BSc in Computer Engineering
CMP4103
Computer Systems and Network Security

Lecture 1

Information Security Management, Governance and Risk Management

Eng Diarmuid O'Briain, CEng, CISSP

Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University

Table of Contents

1. Management Frameworks

A management system is the framework of processes and procedures used to ensure that an organisation can fulfil all tasks required to achieve its objectives.

1.1 ISO/IEC 27001 Information Security Management System

The ISO/IEC 27000-series (also abbreviated to the 'Information Security Management System (ISMS) Family of Standards' or 'ISO27k') comprises information security standards published jointly by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC).

The series provides best practice recommendations on information security management, risks and controls within the context of an overall ISMS.

This series consists of 6 main standards and in excess of 40 documents overall offering standards and guidelines for the implementation, maintenance and auditing of ISMS.

• ISO/IEC 27001	Information Security Management System (ISMS) Requirements
• ISO/IEC 27002	Code of practice for Information Security
• ISO/IEC 27003	Information Security Management – System implementation guidance
• ISO/IEC 27004	Information Security Management – Measurement
• ISO/IEC 27005	Information Security Management – Risk management
• ISO/IEC 27006	Guidelines for Information Security Management – Systems auditing

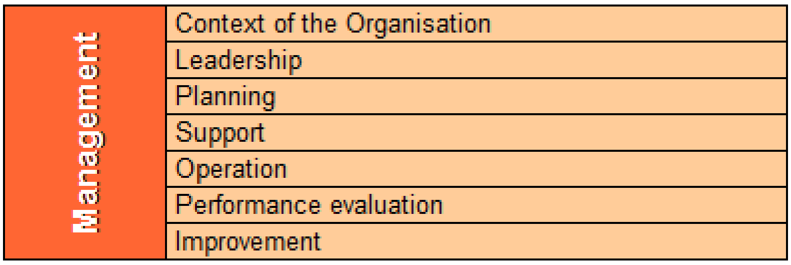
1.2 ISO/IEC 27001 IT Security techniques ISMS requirements

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS) that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organisations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard.

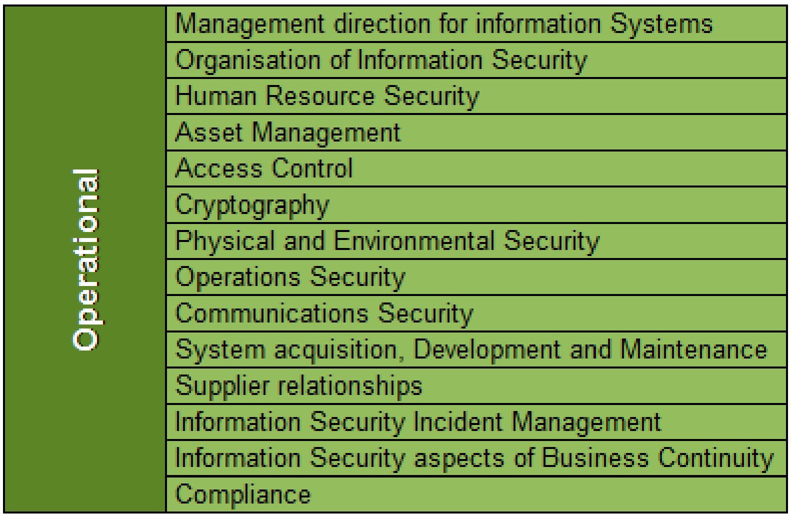
ISO/IEC 27001 requires that management:

- Systematically examines the organisation's information security risks, taking account of the threats, vulnerabilities and impacts
- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable
- Adopts an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

1.2.1 Controls points both Management and Operational



Management	Context of the Organisation
	Leadership
	Planning
	Support
	Operation
	Performance evaluation
	Improvement



Operational	Management direction for information Systems
	Organisation of Information Security
	Human Resource Security
	Asset Management
	Access Control
	Cryptography
	Physical and Environmental Security
	Operations Security
	Communications Security
	System acquisition, Development and Maintenance
	Supplier relationships
	Information Security Incident Management
	Information Security aspects of Business Continuity
	Compliance

1.2.2 Implementation stages for ISMS

Six process for implanting an ISMS as defined within ISO/IEC 27001:

1. Define Information Security Policy
2. Define scope of ISMS
3. Perform risk assessment
4. Manage risks
5. Select controls
6. Prepare statement of applicability

http://www.iso.org

http://www.iec.ch

http://www.27000.org

1.3 IT Infrastructure Library (ITIL)

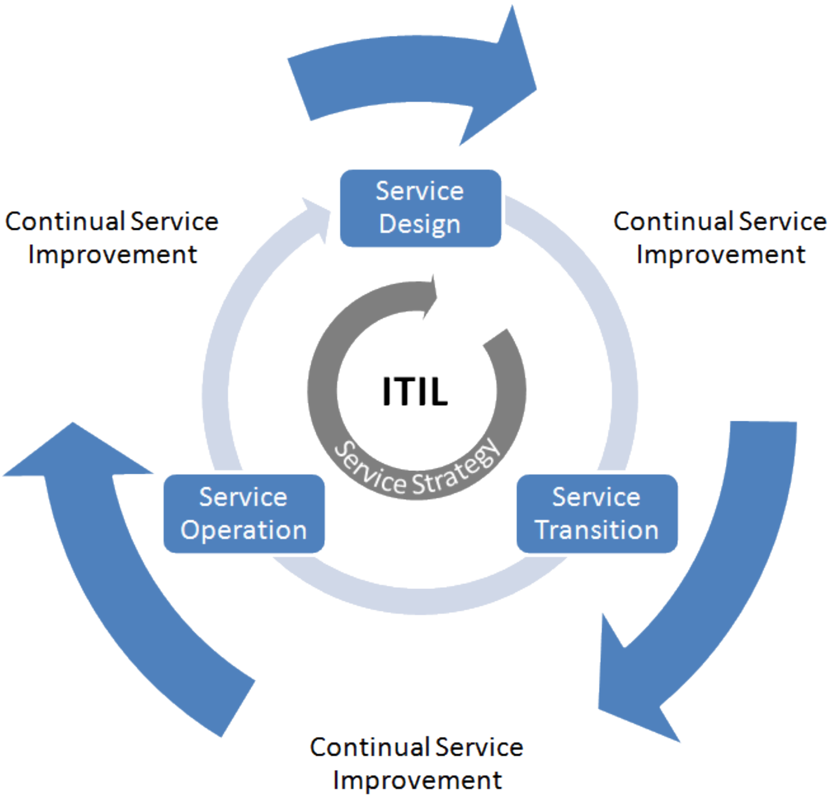
The ITIL is a set of concepts and practices for managing IT services, IT development and IT operations.

ITIL gives detailed descriptions of a number of important IT practices and provides comprehensive check lists, tasks and procedures that any IT organisation can tailor to its needs. ITIL is published in a series of books, each of which covers an IT management topic. The names ITIL and IT Infrastructure Library are registered trademarks of the United Kingdom's Office of Government Commerce (OGC).

Five volumes comprise the ITIL v3, published in May 2007:

1 Service Strategy
2 Service Design
3 Service Transition
4 Service Operation
5 Continual Service Improvement

ITIL The IT Infrastructure Library

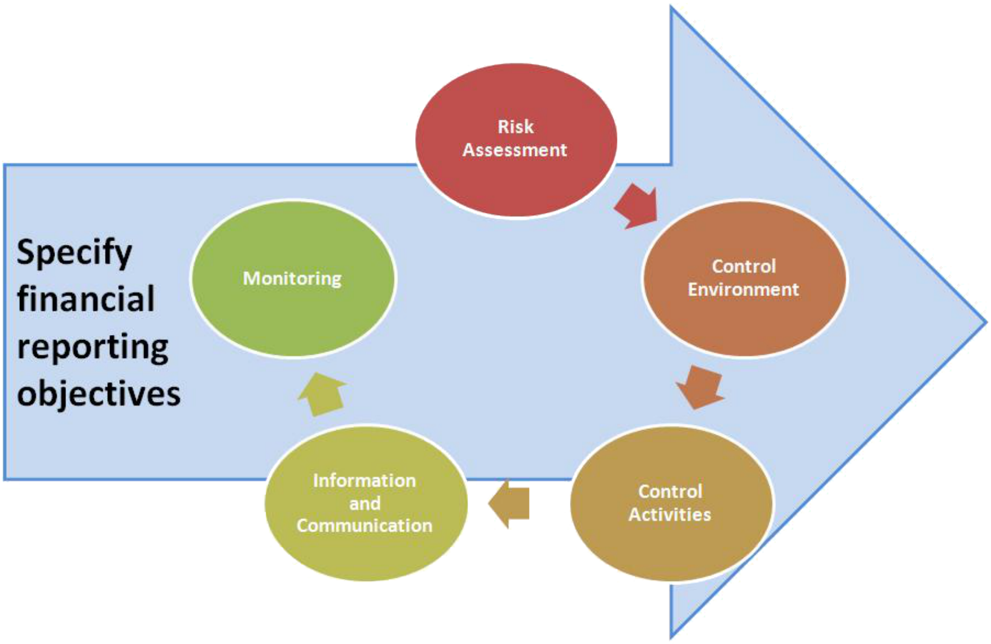

Service Design
Continual Service Improvement
Continual Service Improvement
ITIL
Service Strategy
Service Operation
Service Transition
Continual Service Improvement

http://www.itgovernance.co.uk/ITILLibrary

1.4 Committee of Sponsoring Organisations (COSO)

Committee of Sponsoring Organisations of the Treadway Commission (COSO) is a voluntary private-sector organisation, established in the United States, dedicated to providing guidance to executive management and governance entities on critical aspects of organisational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting. COSO has established a common internal control model against which companies and organisations may assess their control systems.

The COSO "***Enterprise Risk Management Integrated Framework***" defines Enterprise Risk Management (ERM) as a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.


Specify financial reporting objectives
Risk Assessment
Control Environment
Control Activities
Information and Communication
Monitoring

The COSO ERM Framework has four objectives and eight components.

The four objectives categories are:

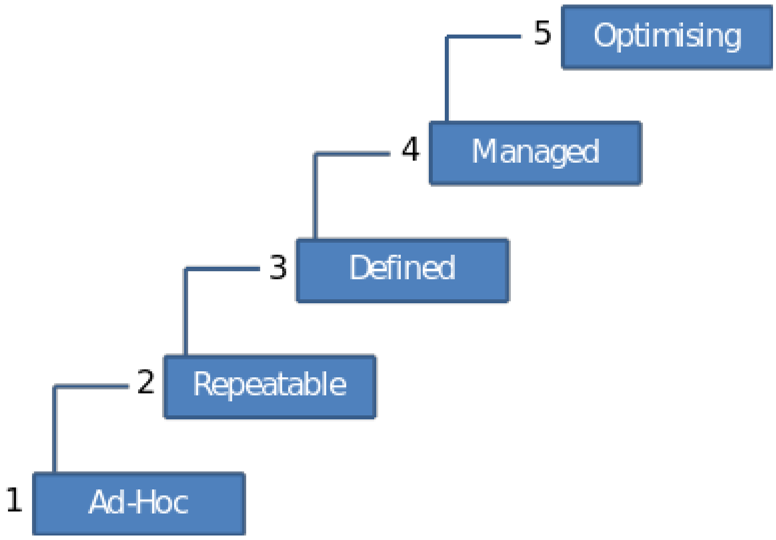
1. ***Strategy*** - high-level goals, aligned with and supporting the organisation's mission
2. ***Operations*** - effective and efficient use of resources
3. ***Financial Reporting*** - reliability of operational and financial reporting
4. ***Compliance*** - compliance with applicable laws and regulations

The eight components are:

1. Internal Environment
2. Objective Setting
3. Event Identification
4. Risk Assessment
5. Risk Response
6. Control Activities
7. Information and Communication
8. Monitoring

http://www.coso.org

1.5 Capability Maturity Model



The Capability Maturity Model (CMM) is a service mark and a model for understanding the capability maturity of an organisation's software development business processes. Because the CMM is about process maturity, it differs from more common maturity models that provide a structured collection of elements that describe certain aspects of maturity in an organisation. The CMM is useful as a general theoretical model, to aid in the definition and understanding of an organisation's process capability maturity.

Level 1 – Initial / Ad-Hoc

- It is characteristic of processes at this level that they are (typically) undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events. This provides a chaotic or unstable environment for the processes.

Level 2 - Repeatable

- It is characteristic of processes at this level that some processes are repeatable, possibly with consistent results.
  - Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.

Level 3 - Defined

- It is characteristic of processes at this level that there are sets of defined and documented standard processes established and subject to some degree of improvement over time. These standard processes are in place and are used to establish consistency of process performance across the organisation.

Level 4 - Managed

- It is characteristic of processes at this level that, using process metrics, management can effectively control the process. In particular, management can identify ways to adjust and adapt the process without measurable loss of quality or deviations from specifications. Process Capability is established from this level

Level 5 - Optimised

- It is characteristic of processes at this level that the focus is on continually improving process performance through both incremental and innovative technological changes/improvements

For software development, the CMM has been superseded by Capability Maturity Model Integration (CMMI). The CMMI is a proven methodology for Performance Management managed by the Software Engineering Institute (SEI). It comes in three models.

CMMI for Acquisition

- Designed for businesses that focus on working with suppliers to assemble a product or deliver a service.
- This model delves into creating effective solicitations and supplier agreements, effectively gathering and communicating requirements to suppliers, monitoring supplier activities and artefacts, and ensuring the results of supplier work meet the needs of end users.

CMMI for Development

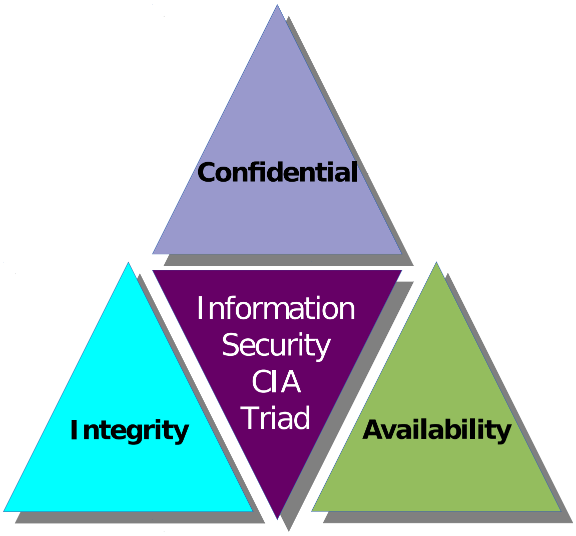
- Designed for businesses that focus on developing products and services.
- This model delves into detail about converting customer requirements into requirements used by developers, effectively integrating product components into the final product or service, performing the technical analysis and development work to design the product or service, and ensuring that development work meets the needs of the end users and the specifications formulated during design.

CMMI for Services

- Designed for businesses that focus on working with suppliers to assemble a product or deliver a service.
- This model delves into creating effective solicitations and supplier agreements, effectively gathering and communicating requirements to suppliers, monitoring supplier activities and artefacts, and ensuring the results of supplier work meet the needs of end users.

http://cmmiinstitute.com

2. Security Management Concepts and Principles



2.1 Confidentiality, Integrity and Availability (CIA) Triad Principles

For over twenty years, information security has held confidentiality, integrity and availability (known as the CIA triad) as the core principles of information security. Many information security professionals firmly believe that Accountability should also be added as a core principle of information security.

2.1.1 Confidentiality

Confidentiality is the term used to prevent the disclosure of information to unauthorised individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorised party obtains the card number in any way, a breach of confidentiality has occurred.

Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorised to have the information.

Confidentiality is necessary (but not sufficient) for maintaining the privacy of the people whose personal information a system holds.

2.1.2 Integrity

In information security, integrity means that data cannot be modified without authorisation. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorised user vandalises a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mis-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.

2.1.3 Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks.

2.2 Other Security Concepts

In addition to the CIA Triad the following list of security concepts need to be considered.

- Privacy
    - Prevention of unauthorised access
    - Freedom from being observed or monitored without consent
- Identification
    - Subjects present their Identification before access is permitted
- Authentication
    - Subjects claimed Identification is valid
- Authorisation
    - Subjects claimed Identification is valid and they are permitted access to a specific object
- Auditing
    - Subjects held accountable for their actions
- Accountability
    - Subjects held accountable for their actions
- Non-repudiation
    - Subject cannot deny the event occurred

3. Protection Mechanisms

3.1 Defence in Depth

The idea behind the Defence in Depth approach is to defend a system against any particular attack using several, varying methods. It is a layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security.

Defence in depth is originally a military strategy that seeks to delay, rather than prevent, the advance of an attacker by yielding space in order to buy time. The placement of protection mechanisms, procedures and policies is intended to increase the dependability of an IT system where multiple layers of defence prevent espionage and direct attacks against critical systems. In terms of computer network defence, Defence in Depth measures should not only prevent security breaches, but buys time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

3.2 Abstraction

This is a mechanism to create efficient management of security tools. Similar elements are grouped for ease of security management. Abstraction defines what kinds of data are in objects, what functions can be performed on objects and/or what capabilities an object is allowed to have. Security controls are assigned to groups of objects that have similar security requirements by role or function.

3.3 Data Hiding

Data Hiding is the prevention of data being discovered or accessed by a subject without rights to access that data.

3.4 Encryption

Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (called ciphertext).

4. Change Management

Change control is a formal process used to ensure that changes to a product or system are introduced in a controlled and coordinated manner. Change in secure environments can create loopholes, overlaps, missing objects leading to new vulnerabilities. Change control reduces the possibility that unnecessary changes will be introduced to a system without forethought, introducing security faults into the system or undoing changes already made.

4.1 Change Control Process

4.1.1 Record/classify

The client initiates change by making a formal request for something to be changed. The change control team then records and categorises that request. This categorisation would include estimates of importance, impact, and complexity.

4.1.2 Assess

The impact assessor or assessors then make their risk analysis typically by answering a set of questions concerning risk, both to the business and to the process, and follow this by making a judgement on who should carry out the change. If the change requires more than one type of assessment, the head of the change control team will consolidate these. Everyone with a stake in the change then must meet to determine whether there is a business or technical justification for the change. The change is then sent to the delivery team for planning.

4.1.3 Plan

Management will assign the change to a specific delivery team, usually one with the specific role of carrying out this particular type of change. The team's first job is to plan the change in detail as well as construct a regression plan in case the change needs to be backed out.

4.1.4 Build/test

If all stakeholders agree with the plan, the delivery team will build the solution, which will then be tested. They will then seek approval and request a time and date to carry out the implementation phase.

4.1.5 Implement

All stakeholders must agree to a time, date and cost of implementation. Following implementation, it is usual to carry out a post-implementation review which would take place at another stakeholder meeting.

4.1.6 Close/gain acceptance

When the client agrees that the change was implemented correctly, the change can be closed.

5. Data Classification

Data Classification is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled / secured and is also indicative of its value in terms of Business Assets.

The classification of data and documents is essential if you are to differentiate between that which has a little value, and that which is highly sensitive and confidential. When data is stored, whether received, created or amended, it should always be classified into an appropriate sensitivity level. The military tend to use a simple scale follows:

5.1 Military Data Classification Scale

5.1.1 Top Secret

The highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to national security if publicly available.

5.1.2 Secret

Such material would cause "grave damage" to national security if it were publicly available.

5.1.3 Confidential

Such material would cause "damage" or be "prejudicial" to national security if publicly available.

5.1.4 Restricted

Such material would cause "undesirable effects" if publicly available. Some countries (like the US) do not have such a classification.

5.1.4.1 Sensitive But Unclassified (SBU)

SBU is a designation of information in the United States that, though unclassified, often requires strict controls over its distribution. Similar to restricted in other countries though the US treats documents received marked Restricted from other countries as Confidential.

5.1.5 Unclassified

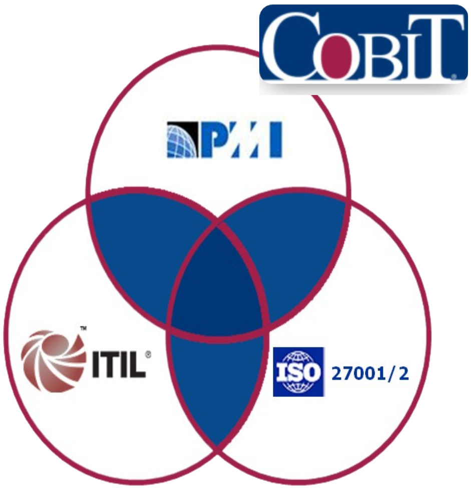
Technically not a classification level, but is used for government documents that do not have a classification listed above. Such documents can sometimes be viewed by those without security clearance.

5.2 Commercial Data Classification Scale

There is no set scale though companies usually implement something like this:

- Confidential
- Private
- Sensitive
- Public

5.3 Control Objectives for Information and related Technology (CobiT)



CobiT is a framework for 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 maximising the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

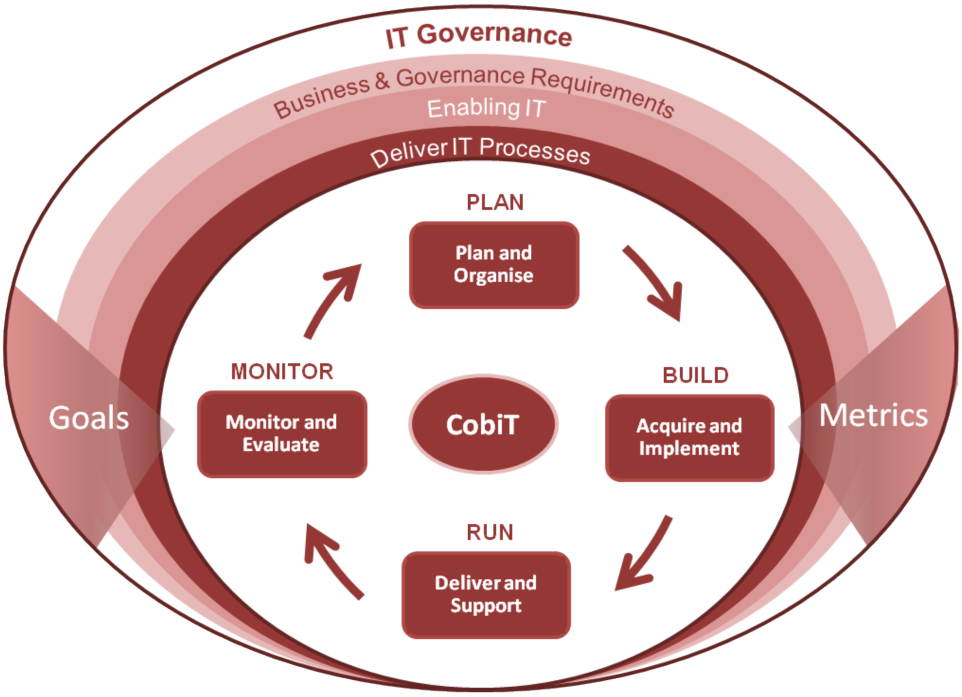
CobiT combines other frameworks like Project Management Institute (PMI), ISO 27000 and ITIL to build IT Governance that provides

- Value Delivery
- Risk Management
- Resource Management
- Performance Measurement
- Strategic Alignment

CobiT has high level processes that cover hundreds of control objectives categorised into four domains:

- Planning and Organisation
- Acquisition and Implementation
- Delivery and Support
- Monitoring and Evaluation

CobiT provides benefits to managers, IT users, and auditors. Managers benefit from CobiT because 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. IT users benefit from CobiT because of the assurance provided to them by CobiT's defined controls, security, and process governance. CobiT benefits auditors because it helps them identify IT control issues within a company's IT infrastructure. It also helps them corroborate their audit findings.



6. Employment Policies and Practices

6.1 Hiring of new staff

- Creating a Job Description
- Setting a classification for the job
- Screening candidates
- Hiring and Training the selected candidate

The objective of a job description is to have a clear outline of duties and responsibilities to make the screening process as direct and focused as possible. The creation of a job description is an essential building block to addressing security concerns. From the job description it should be determinable what level of access to sensitive material or classified information is needed. With this known it is a standard enough affair to assign the new staff member a security classification. The Job Description should contain the following elements.

- Separation of Duties (SoD)
  - SoD is the concept of having more than one person required to complete a task. It is alternatively called segregation of duties or, in the political realm, separation of powers
- Job Responsibilities
- Job Rotation
  - Job rotation is an approach to management development where an individual is moved through a schedule of assignments designed to give a breadth of exposure to the entire operation.
- Knowledge Redundancy
  - Reduces the risk of fraud, data modification, theft, sabotage and misuse of information.

6.2 Screening and Background Checks

Background checking is the process of authenticating the information supplied to a potential employer by a job applicant in his or her resume, application, and interviews. In most application processes, lying about background and credentials will keep the employer from hiring the applicant. Background checking ensures the employer that the candidate has the background and experience claimed.

Additionally, if it is determined at a later date through a background check, that an employee lied about credentials, qualifications, experience, education and so forth, the employer may fire the employee. This assumes that the employee signed a statement attesting to the truth of his or her provided information.

Common background checks include:

- ***Verification of academic credentials***
  - Verification of prior employment including position, longevity, salary, and job performance, sometimes tracing back ten years or to the three prior positions
- Discussions with business, professional, and ***personal references*** and verification of ***letters of recommendation***
- ***Drug screens and physical medical exams***
- ***Testing*** to confirm skills and knowledge
- ***Internet Search***
  - An Internet search, on the candidate's name, especially at google.com to confirm an individual's claims about their jobs, performance, awards, and more
- ***Criminal background checks***
- ***Credit Checks***
  - Especially for accounting and finance professionals

Background checking is usually conducted by Human Resources professionals, but occasionally, the supervisor of the position being filled assists, especially with reference background checking.

Additionally, background checking of people who are candidates for the same job should be the same. A clear connection should exist between the background checks conducted and the requirements of the job.

6.3 Employee Agreements

You may want some high-level employees to sign a formal Employment Agreement indeed some employees may even ask for one. A well-drafted Employment Agreement addresses the following key issues:

- The job position
- Whether the position can be changed by the employer
- The length of the agreement
- The salary, bonus and benefits
- Whether the employee gets stock or stock options in the company
- When the employee can be terminated for good cause
- What "*good cause*" means in terms of the role
    - An employee is said to be discharged for good cause if the reasons for the termination are work related. However, if the employer simply did not like the employee's personality, this would not ordinarily constitute good cause, unless the employee held a position, such as a salesperson, for which a likeable personality was required.
- When the employee can be terminated without good cause and what severance payment will be due
- The employee's job responsibilities
- The employee's confidentiality obligations
- Where and how disputes will be handled

6.3.1 Non-Disclosure Agreement (NDA)

An NDA is a contract signed by employees and/or third parties agreeing not to disclose proprietary company information to anyone outside the company. This prevents outside parties you're working with from revealing inside information about your company with anyone else, or employees from using confidential company information to benefit any person or entity other than your company.

A Non-compete Agreement or Clause, is a term used in contract law under which an employee agrees not to pursue a similar profession or trade in competition against the employer. The use of such agreements is premised on the possibility that upon their termination or resignation, an employee might begin working for a competitor or starting a business, and gain competitive advantage by abusing confidential information about their former employer's operations or trade secrets, or sensitive information such as customer/client lists, business practices, upcoming products, and marketing plans.

6.4 Employee Termination

Employee Termination is the end of an employee's duration with an employer. Depending on the case, the decision may be made by the employee, the employer, or mutually agreed upon by both.

It is essential to integrate IT into the process to help ensure that employee termination controls are comprehensive enough to meet relevant Employee Termination requirements (i.e. Sarbanes-Oxley).

Information security and data retention policies must be company-specific and tailored to the laws under which the company operates. Nevertheless, there are at least three broad IT principles to which a company should adhere when and after terminating an employee.

6.4.1 Prompt notification of termination

Every company should have a strictly enforced policy that clearly states who is to notify whom when someone's employment is ending or has ended. This policy should also mandate that these notifications be given immediately.

An information security contact should be among those who are notified, and this person's responsibilities should entail researching, documenting, and revoking an employee's access to the company's electronically stored proprietary information and its information systems.

6.4.2 Prudent revocation of access

In the case of a terminated employee, IT should immediately revoke all computer, network, and data access the former employee has. Remote access should also be removed, and the former employee should be dispossessed of all company-owned property, including technological resources like a laptop and intellectual property like corporate files containing customer, sales, and marketing information.

However, in the case of an employee whose end of employment is only imminent (working out notice for example), IT should consult with the employee's manager, HR, and other key decision-makers to determine the appropriate manner in which to stagger the revocation of access over the person's remaining days of employment.

Just as the granting of access and security clearances should be documented for future reference, the revocation of access should also be documented, especially for legal purposes. The goal, of course, should always be to revoke access in ways that make good business sense financially, technologically, and legally.

6.4.3 Pre-emptive Preservation of Data

Every company should have data redundancy and retention policies that satisfy its business needs and adhere to applicable laws. Such policies address the backup, restoration, and preservation of corporate data in general.

However, a company should also enact policies that detail when and how IT should go about preserving potentially and particularly sensitive data, records, logs and other materials that could be of legal significance were the company and former employee to wage a legal battle. It is especially important to do this in the case of a former employee who held a high-level position or left the company under a cloud of suspicion.

The appropriation and application of these three principles should be the collective work of the company's executive staff, IT and HR departments, and legal counsel that specialises in computer forensics and the laws governing the company's use of computing technology.

The results of this cooperative effort should be greater protection of corporate data as well as better preparedness for litigation regarding corporate data theft, hacking, and other forms of illegal or ill-advised uses of computing technology.

7. Security Roles

7.1 Senior Manager

The Senior Manager is the corporation's top executive with responsibility for security. This role gives sponsorship to the Security Professionals who execute it. He/she signs off on all security policies.

7.2 Security Professional

The Security Professional is a job that focuses on the execution of the security policies within an organisation. He/she typically develop the policies according to the instructions of the Senior Manager. Once sign-off on the policies are accepted and signed off then the Security Professional is responsible for their execution. Note: This role is NOT that of a decision maker but that of an implementer.

7.3 Data Owner

Entity that can authorise or deny access to certain data, and is responsible for its accuracy, integrity, and timeliness.

7.4 Data Custodian

The data custodian is the person responsible for, or the person with administrative control over, granting access to an organisation's documents or electronic files while protecting the data as defined by the organisation's security policy or its standard IT practices.

7.5 User

Any person who has access to the secured system. Access levels for the users should be mapped to their Job role. Users should be aware of and are responsible to the Security Policy.

7.6 Auditor

The Auditor has responsibility for testing and verifying that the Security Policy is properly implemented and is adequate to the task. The auditor produces compliance and effectiveness reports for review by the Senior Manager. The Senior Manager should take issues from the reports and drive change directives via the Security Professional.

8. Security Management Planning

This is the proper creation, implementation and enforcement of a security policy. Such planning is usually implemented in a top to bottom approach with the Senior Manager defining a Security Policy for the organisation with the assistance of the Security Professional. The Security Professional creates standards, guidelines and procedures to meet the requirements of the policy as the Security Management Documentation. Operational Managers, Line Managers, IT and Security departments must then implement the Security Management Documentation and End users must comply with the Policy and the Security Management Documentation guidelines and procedures.

NOTE: Security Management is the responsibility of Senior Management and NOT of the IT department.

8.1 Security Management Plans

8.1.1 Strategic Plan

Long term, horizon plan. It should include:

- Goals
- Missions
- Objectives
- Risk Assessment

8.1.2 Tactical Plan

Medium term plan on how the Goals and Objectives of the Strategic Plan should be achieved. These include:

- Project Plans
- Acquisition Plans
- Hiring Plans
- Maintenance Plans
- Support Plans
- System Development Plans

8.1.3 Operational Plan

Short term plans that are specific to actions being carried out to achieve Strategic and Tactical goals and objectives. The operational plans include:

- Resource planning
- Budgets
- Staff Assignment
- Implementation procedures

8.2 Security Documents

Information security policies are high-level statements or rules about protecting people or systems.

- A "standard" is a low-level prescription for the various ways the company will enforce the given policy.
- A "procedure" can describe a step-by-step method to implementing various standards.

8.3 Security Policies

The Security policy is a definition of what it means to be secure for a system, organisation or other entity. For an organisation, it addresses the constraints on behaviour of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

Because the security policy is a high level definition of secure behaviour, it is meaningless to claim an entity is "secure" without knowing what "secure" means. It is also foolish to make any significant effort to address security without tracing the effort to a security policy.

8.3.1 Information Security Policy

Information security policies are a special type of documented business rule for protecting information and the systems which store and process the information. Within an organisation, these written policy documents provide a high-level description of the various controls the organisation will use to protect information.

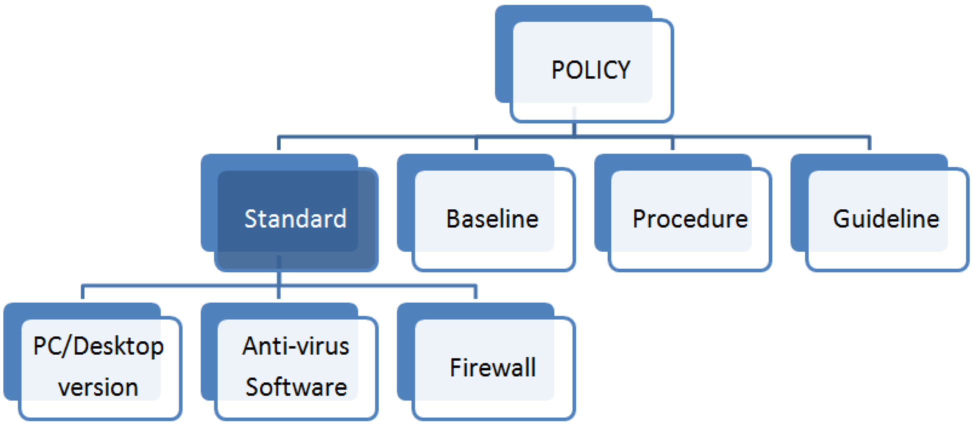
Written information security policy documents are also a formal declaration of management's intent to protect information, and are required for compliance with various security and privacy regulations. Organisations that require audits of their internal systems for compliance with various regulations will often use information security policies as the reference for the audit.

An information security policy document contains the written statements for how an organisation intends to protect information. Written information security policy documents are required for compliance with various security and privacy regulations such as the Sarbanes-Oxley Act.

An ideal information security policy document should contain the following elements:

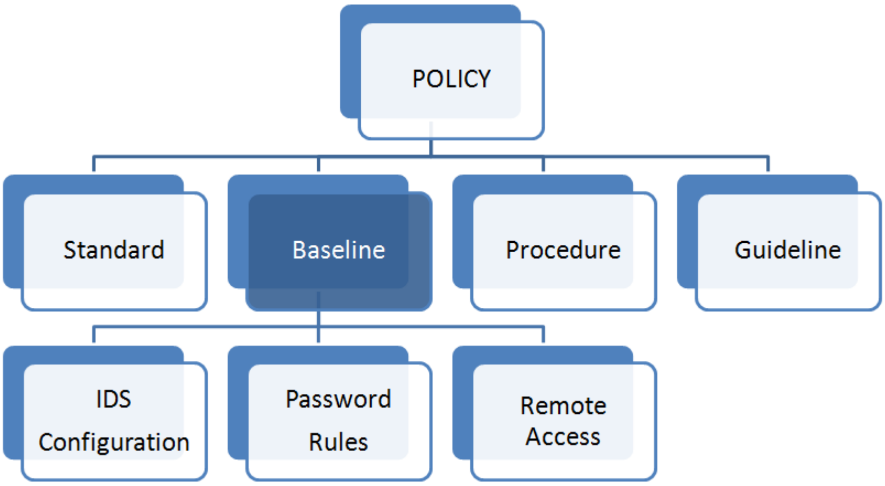
- **Title** - Brief description of the document
- **Number** - A number or unique identifier for the policy document
- **Author** - The author of the document
- **Publish Date** - The date the policy has been officially approved
- **Scope** - Describes the organisational scope that this policy applies to
- **Policy Text** - The written policies
- **Sanctions** - Provides information on violations of the written policy
- **Sponsor** - The executive sponsor of the policy document

8.4 Security Standards



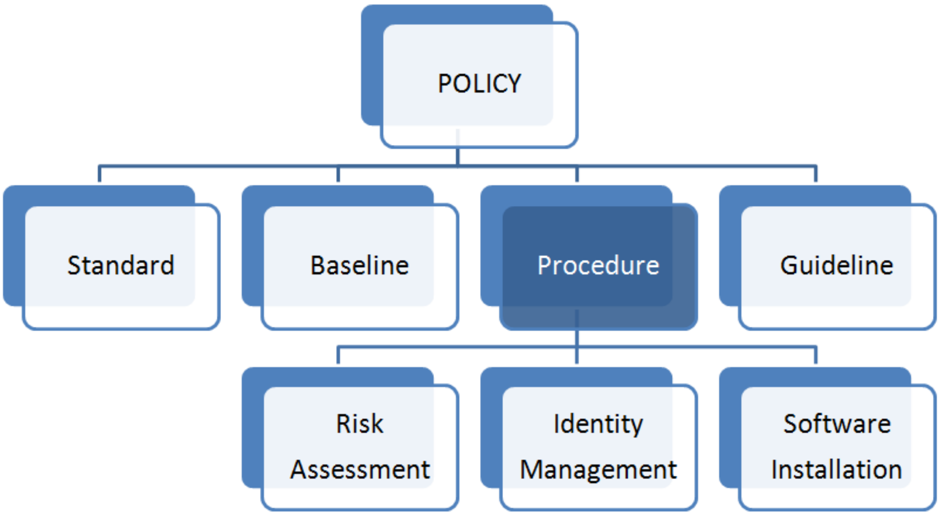
Security Standards define compulsory requirements for use of equipment and software plus security controls.

8.5 Security Baselines



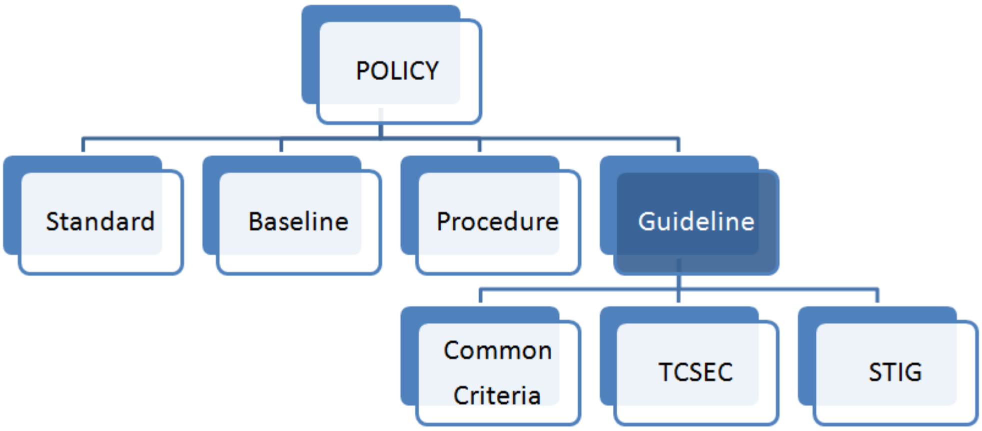
Security Baselines are the minimum level of security that all organisations systems must meet.

8.6 Security Procedures



Security Procedures are detailed step by step documents that describe the exact actions to implement a security mechanism, control or solution.

8.7 Security Guidelines



Security Guidelines define how both standards and baselines should be implemented. Guidelines also act as operational guides for employees who need them. We will look at the Common Criteria, Trusted Computer System Evaluation Criteria (TCSEC) and Security Technical Implementation Guides (STIG) in the Security Architecture chapter.

http://iase.disa.mil/stigs/index.html

9. Risk Management

Risk management is the identification, assessment, and prioritisation of risks followed by coordinated and economical application of resources to minimise, monitor, and control the probability and/or impact of unfortunate events.

It is necessary to identify associated IT security weaknesses, to evaluate and prioritise the associated risks, and to develop and implement an effective response strategy. This process, called risk assessment, forms the foundation for an effective information security programme.

9.1 What is Risk?

Risk is a function of the **likelihood** of a given **threat-source's** exercising a particular potential **vulnerability**, and the resulting **impact** of that adverse event on the organisation.

9.2 Risk Assessment Process

It is important to emphasise that risk assessment is a process as opposed to a once off event. Because technology and processes change, risk assessments need to be conducted periodically.

9.2.1 Phase 1: Preliminary Risk Assessment

In the first phase, it is necessary to perform a preliminary risk assessment and educate upper management about the risks so that they can make informed decisions about where to allocate the necessary resources.

9.2.2 Phase 2: Risk Analysis of Critical Areas and Processes

In the second phase a more in-depth set of risk assessments are performed on critical areas and processes identified in the preliminary risk assessment.

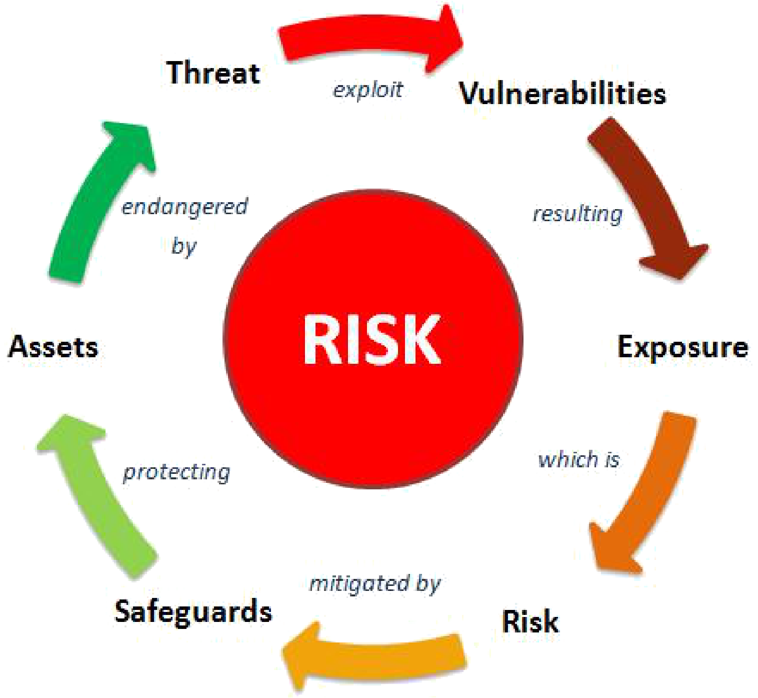
9.2.3 Phase 3: Organisation-Wide Risk Assessment

The goal of the third phase is to perform a thorough, wide risk assessment.

This phase focuses on IT issues relating to risk assessment with the understanding that this is only part of the process. Ultimately, risk assessment must take into account natural disasters, fire, and other events that can make a system unavailable.

Definition from National Institute of Standards and Technology (NIST) SP 800-30

9.3 Risk Terminology



9.3.1 Asset

Anything within the environment that should be protected.

9.3.2 Asset Valuation

Monitory value of an asset. This value should include not just the physical value of the item but costs associated with development, maintenance, repair and replacement for example.

9.3.3 Threats

Anything that may cause an undesirable outcome for the organisation of a specific asset. This includes any action or in-action that could cause damage, loss, disclosure of assets.

9.3.4 Vulnerability

Absence or weakness of safeguards that protect an organisation or asset.

9.3.5 Exposure

Being susceptible to an asset loss because of a threat. Exposure is not a realised threat but the fact that a vulnerability exists and it could be exposed.

9.3.6 Risk

Possibility that a threat will exploit a vulnerability to cause harm to an asset.

9.3.7 Safeguards

A safeguard is a countermeasure that removes a vulnerability or protects an asset from all or specific threats.

9.3.8 Attack

The actual exploitation of a vulnerability that may cause damage, loss or disclosure of assets.

9.3.9 Breech

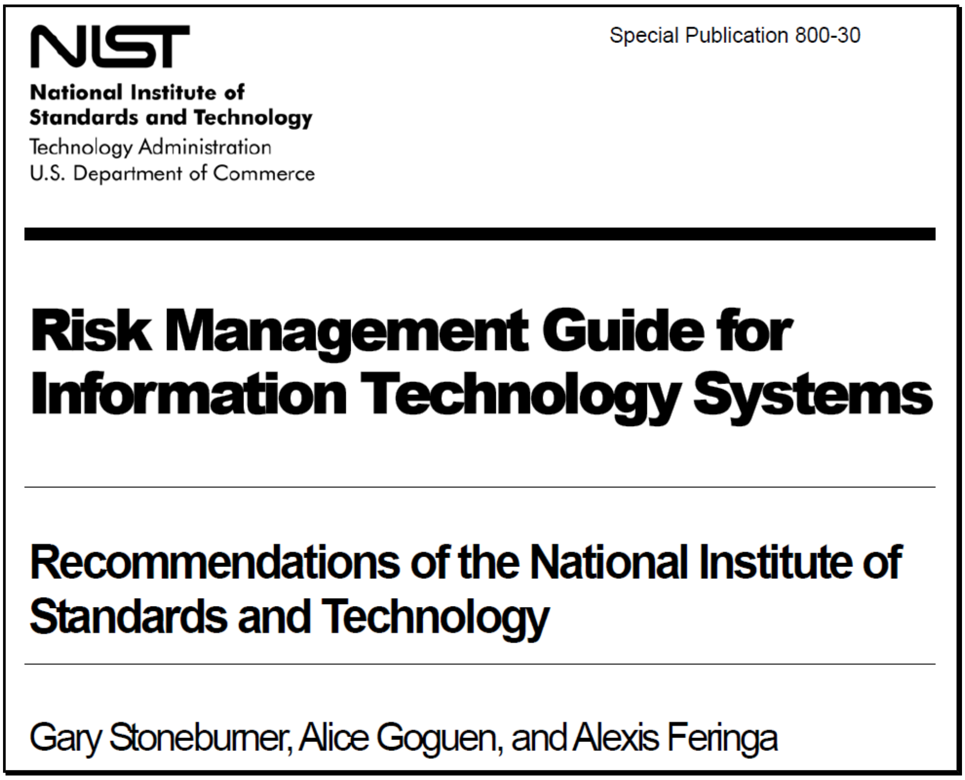
A breech is the occurrence of a security mechanism being bypassed or thwarted.

10. Risk Assessment

Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognised threat.

NIST SP 800-30 gives us Risk Assessment and Analysis steps.

- System Characterisation
- Thread Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Determination
- Control Recommendations
- Results Documentation



NIST

National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-30

Risk Management Guide for Information Technology Systems

Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa

http://www.nist.gov

10.1 Quantitative Risk Analysis

Quantitative risk analysis attempts to assign monetary values to the components of the risk assessment and to the assessment of the potential loss.

10.1.1 Asset Value (AV)

Asset valuation is the process of assigning financial value or worth to each information asset.

Some of the components of asset valuation include:

1. Value retained from the cost of creating the information asset
2. Value retained from past maintenance of the information asset
3. Value implied by the cost of replacing the information
4. Value from providing the information
5. Value acquired from the cost of protecting the information
6. Value to owners
7. Value of intellectual property
8. Value to adversaries
9. Loss of productivity while the information assets are unavailable
10. Loss of revenue while information assets are unavailable

An organisation must be able to place a dollar value on each information asset it owns, based on:

1. How much did it cost to create or acquire?
2. How much would it cost to recreate or recover?
3. How much does it cost to maintain?
4. How much is it worth to the organisation?
5. How much is it worth to the competition?

10.1.2 Exposure Factor (EF)

Loss Potential or the percentage of loss an organisation would realise if a risk was realised.

10.1.3 Single Loss Expectancy (SLE)

The monetary value expected from the occurrence of a risk on an asset. It is:

SLE = AV x EF

10.1.4 Annualised Rate of Occurrence (ARO)

An estimate based on the data of how often a threat would be successful in exploiting a vulnerability.

10.1.5 Annualised Loss Expectancy (ALE)

A calculation of the single loss expectancy multiplied the annual rate of occurrence, or how much an organisation could estimate to lose from an asset based on the risks, threats, and vulnerabilities. It is:

ALE = SLE x ARO

10.1.6 Annual Cost of Safeguard (ACS)

This is the cost of the researched safeguard.

10.1.7 Cost Benefit Analysis (CBA)

CBA determines whether or not a control alternative is worth its associated cost. CBAs may be calculated before a control or safeguard is implemented, to determine if the control is worth implementing, or calculated after controls have been implemented and have been functioning for a time:

CBA = (ALE(prior) – ALE(post)) – ACS

ALE (prior to control) is the annualised loss expectancy of the risk before the implementation of the control.

ALE (post-control) is the ALE examined after the control has been in place for a period of time.

10.2 Performing a quantitative risk analysis

The following is a step by step breakdown of the quantitative risk analysis.

1. Create an inventory of assets and assign a value [Asset Value (AV)].
2. Conduct a risk assessment and vulnerability study to determine the risk factors for each asset. For each threat calculate the Exposure Factor (EF) and Single Loss Expectancy (SLE).
3. Perform threat analysis to determine the likelihood of the threat occurring in a single year – Annualised Rate of Occurrence (ARO).
4. Determine the Annualised Loss Expectancy (ALE) for each risk factor.
5. Research countermeasures for each threat and calculate the change to the ARO and ALE if they were deployed.
6. Perform a Cost/Benefit analysis of the countermeasures and choose the most appropriate response to each threat.

Example

A Primary Webserver is compromised and becomes unavailable.

The server is valued at USh 12,000,000 and the EF is 70% (0.7).

SLE = AV x EF = USh 12,000,000 x 0.7 = USh 8,400,000

The cost for a single occurrence of the web site being unavailable is USh 8,400,000.

The ARO has been estimated to be four times per year based on types of vulnerabilities and threats that are known and documented that relate to this type of web-server.

This information is obtained from cases around the world, documented publications etc.

ARO = 4/year

This information is obtained from cases around the world, documented publications etc.

ALE = SLE x ARO = USh 8,400,000 x 4 = USh 33,600,000

Having completed research into possible safeguards a firewall/IDS was chosen at a cost of USh 18,000,000 per year with service contract.

ACS = USh 18,000,000

This system estimates a reduction in vulnerability of the system by 80% (0.2).

ALE (post) = ALE (prior) x 0.2 = USh 6,720,000

The CBA of the firewall/IDS can be obtained now.

CBA = (ALE(prior) – ALE(post)) – ACS = (USh 33,600,000 - USh 6,720,000) - USh

18,000,000 = USh 8,880,000

CBA = USh 8,880,000

A USh 18,000,000 annual expense yields a USh 8,880,000 annual cost saving.

10.3 Qualitative Risk Analysis

Relative measure of risk or asset value based on ranking or separation into descriptive categories such as low, medium, high; not important, important, very important; or on a scale from 1 to 10. Techniques such as the following are used to assess the risk and produce a Risk Registrar.

- Brainstorming
- Delphi Technique
- Storyboarding
- Focus Groups
- Surveys
- Questionnaires
- Check Lists
- Interviews

The Delphi Technique is a systematic, interactive forecasting method which relies on a panel of experts. The experts answer questionnaires in two or more rounds. After each round, a facilitator provides an anonymous summary of the experts' forecasts from the previous round as well as the reasons they provided for their judgements. Thus, experts are encouraged to revise their earlier answers in light of the replies of other members of their panel. It is believed that during this process the range of the answers will decrease and the group will converge towards the "correct" answer. Finally, the process is stopped after a pre-defined stop criterion (e.g. number of rounds, achievement of consensus, stability of results) and the mean or median scores of the final rounds determine the results.

11. Bibliography

(2012). COBIT 5, An ISACA Framework. A Business Framework for the Governance and Management of Enterprise IT. ISACA.

Lahti C, Peterson R (2005). Sarbanes-Oxley Compliance Using COBIT and Open Source Tools. First Edition Edition. Elsevier / Syngress.

Faris C, Gilbert B, LeBlanc B. (2013). Integrating the triple bottom line into an enterprise risk management program. [ONLINE] Available at: http://www.coso.org/documents/COSO-ERM%20Demystifying%20Sustainability%20Risk_Full%20WEB.pdf. [Accessed 06 December 2013].

Henning D (2009). Tackling ISO 27001: A Project to Build an ISMS. [ONLINE] Available at: http://www.iso27001security.com/GIAC_GCPM_gold_henning.pdf. [Accessed 06 December 2013].

ITIL (2013). ITIL - Core Cabinet Office Material . [ONLINE] Available at: http://www.itil-officialsite.com/Publications/Core.aspx. [Accessed 06 December 2013]. APM Group Ltd.

SEL (2010). CMMI for Development, Version 1.3. Carnegie Mellon University, SEI.

SEI (2010). CMMI for Services, Version 1.3. Carnegie Mellon University, SEI.

NIST (2012). Information Security: Guide for Conducting Risk Assessments. National Institute of Standards and Technology (NIST) SP 800-30.

NIST (2011). Information Security - Managing Information Security Risk Organization, Mission, and Information System View. National Institute of Standards and Technology (NIST) SP 800-39.

(ISC)² (2015) Official (ISC)² Guide to the CISSP Common Body of Knowledge. Fourth Edition.