INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

CONTENTS

- IS Audit Standards
- BS 7799 (British Standard)
- ISMS (Information Security Management Standard)
- CMM (Capability Maturity Model)
- COBIT (Control Objective for Information and Related Technology)
- COCO (Guidance on Control)
- SysTrust and WebTrust
- HIPAA (Health Insurance Portability and Accountability Act)
- Service Auditor’s report

IS audit Standards

Year	Standards
1994	CoCo
1996	HIPAA
1998	BS7799
2000	COBIT

BS 7799

- BS7799 is an **International Standard** setting out the requirements for an Information Security Management System.
- It helps **to identify, manage and minimize** the range of threats to which information is regularly subjected
- Specifications for "**Information Security Management Systems**", constitutes what is known as BS 7799 from the **British Standards** Institute
- BS7799 focused on **protecting the *availability, confidentiality* and *integrity*** of organizational information and this remains, today, the driving objective of the standard

Benefits of BS 7799

Using it well will result in:

- Reduced operational risk
- Increased business efficiency
- Assurance that information security is being logically applied

ISMS

Issues to consider before implementing ISMS

- General
  - Addressing Asset to be protected
  - Organisation approach to Risk Management
  - Control objective
  - Degree of Assurance
- Establishing management framework
  - Proper risk assessment;
  - Areas of risk to be managed and degree of assurance required;
  - Information security policy;
  - Reasonable level controls;

ISMS

Issues to consider before implementing ISMS

- Implementation
  - Effectiveness of controls implementation procedures should be verified while reviewing security policy and technical compliance.
- Documentation
  - Management controls.
  - ISMS management procedure
- ***Document Control – Issues to be focused under this clause;***
  - Read availability
  - Periodic review
  - Maintain version control
  - Withdrawal when obsolete
  - Preservation for legal purpose

CMM

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 change towards a culture of software engineering and management excellence

Five levels of CMM

LEVEL 1: Initial level

- Organizations at this level frequently develop products that work, even though they may be over the budget and schedule
- Success in level 1 organizations depends on the competence and heroics of the people in the organization
- at level 1, capability is a characteristic of the individuals, not of the organization

Five levels of CMM

LEVEL 2: Repeatable level

- At the this 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 previous projects
- disciplined because planning and tracking of the software project is stable and earlier successes can be repeated

Five levels of CMM

LEVEL 3: Defined level

- At this level, the standard process for developing and maintaining software across the organization is documented, including both software engineering and management processes
- used to help the software managers and technical staff to perform more effectively
- Project's team tailors the organization's standards software process to develop their own defined software process

Five levels of CMM

LEVEL 3: Defined level

- At this level, the standard process for developing and maintaining software across the organization is documented, including both software engineering and management processes
- used to help the software managers and technical staff to perform more effectively
- Project's team tailors the organization's standards software process to develop their own defined software process

Five levels of CMM

LEVEL 3: Defined level

- This tailored process is referred to in the CMMas the project’s defined software process
- A defined software process contains a logically integrated set of well-defined software engineering and management processes

Five levels of CMM

LEVEL 4: Managed Level

- At this level, the organization sets quantitative quality goals for both software products and process
- Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program
- Software products are of predictably high quality

Five levels of CMM

LEVEL 5: Optimizing level

- At this level organizations can be characterized as continuously improving
- Organizations are continuously motivated 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

COBIT-IT Governance Model

The fundamental concept of the COBIT Framework is that control in IT is approached by looking at information that is needed to support the business objectives or requirements, and by looking at information as being as result of the combined application of IT-related resources that need to be managed by IT processes

COBIT-IT Governance Model

To satisfy business objectives, information needs to conform to certain criteria, which COBIT refers to as business requirements for information. The list of requirements established includes

- Quality requirements
- Fiduciary requirements
- Security requirements

IT resources

- Data
- Application system
- Technology
- Facilities
- People

CoCo

- The “Guidance on Control” report, generally known as CoCo, was produced in 1999 by the Criteria of Control Board of The Canadian Institute of chartered Accountants
- CoCo does not cover any aspect of information assurance
- It is concerned with control in general
- It is about “designing, assessing and reporting on the control systems of organizations”

CoCo

Four important concepts about "control" are

- Control is affected by people throughout the organization, including the board of directors (or its equivalent), management and all other staff.
- 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.
- Organizations are constantly interacting and adapting.
- Control can be expected to provide only reasonable assurance, not absolute assurance

SYSTRUST AND WEBTRUST

Sys Trust

- Sys Trust engagements are designed for the provision or advisory services or assurance on the reliability of a system

Web Trust

- Web Trust engagements relate to assurance or advisory services on an organization’s system related to e-commerce

SYSTRUST AND WEBTRUST

Principles

- Security-Against unauthorized access
- Availability-Available for Operation & use as committed as agree
- Processing integrity-System processing is complete, accurate, timely and authorized
- Online privacy-Personal Information obtained is collected, used, disclosed and retained as committed or agreed
- Confidentiality-Information is protected

HIPAA

- Title 1 of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs
- Title 2 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 Security Rule

- Administrative safeguards-Privacy Policy and Procedures, Review, Contingency Plan, Internal Audit
- Physical safeguards-Removal of Hardware and Software should be control, Access to hardware and Software, Visitors Escort, Control over Agent
- Technical safeguards-Controlling Access to computer systems, networks etc.

SAS 70

- 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)
- SAS No. 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customer's auditors in a uniform reporting format

SAS 70

- A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm
- 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

- 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
- SAS 70 is not a pre-determined set of control objectives or control activities that service organizations must achieve
- 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 Auditor’s Report

One of the most effective ways a service organization can communicate information about its control is through a Service Auditor’s Report.

There are two types of Service Auditor’s Reports: Type I and Type II

Service Auditor’s Report

- A Type I report describes the service organization’s description of controls at a specific point in time
- 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

Service Auditor’s Report

In a type I report, the service auditor will express an opinion on

(1) whether the service organization’s description of its controls presents fairly, in all material respects, the relevant aspects of the service organization’s controls that had been placed in operation as of a specific date, and

(2) whether the controls were suitably designed to achieve specified control objectives

Service Auditor’s Report

In a type II report, the service auditor will express an opinion on the same items noted above in a Type I report, and

(3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified

Benefits to the service organization

- Service organizations receive significant value from having a SAS 70 engagement performed
- 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