.
- node authentication, segregation of networks, network connection control, network routing control.
- operating system access control, user identification and authentication, use of system utilities, application access control, monitoring system access and use and ensuring information security when using mobile computing and tele-working facilities.

The detailed **control and objectives** thereof are as follows:

- *Business requirement for access control* : To control access to information
- *User access management* : To prevent unauthorised access to info systems
- *User responsibilities* : To prevent unauthorised user access
- *Network access control* : Protection of networked services
- *Operating system access control* : To prevent unauthorised computer access
- *Application Access Control* : To prevent unauthorised access to information held in information systems
- *Monitoring System Access and use* : To detect unauthorised activities
- *Mobile Computing and teleworking* : To ensure information security when using mobile computing & teleworking facilities

- (viii) **Systems Development and Maintenance** : Security should ideally be built at the time of inception of a system. Hence security requirements should be identified and agreed prior to the development of information systems. This begins with security requirements analysis and specification and providing controls at every stage i.e. data input, data processing, data storage and retrieval and data output. It may be necessary to build applications with cryptographic controls. There should be a defined policy on the use of such controls, which may involve encryption, digital signature, use of digital certificates, protection of cryptographic keys and standards to be used for cryptography. A strict change control procedure should be in place to facilitate tracking of changes. Any changes to operating system changes, software packages should be strictly controlled. Special precaution must be taken to ensure that no covert channels, back doors or Trojans are left in the application system for later exploitation.

The detailed **control and objectives** thereof are as follows:

- *Security requirements of system* : To ensure that security is built into information systems
- *Security in application systems* : To prevent loss, modification or misuse of user data in application system
- *Cryptographic Controls* : To protect the confidentiality, authenticity or integrity of information
- *Security of system files* : To ensure that IT projects and support activities are conducted in a secure manner
- *Security in development and support process* : To maintain the security of application system software and information

- (ix) **Business Continuity Management** : A business continuity management process should be designed, implemented and periodically tested to reduce the disruption caused by disasters and security failures. This begins by identifying all events that could cause interruptions to business processes and depending on the risk assessment, preparation of a strategy plan. The plan needs to be periodically tested, maintained and re-assessed based on changing circumstances

There is one control which is described here in below along with its objectives:

- *Aspects of business continuity management* : To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

- (x) **Compliance** : It is essential that strict adherence is observed to the provision of national and international IT laws, pertaining to Intellectual Property Rights (IPR), software copyrights, safeguarding of organizational records, data protection and privacy of personal information, prevention of misuse of information processing facilities, regulation of cryptographic controls and collection of evidence. Information Technology's use in business has also resulted in enacting of laws that enforce responsibility of compliance. All legal requirements must be complied with to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations and of any security requirements.

The detailed **control and objectives** thereof are as follows:

- *Compliance with legal requirements* : To avoid breaches of any criminal and civil law, and statutory, regulatory, or contractual obligations, and of any security requirements
- *Review of security policy and technical compliance* : To ensure compliance of systems with organisational security policies and standards
- *System Audit Consideration* : To maximise the effectiveness, and to minimise interference to / from the system audit process.

CMM - CAPABILITY MATURITY MODEL

The CMM presents sets of recommended practices in a number of key process areas that have been shown to enhance software process capability. The CMM is based on knowledge acquired from software process assessments and extensive feedback from both industry and government.

The Capability Maturity Model for Software provides software organizations with guidance on how to gain control of their processes for developing and maintaining software and how to evolve toward a culture of software engineering and management excellence.

Fundamental Concepts Underlying Process – Maturity : A software process can be defined as a set of activities, methods, practices, and transformations that people use to develop and maintain software and the associated products (e.g., 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.
- **Software process performance** represents the actual results achieved by following a software process. Thus, software process performance focuses on the results achieved, while software process capability focuses on results expected.
- **Software process maturity** is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization. As a software organization gains in software process maturity, it institutionalizes its software process via policies, standards, and organizational structures.

The Five Levels of Software Process Maturity

Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The CMM provides a framework for organizing these evolutionary steps into five maturity levels that lay successive foundations for continuous process improvement. The levels also help an organization prioritize its improvement efforts.

- (i) Level 1 - The Initial Level :** At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. Success depends entirely on having an exceptional manager and a seasoned and effective software team. Success in Level 1 organizations depends on the competence and heroics of the people in the organization and cannot be repeated unless the same competent individuals are assigned to the next project. Thus, at Level 1, capability is a characteristic of the individuals, not of the organization.
- (ii) Level 2 - The Repeatable Level :** At the Repeatable Level, policies for managing a software project and procedures to implement those policies are established. Planning and managing new projects is based on experience with similar projects. Projects in Level 2 organizations have installed basic software management controls. Realistic project commitments are based on the results observed on previous projects and on the requirements of the current project. The software managers for a project track software costs, schedules, and functionality; problems in meeting commitments are identified when they arise. The software process capability of Level 2 organizations can be summarized as disciplined because planning and tracking of the software project is stable and earlier successes can be repeated. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.
- (iii) Level 3 - The Defined Level :** At the Defined Level, the standard process for developing and maintaining software across the organization is documented, including both software engineering and management processes, and these processes are integrated into a coherent whole. This standard process is referred to throughout the CMM as the organization's standard software process. Processes established at Level 3 are used (and changed, as appropriate) to help the software managers and technical staff perform more effectively. The organization exploits effective software engineering practices when standardizing its software processes. Projects tailor the organization's standard software process to develop their own defined software process, which accounts for the unique characteristics of the project.

The software process capability of Level 3 organizations can be summarized as standard and consistent because both software engineering and management activities are stable and repeatable. Within established product lines, cost, schedule, and functionality are under control, and software quality is tracked. This process capability is based on a common, organization-wide understanding of the activities, roles, and responsibilities in a defined software process.

- (iv) **Level 4 - The Managed Level :** At the Managed Level, the organization sets quantitative quality goals for both software products and processes. Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes. Software processes are instrumented with well-defined and consistent measurements at Level 4. The software process capability of level 4 organizations can be summarized as being quantifiable and predictable because the process is measured and operates within measurable limits. This level of process capability allows an organization to predict trends in process and product quality within the quantitative bounds of these limits. Because the process is both stable and measured, when some exceptional circumstance occurs, the "special cause" of the variation can be identified and addressed. When the known limits of the process are exceeded, action is taken to correct the situation. Software products are of predictably high quality.
- (v) **Level 5 - The Optimizing Level :** At the Optimizing Level, the entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Software project teams in Level 5 organizations analyze defects to determine their causes. Software processes are evaluated to prevent known types of defects from recurring, and lessons learned are disseminated to other projects. The software process capability of Level 5 organizations can be characterized as continuously improving because Level 5 organizations are continuously striving to improve the range of their process capability, thereby improving the process performance of their projects. Improvement occurs both by incremental advancements in the existing process and by innovations using new technologies and methods. Technology and process improvements are planned and managed as ordinary business activities.

COCO

- The "Guidance on Control" report, known colloquially as CoCo, was produced in 1999 by the Criteria of Control Board of The Canadian Institute of Chartered Accountants.
- CoCo is "guidance," meaning that it is not intended as "prescriptive minimum requirements" but rather as "useful in making judgments" about "designing, assessing and reporting on the control systems of organizations."
- CoCo can be said to be a concise superset of COSO.
- It uses the same three categories of objectives:
 - effectiveness and efficiency of operations
 - reliability of financial reporting
 - compliance with applicable laws and regulations

- CoCo states that the “essence of control is purpose, capability, commitment, and monitoring and learning,”
- Four important concepts about “control” are as follows :
 - o Control is affected by people throughout the organization, including the board of directors (or its equivalent), management and all other staff.
 - o People who are accountable, as individuals or teams, for achieving objectives should also be accountable for the effectiveness of control that supports achievement of those objectives.
 - o Organizations are constantly interacting and adapting.
 - o Control can be expected to provide only reasonable assurance, not absolute assurance.

ITIL (IT INFRASTRUCTURE LIBRARY)

The IT Infrastructure Library (ITIL) is so named as it originated as a collection of books (standards) each covering a specific 'practice' within IT management. After the initial published works, the number of publications quickly grew (within ITIL v1) to over 30 books.

The eight ITIL books and their disciplines are:

The **IT Service Management** sets relating to

1. Service Delivery
2. Service Support
3. ICT Infrastructure Management
4. Security Management
5. The Business Perspective
6. Application Management
7. Software Asset Management
8. Planning to Implement Service Management

Details of the ITIL Framework

- (a) The **Service Support** ITIL discipline is focused on the User of the ICT services and is primarily concerned with ensuring that they have access to the appropriate services to support the business functions. The service desk will try to resolve it, if there is a direct solution or will create an incident.
- (b) The goal of **Problem Management** is to resolve the root cause of incidents and thus to minimize the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors.

- (c) Configuration Management** is a process that tracks all of the individual Configuration Items (CI) in a system. A system may be as simple as a single server, or as complex as the entire IT department.

Configuration Management includes:

- Creating a parts list of every CI (hardware or software) in the system.
- Defining the relationship of CIs in the system
- Tracking of the status of each CI, both its current status and its history.
- Tracking all Requests for Change to the system.
- Verifying and ensuring that the CI parts list is complete and correct.

There are five basic activities in configuration management:

- Planning
- Identification
- Control
- Status accounting
- Verification and Audit

- (d) Release Management** is used for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Quality control during the development and implementation of new hardware and software is also the responsibility of Release Management.

The goals of release management are:

- Plan to rollout of software
- Design and implement procedures for the distribution and installation of changes to IT systems
- Effectively communicate and manage expectations of the customer during the planning and rollout of new releases
- Control the distribution and installation of changes to IT systems

- (e) Service Delivery :** The Service Delivery discipline is primarily concerned with the proactive and forward-looking services that the business requires of its ICT provider in order to provide adequate support to the business users.

The discipline consists of the following processes, explained in subsections below:

- Service Level Management
- Capacity Management
- IT Service Continuity Management
- Availability Management
- Financial Management

- (f) **Service Level Management** : Service Level Management provides for continual identification, monitoring and review of the levels of IT services specified in the Service Level Agreements (SLAs). The process involves assessing the impact of change upon service quality and SLAs.
- (g) **Capacity Management** : Capacity Management supports the optimum and cost effective provision of IT services by helping organizations match their IT resources to the business demands. The high-level activities are Application Sizing, Workload Management, etc.
- (h) **Security Management** : The ITIL-process Security Management describes the structured fitting of information security in the management organization. ITIL Security Management is based on the code of practice for information security management also known as ISO/IEC 17799. When protecting information it is the value of the information that has to be protected. These values are stipulated by the confidentiality, integrity and availability. Inferred aspects are privacy, anonymity and verifiability.
- (i) **ICT Infrastructure Management** : ICT Infrastructure Management processes recommend best practice for customers. They are following
- ICT Design and Planning
 - ICT Deployment
 - ICT Operations
 - ICT Technical Support
- The Infrastructure Management processes describe those processes within ITIL that directly relate to the ICT equipment and software that is involved in providing ICT services to
- (j) **The Business Perspective** : The Business Perspective is the name given to the collection of best practices that is suggested to address some of the issues often encountered in understanding and improving IT service provision, as a part of the entire business requirement for high IS quality management. These issues are:
- Business Continuity Management describes the responsibilities and opportunities available to the business manager to improve what is, in most organizations one of the key contributing services to business efficiency and effectiveness.
 - Surviving Change. It is important that business managers take notice of these changes and ensure that steps are taken to safeguard the business from adverse side effects.
 - Transformation of business practice through radical change helps to control IT and to integrate it with the business.
 - Partnerships and outsourcing

(k) Application Management : ITIL Application Management set encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet business objectives.

(l) Software Asset Management :

Software Asset Management is a part of overall IT Service Management best illustrated by the IT Infrastructure Library (ITIL) guides, which is the mostly widely accepted approach to providing a comprehensive and consistent set of best practices. Good Software Asset Management achieved through Best Practice enables organisations to save money through effective policies and procedures which are continuously reviewed and improved

SYSTRUST AND WEBTRUST

SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and Criteria.

- **SysTrust** engagements are designed for the provision or advisory services or assurance on the reliability of a system.
- **WebTrust** engagements relate to assurance or advisory services on an organization's system related to
- e-commerce.
- Only certified public accountants (CPAs) may provide the assurance and in order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.

The following principles

- *Security.* The system is protected against unauthorized access (both physical and logical).
- *Availability.* The system is available for operation and use as committed or agreed.
- *Processing integrity.* System processing is complete, accurate, timely, and authorized.
- *Online privacy.* Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.
- *Confidentiality.* Information designated as confidential is protected as committed or agreed.

Each of these Principles and Criteria are organized and presented in four broad areas:

- *Policies.* The entity has defined and documented its policies relevant to the particular principle.
- *Communications.* The entity has communicated its defined policies to authorized users.
- *Procedures.* The entity uses procedures to achieve its objectives in accordance with its defined policies.
- *Monitoring.* The entity monitors the system and takes action to maintain compliance with its defined policies.

At the completion of a SysTrust engagement, the practitioner renders an opinion on the management's assertion that effective controls have been maintained.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. Congress in 1996.

- Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.
- Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data.

The Security Rule :

The Security lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule.

The standards and specifications are as follows:

- (a) Administrative Safeguards :** policies and procedures designed to clearly show how the entity will comply with the act
- Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies & procedures.
 - The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
 - Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI).
 - The procedures must address access authorization, establishment, modification, and termination.
 - must show that an appropriate ongoing training program regarding the handling PHI is provided to employees performing health plan administrative functions.
 - Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements.
 - A contingency plan should be in place for responding to emergencies.
 - Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations.
 - Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

(b) Physical Safeguards :

- controlling physical access to protect against inappropriate access to protected data
- Controls must govern the introduction and removal of hardware and software from the network.
- Access to equipment containing health information should be carefully controlled and monitored.
- Access to hardware and software must be limited to properly authorized individuals.
- Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
- Policies are required to address proper workstation use.
- If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

(c) Technical Safeguards :

- controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient .
- Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized.
- Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
- Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
- Covered entities must also authenticate entities it communicates with. Authentication consists password systems, two or three-way handshakes, telephone call-back, and token systems.
- Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
- information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
- Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act.

SAS 70–STATEMENT OF AUDITING STANDARDS FOR SERVICE ORGANISATIONS

- Statement on Auditing Standards (SAS) No. 70, Service Organizations, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA).
- A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.
- A formal report including the auditor's opinion ("Service Auditor's Report") is issued to the service organization at the conclusion of a SAS 70 examination.
- SAS 70 provides guidance to enable an independent auditor ("service auditor") to issue an opinion on a service organization's description of controls through a Service Auditor's Report.
- Service auditors are required to follow the AICPA's standards for fieldwork, quality control, and reporting.
- A SAS 70 examination is not a "checklist" audit.
- SAS No. 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"). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centres, Internet data centres, or other data processing service bureaus.

Service Auditor's Reports : One of the most effective ways a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports:

- A Type I report describes the service organization's description of controls at a specific point in time (e.g. June 30, 2003).
- 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 minimum six month period (e.g. January 1, 2003 to June 30, 2003).

Benefits to the Service Organization :

- A Service Auditor's Report with an unqualified opinion that is issued by an Independent Accounting Firm differentiates the service organization from its peers by demonstrating the establishment of effectively designed control objectives and control activities.
- A Service Auditor's Report also helps a service organization build trust with its user organizations (i.e. customers).
- A Service Auditor's Report ensures that all user organizations and their auditors have access to the same information and in many cases this will satisfy the user auditor's requirements.
- SAS 70 engagements are generally performed by control oriented professionals who have experience in accounting, auditing, and information security.
- A SAS 70 engagement allows a service organization to have its control policies & procedures evaluated and tested (in the case of a Type II engagement) by an independent party.

Benefits to the User Organization :

- User organizations that obtain a Service Auditor's Report from their service organization(s) receive valuable information regarding the service organization's controls and the effectiveness of those controls.
- The user organization receives a detailed description of the service organization's controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively (in the case of a Type II report).

COBIT – IT GOVERNANCE MODEL

Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology (IT) management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1996. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

COBIT 4.1 has 34 high level processes that cover 210 control objectives categorized in four domains: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring and Evaluation.

COBIT provides benefits to managers, IT users, and auditors. Managers' benefit from COBIT as it provides them with a foundation upon which IT related decisions and investments can be based. Decision making is more effective because COBIT aids management in defining a strategic IT plan, defining the information architecture, acquiring the necessary IT hardware and software to execute an IT strategy, ensuring continuous service, and monitoring the performance of the IT system.

Executive summary

Sound business decisions are based on timely, relevant and concise information. Specifically designed for time-pressed senior executives and managers, the COBIT Executive Summary consists of an Executive Overview, which provides a thorough awareness and understanding of COBIT's key concepts and principles. Also included is a synopsis of the Framework, which provides a more detailed understanding of these concepts and principles, while identifying COBIT's four domains (Planning and Organization, Acquisition and Implementation, Delivery and Support, Monitoring and Evaluation) and the 34 IT processes.

Framework

A successful organization is built on a solid framework of data and information. The Framework explains how IT processes deliver the information that the business needs to achieve its objectives. This delivery is controlled through 34 high-level control objectives, one for each IT process, contained in the four domains. The Framework identifies which of the seven Information Criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability), as well as which IT resources (people, applications, information and infrastructure) are important for the IT processes to fully support business.

Control Objectives

The key to maintaining profitability in a technologically changing environment is how well we maintain control. COBIT's Control Objectives provides the critical insight needed to delineate a clear policy and good practice for IT controls. Included are the statements of desired results or purposes to be achieved by implementing the 210 specific and detailed control objectives throughout the 34 high-level IT processes.

Management Guidelines

To ensure a successful enterprise, you must effectively manage the union between business processes and information systems. The new Management Guidelines are composed of Maturity Models, to help and determine the stages and expectation levels of control and compare them against industry norms; Critical Success Factors, to identify the most important actions for achieving control over the IT processes; Key Goal Indicators, to define target levels of performance; and Key Performance Indicators, to measure whether an IT control process is meeting its objective. These Management Guidelines will help to answer the questions of immediate concern to all those who have a stake in enterprise success.

IT Assurance Guide

To be certain that the control objectives are being achieved, there is an implicit need to assess the controls linked to them. The Assurance Guide provides the tools to assess the controls in every form needed, from their design to the results. The guide also allows for the assurance initiative planning and scoping in a standardized, repeatable way so that the business and IT can be assessed under a single framework, completely compatible with ISACA's ITAF. There is a misunderstanding that the Assurance Guide is the successor to the Audit Guidelines. The truth is, however, that it is a completely new book, based on the Control Practices. The Audit Guidelines is not part of COBIT anymore, as the Assurance Guide is not part of the book, but a related publication.

COBIT structure

COBIT covers four domains which are given as follows:

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

Plan and Organize

The Plan and Organize domain covers the use of information & technology and how best it can be used in a company to help achieve the company's goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT. The following table lists the IT processes contained in the Planning and Organization domain.

IT PROCESSES**Plan and Organize**

- P01 Define a Strategic IT Plan and direction
- P02 Define the Information Architecture
- P03 Determine Technological Direction
- P04 Define the IT Processes, Organization and Relationships
- P05 Manage the IT Investment
- P06 Communicate Management Aims and Direction
- P07 Manage IT Human Resources
- P08 Manage Quality
- P09 Assess and Manage IT Risks
- P010 Manage Projects

Acquire and Implement

The Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company's current business processes. This domain also addresses the development of a maintenance plan that a company should adopt in order to prolong the life of © **The Institute of Chartered Accountants of India**.

Information Systems Control and 8.18 nd Audit an IT system and its components. The following table lists the IT processes contained in the Acquire and Implement domain.

IT PROCESSES**Acquire and Implement**

- AI1 Identify Automated Solutions
- AI2 Acquire and Maintain Application Software
- AI3 Acquire and Maintain Technology Infrastructure
- AI4 Enable Operation and Use
- AI5 Procure IT Resources
- AI6 Manage Changes
- AI7 Install and Accredited Solutions and Changes

Deliver and Support

The Deliver and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results as well as the support processes that enable the effective and efficient execution of these IT systems. These support processes include security issues and training. The following table lists the IT processes contained in the Deliver and Support domain.

IT PROCESSES**Deliver and Support**

- DS1 Define and Manage Service Levels
- DS2 Manage Third-party Services
- DS3 Manage Performance and Capacity
- DS4 Ensure Continuous Service
- DS5 Ensure Systems Security
- DS6 Identify and Allocate Costs
- DS7 Educate and Train Users
- DS8 Manage Service Desk and Incidents
- DS9 Manage the Configuration
- DS10 Manage Problems
- DS11 Manage Data
- DS12 Manage the Physical Environment
- DS13 Manage Operations

Monitor and Evaluate

The Monitor and Evaluate domain deals with a company's strategy in assessing the needs of the company and whether or not the current system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company's control processes by internal and external auditors. The following table lists the IT processes contained in the Monitor and Evaluate domain.

IT PROCESSES**Monitor and Evaluate**

- ME1 Monitor and Evaluate IT Processes
- ME2 Monitor and Evaluate Internal Control
- ME3 Ensure Regulatory Compliance
- ME4 Provide IT Governance

COBIT and other standards

COBIT, Val IT and Risk IT: Building on the success of COBIT, and focusing on key IT governance areas of value delivery and risk management, ISACA developed two additional IT governance frameworks, Val IT™ and Risk IT. These frameworks are closely aligned with and complement COBIT, but deliver value to enterprises in their own right. While COBIT ensures that IT is working as effectively as possible to maximize the benefits of technology investment, Val IT helps enterprises make better decisions about where to invest, ensuring that the investment is consistent with the business strategy. And while COBIT provides a set of controls to mitigate IT risk in IT processes, Risk IT provides a framework for enterprise to identify, govern and manage IT-related risks.

COBIT and ISO/IEC 27002:2007: COBIT was released and used primarily by the IT community, and has become the internationally accepted framework for IT governance and control. ISO/IEC 27002:2007 (The Code of Practice for Information Security Management) is also an international standard and is best practice for implementing security management. The two standards do not compete with each other and actually complement one another. COBIT typically covers a broader area while ISO/IEC 27002 is deeply focused in the area of security.

The table below describes the inter-relation of the two standards as well as how ISO/IEC 27002 can be integrated with COBIT.

COBIT DOMAIN 1 2 3 4 5 6 7 8 9 10 11 12 13

Plan and Organize - + - - + + + - - 0 ..

Acquire and Implement + 0 0 - 0 +

Deliver and Support - + 0 + + . + 0 0 0 + 0 0

Monitor and Evaluate - 0 - 0

(+) Good match (more than two ISO/IEC 27002:2007 objectives were mapped to a COBIT process)

(0) Partly match (one or two ISO/IEC 27002:2007 objectives were mapped to a COBIT process)

(-) No or minor match (no ISO/IEC 27002:2007 objective was mapped to a COBIT process)

(.) Does not exist

COBIT and Sarbanes Oxley : Public companies that are subject to the U.S. Sarbanes-Oxley Act of 2002 are encouraged to adopt COBIT and/or the Committee of Sponsoring Organizations of the Treadway Commission (COSO) "Internal Control – Integrated Framework." In choosing which of the control frameworks to implement in order to comply with Sarbanes-Oxley, the U.S. Securities and Exchange Commission suggests that companies follow the COSO framework.

COSO Internal Control - Integrated Framework states that internal control is a process — established by an entity's board of directors, management, and other personnel — designed to provide reasonable assurance regarding the achievement of stated objectives. COBIT approaches IT control by looking at information — not just financial information — that is needed to support business requirements and the associated IT resources and processes.

COSO control objectives focus on effectiveness, efficiency of operations, reliable financial reporting, and compliance with laws and regulations. The two frameworks have different audiences. COSO is useful for management at large, while COBIT is useful for IT management, users, and auditors. COBIT is specifically focused on IT controls. Because of these differences, auditors should not expect a one-to-one relationship between the five COSO control components and the four COBIT objective domains.

AAS 29: requires the auditor to consider the effect of a CIS environment on his audit and discuss the risk and caution that an auditor should exercise while carrying out traditional audit objectives in a computer information system environment and elaborates on the following: • The auditor’s responsibility in gaining sufficient understanding and assurance on the adequacy of accounting and internal controls. • The potential impact of auditing in a CIS on the assessment of control and audit risks. • The auditor is required to determine the following factors to determine the effect of CIS environment on the audit arising from. • The extent to which the CIS is used for recording, compiling and analysing accounting information. • The system of internal controls relating to the authorised, complete, accurate and valid processing & reporting procedures. • The impact of CIS accounting system on the audit trail.	BS 7799: is an International Standard (British Standard) setting out the requirements for an Information Security Management System. • It helps identify, manage and minimize the range of threats to which information is regularly subjected. • The “Security Code of Conduct” was a originator from which grew BS 7799, which has, in turn, subsequently grown into ISO 17799. • BS 7799 was originally just a single standard, and had the status of a Code of Practice. In other words, it provided guidance for organisations, but hadn’t been written as specification that could form the basis of an external third party verification and certification scheme. Objectives: (CIA) BS 7799 focused on protecting the Confidentiality, Integrity and Availability of organisational information.	BENEFIS OF USING BS 7799 • Reduced operational risk • Increased business efficiency • Assurance that information security is being rationally applied This is achieved by ensuring that: • Security controls are justified. • Policies and procedures are appropriate. • Security awareness is god amongst staff and managers. • All security relevant information processing and supporting activities are auditable and are being audited. • Internal audit, incident reporting/management mechanisms are being treated appropriately. • Management actively focus on information security and its effectiveness. COMPONENTS OF BS 7799: • BS 7799 (ISO 17799) Part 1 – Code of Practice on Information Security Management • BS 7799 Part 2 – Specification for Information Security Management Systems
---	---	---

ISO 27001 – (BS 7799: PART II) – INFORMATION SECURITY MANAGEMENT STANDARD (ISMS): To address assets to be protected, organisation approach to risk management, control objectives and control, and degree of assurance required. • Establishing Management Framework • Implementation • Documentation	AREAS OF FOCUS OF ISMS: (<u>SOAP's</u> Physics & <u>C</u>hemistry <u>A</u>llows Scientists to <u>B</u>uild <u>C</u>inthal) • <u>S</u>ecurity Policy • <u>O</u>rganisational Security • <u>A</u>sset Classification and Control • <u>P</u>ersonnel Security • <u>P</u>hysical and Environmental Security • <u>C</u>ommunications and Operations Management • <u>A</u>ccess Control • <u>S</u>ystems Development and Maintenance • <u>B</u>usiness Continuity Management • <u>C</u>ompliance	CMM – CAPABILITY MATURITY MODEL: The CMM presents sets of recommended practices in a number of key process areas that have been shown to enhance software process capability. The CMM was designed to guide software organisations in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement.
THE FIVE LEVELS OF SOFTWARE PROCESS MATURITY: (<u>I</u> Remember <u>D</u>esigning <u>M</u>y <u>O</u>ffice) • Level 1 – The <u>I</u>nitial Level • Level 2 – The <u>R</u>epeatable Level • Level 3 – The <u>D</u>efined Level • Level 4 – The <u>M</u>anaged Level • Level 5 - The <u>O</u>ptimizing Level	CONTROL OBJECTIVES FOR INFORMATION RELATED TECHNOLOGY (COBIT): The ISACF developed COBIT. COBIT is a trademark of generally applicable information systems security and control practices for IT controls. COBIT, which consolidates standards from 36 different sources into a single framework, is having a big impact on the information systems profession.	<u>The COBIT framework allows:</u> • Management to benchmark the security and control, practices of IT environments. • Users of IT services to be assured that adequate security and control exist • Auditors to substantiate their opinions on internal control and to advice on IT security and control matters.

<u>The COBIT framework addresses the issue of control from three vantage points or dimensions:</u> • Business Objectives • IT resources • IT processes	COBIT – IT GOVERNANCE MODEL: • Quality requirements • Fiduciary requirements • Security requirements	BUSINESS OBJECTIVES/COBIT'S WORKING DEFINITIONS: (<u>CIA</u> & <u>Cops Eat Eggs Regularly</u>) • <u>C</u>onfidentiality • <u>I</u>ntegrity • <u>A</u>vailability • <u>C</u>ompliance • <u>E</u>ffectiveness • <u>E</u>fficiency • <u>R</u>eliability of Information
IT RESOURCES: (<u>DID Tendulkar Pay A Fine</u>) • <u>D</u>ata • <u>T</u>echnology • <u>P</u>eople • <u>A</u>pplication systems • <u>F</u>acilities	IT PROCESSES/THE COBIT FRAMEWORK/DOMAIN OF COBIT: (<u>My Dad Is Powerful</u>) • <u>M</u>onitoring • <u>D</u>elivery and Support • <u>A</u>cquisition and Implementation • <u>P</u>lanning and Organisation	COBIT AND OTHER STANDARDS: • COBIT and ISO 17799 (BS 7799) • COBIT and Sarbanes Oxley • COSO and COBIT
COCO: The “Guidance on Control” report, known colloquially as CoCo, was produced by The Canadian Institute of Chartered Accountants. CoCo does not cover any aspect of information assurance per se. It is concerned with control in general. CoCo can be said to be a concise superset of COSO.	It use the same three categories of objectives: (<u>Cops Eat Eggs Regularly</u>) • <u>C</u>ompliance with applicable laws and regulations • <u>E</u>ffectiveness of operations • <u>E</u>fficiency of operations • <u>R</u>eliability of financial reporting	Concepts about “control”: • Control is affected by people throughout the organisation • People who are accountable for achieving objectives should also be accountable for the effectiveness of control • Organisations are constantly interacting and adapting • Control can be expected to provide only reasonable assurance, not absolute assurance

ITIL (IT INFRASTRUCTURE LIBRARY): The IT Infrastructure Library (ITIL) is so named as it originated as a collection of books (standards) each covering a specific 'practice' within IT management.	<u>The eight ITIL books and their disciplines are:</u> The IT Service Management sets relating to: 1. Service Delivery 2. Service Support Other operational guidance relating to: 3. ICT Infrastructure Management 4. Security Management 5. The Business Perspective 6. Application Management 7. Software Asset Management 8. Planning to Implement Service Management	
SYSTRUST AND WEBTRUST: • SysTrust engagements are designed for the provision or advisory services or assurance on the reliability of a system • WebTrust engagements relate to assurance or advisory services on an organisation's system related to e-commerce	<u>Principles and Criteria:</u> (SAP CO.) • <u>S</u>ecurity • <u>A</u>vailability • <u>P</u>rocessing integrity • <u>C</u>onfidentiality • <u>O</u>nline privacy	<u>Broad Areas:</u> (Policies Communicates Procedures and also Monitors it) • <u>P</u>olicies • <u>C</u>ommunications • <u>P</u>rocedures • <u>M</u>onitoring
HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) were enacted by the U.S. Congress for: • Protection of health insurance coverage for workers and their families when they change or lose their jobs • Administrative Simplification provisions	SAS 70 – STATEMENT OF AUDITING STANDARDS FOR SERVICE ORGANISATIONS: A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organisation has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes.	SERVICE AUDITOR'S REPORTS: • Type I report • Type II report
