ISM^3 1.20

Information Security Management Maturity Model

By Vicente Aceituno Canal

Thanks

I would like to thank the following people who contributed with work, organization or valuable comments to the development of this model (surname alphabetical order):

Editor and principal contributor:
Edward Stansfeld

Organization of V1.0:
Lorenzo Cavassa, Sicurante.
Pete Herzog, ISECOM.
Balwant Rathore, Oissg.

Intern of V1.0:
Marco Clemente, Sicurante

Reviewers of v1.0:
José Pedro Arroyo, Grupo SIA.
Rafael Ausejo, IT Deusto.
Marta Barceló, ISECOM
Ralph Hoefelmeyer, N-Frontier Technology.
Anthony B. Nelson, Estec Systems.
David Pye, Prism Infosec.
Dan Swanson, The Institute of Internal Auditors.

Reviewers of v1.2 (March 2006):
Gonzalo Lozano, Grupo SIA
Anup Narayanan, First Legion Consulting
Edward Stansfeld

Table of Contents

1 Executive Summary

The Information Security Management Maturity Model (ISM3, or ISM-cubed) offers a practical and efficient approach for specifying, implementing and evaluating process-oriented information security management (ISM) systems.

ISM3 aims to:

- Enable the creation of ISM systems that are fully aligned with the business mission.
- Be applicable to any organization regardless of size, context and resources.
- Enable organisations to prioritize and optimize their investment in information security.
- Enable continuous improvement of ISM systems.
- Support the outsourcing of security processes.

ISM3 is compatible with the implementation and use of ITIL, ISO9001, Cobit and ISO27001. This compatibility protects the existing investment in ISM systems when they are enhanced using ISM3. ISM3 based ISM systems are themselves accreditable, giving organisations an objective means of measuring and advertising their progress with information security management.

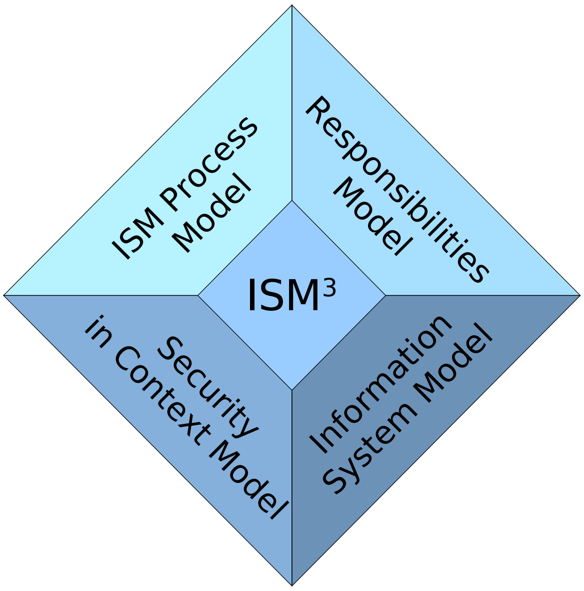
The management discipline and internal control framework required by ISM3 assists compliance with corporate governance law.

2 Introduction

2.1 General

The purpose of information security management (ISM) systems is to prevent and mitigate the attacks, errors and accidents that can jeopardize the security of information systems and the organizational processes supported by them.

ISM3 defines maturity in terms of the operation of key ISM processes and requires security to be aligned with business objectives. It recognises three broad levels of management responsibility and introduces a simple structural model for categorizing information assets.



1. ISM Process Model: Identifies key ISM processes at various levels of maturity.
2. Responsibilities Model: Provides a responsibilities-based view of an organization.
3. Security in Context Model: allows an organization to tailor its security objectives to its business needs.
4. Information System Model: Provides terminology for describing the main components and properties of information systems.

Process management is the core discipline of ISM3. It is through well-defined processes that information security is improved, risk is reduced and maturity is measured. Clear responsibilities are essential to process management and for corporate governance. Security aims must be appropriate to the business needs of the organisation and the security in context model helps to achieve this. Lastly, clear terminology is required for identifying the common components of information systems, so that ISM3 compliant security policies are robust and able to adapt to changing technologies.

ISM3 is designed with all kinds of organization in mind. In particular, businesses, non-governmental organisations and enterprises that are growing or out-sourcing may find ISM3 attractive.

2.2 Approach

Current standards approaches to information security and management can be classified as:

- Process oriented, (ISM3, CMMI, ISO9001:2000, ITIL/ITSM);
- Controls oriented (ISO27001:2005, BSI-ITBPM , ISO13335-4);
- Product oriented (Common Criteria / ISO15408);
- Risk analysis oriented (CORAS, CRAMM, Magerit, Mehari, Octave);
- Best practice oriented (ISO/IEC 17799:2000, Cobit, ISF-SGP).

ISM3 is a process-oriented standard that uses maturity levels. The approach applies ISO9001 quality management concepts to ISM systems. The equivalent of a quality manual is provided by the Security in Context Model, which ensures that an organisation's security objectives are aligned with its business aims and resources. The quality standard for each maturity level is determined by the adopted processes. The approach is therefore technology neutral and practitioners may use whatever protection techniques achieve the process objectives and work products.

2.3 Application

In applying the maturity model, a number of key ISM processes must be considered. Within a process, ISM3 does not take a prescriptive view of what activities should be performed, or their frequency.

The notation used for ISM3 processes describes certain fundamental properties. These include:

- The level of the organization responsible for each set of processes (strategic, tactical or operational);
- A rationale for the process. Every organization has a different context and resources, and therefore different processes are likely to be used;
- Inputs to the process;
- Products of the process. These can be documents, such as policies and reports, or they can be the result of recurring events, such as taking back-ups or analysing log files.

Every organization has unique context and resources, and so within maturity levels, different processes are likely to be applicable. Processes can also run several times in an organisation under different process owners or in different logical environments.

The structure of the process template is as follows:

Process	**Process Code and Denomination**
Description	The activity performed in the process.
Rationale	How the process contributes to specific and generic goals.
Documentation	Policies, Procedures and Templates Process Definitions needed to describe and perform the process.
Inputs	Inputs to the process. Inputs in *italics* or obtain from sources other than documents.
Work Products	Results of the process. Work Products in *italics* are work products other than documents.
Activity	Metric description of the volume of work products produced.
Scope	Metric description showing how much of the organisation or the environment is covered by the process.
Update	Metric description of the frequency of update of the process activity and the systems that support this activity.
Availability	Metric description of the period of time that a process has performed as expected upon demand, and the frequency and duration of interruptions.
Process Owner	An example of a process owner is given in this row. Every process should have one and no more than one process owner. When several people, such as business managers, are referred to as process owner, it means they are each responsible for separate instances of the process.
Related Processes	Other ISM3 processes that are required to generate key inputs.
Related Methodologies	Well-known methodologies and best practices. These methodologies may be useful to identify relevant activities, risks and controls.

2.4 Responsibilities Model

2.4.1. Structure

In describing organizational structure, the following definitions are used:

- Process owner: the person or team responsible for performance of a process;
- Role: a set of responsibilities assigned to a person or a team (process owner is an example of a role);
- Organizational chart: diagram of the responsibilities for supervision between roles;
- Border: defines the limits of the organization.

For a responsibility to be carried out properly, the person or team must be:

- Competent (have the appropriate knowledge and experience);
- Accountable (have a personal stake in the outcome);
- Empowered (have the freedom to take decisions and give feedback).

The following roles have special importance in ISM3:

- *Client*: as in the ITIL definition of a customer, a client is the person who provides resources and sets requirements for a process and a process owner;
- *Strategic management*: managers involved in the long-term alignment of IT with business needs;
- *Tactical management*: managers involved in the allocation of resources and the configuration and management of the ISM system;
- *Operational management*: managers involved in setting up, operating and monitoring specific processes.

The above definitions recognise that an individual can have more than one role, in relation to different duties. For example, in a small organisation, the IT manager may perform ISM duties at strategic, tactical and operational levels. In ISM3, the terminology is intended to indicate a level of abstraction above the operational role, not the job title or position of an individual. Some roles relevant to organizations are:

- Stakeholder (a shareholder, owner, bond holder, non-executive board member, or other, who has a stake in performance of the organisation, but no direct role in management);
- CEO (Chief Executive Officer or Managing Director, the senior executive with a strategic role);
- CIO (Chief Information Officer, manager with a strategic role responsible for the performance and integrity of information systems);
- CSO (Chief Security Officer, manager with a strategic role responsible for all aspects of organisational security;
- System Owner (a manager with a strategic role responsible for a business process reliant on an information system);
- User (someone authorised to use an information system);
- Information Security Officer (manager with tactical responsibility for ISM processes)
- Business Unit Managers;
- Human Resources (the part of the organization that selects, hires, and manages the professional progression of personnel);
- Facilities (the part of the organization that takes care of commodities like office space, storage, etc);
- Data Custodian (someone with an operational management role over a repository);
- Systems Administrator (someone an operational management role over an information system).
- Authorizer (someone permitted by the System Owner to authorise system access requests);
- Authority (the Systems Administrator of an access control system).
- Tester (someone in the organization testing on behalf of a Process Owner);
- Auditor (someone external to the organization testing on behalf of a Process Owner or a Client).

Some Committees (teams) relevant to organizations are:

- Executive Security Committee (oversees coordination between Internal Security and Partners Security, sets the rules on trust for suppliers and vendors)
  - CEO;
  - CIO.

- Security Committee (oversees coordination between Information Security, Security in the Workplace, Physical Security):
  - CEO;
  - CIO;
  - CSO;
  - Head of Human Resources;
  - Facilities Manager.

- Information Security committee (oversees Information Security):
  - CIO;
  - CSO;
  - Business Unit Managers.

2.4.2 Business Processes

ISM3 requires every information security process to have an identified process owner. A process owner may delegate operation or maintenance of a process to another role, while retaining responsibility and supervision for the process. The output from business processes may be either products or services and these may be produced automatically or not.

2.5 Security in Context Model

2.5.1 Security Definition

Security is defined as the result of the **continuous** meeting or surpassing of a set of objectives. The security in context approach aims to guarantee that business objectives are met. The ISM3 definition of security is therefore **context dependent**.

Traditionally, to be secure means to be *invulnerable (resilient to any possible attack)*. Using security in context, to be secure means to be *reliable, in spite of attacks, accidents and errors*. Traditionally, an incident is any loss of *confidentiality, availability or integrity*. Under security in context, an incident is a failure to meet the *organization's business objectives*.

This definition implies that an event which is classed as an incident at one organization may not be classed as an incident at other. For example, an organization, or a logical environment that handles no confidential information may not class viewing of its files by an unauthorised party as an incident.

2.5.2 Business Objectives

Organizations usually exist for a strategic purpose, such as growing capital or providing a service. There are also likely to be formal business objectives, such as growing revenue, preventing fraud and corruption and paying bills on time. The achievement of the business objectives depends on several factors, such quality issues, the competence and commitment of staff, competition and other market conditions. Business objectives depend increasingly dependent on information security as well. A key feature of the ISM3 approach is linkage of business objectives with security objectives.

Every organization exists for a certain purpose. Many organizations have the following business goals:

- Achieving a vision and mission;
- Continuing to exist;
- Maintaining and growing revenue;
- Maintaining and growing brand and reputation;
- Complying with regulations and contracts;

These general goals imply the accomplishment of specific business objectives, like;

- Paying the payroll on the 1st of every month;
- Paying all incoming invoices within a certain time frame;
- Paying taxes in time;
- Invoice all products and services provided;
- Deliver the products and services when and where committed by the organization;
- Keep any records needed to pass successfully any audit, like a tax audit or a software licences audit.
- Prevent theft, fraud and corruption;
- Prevent breach of contractual agreements;
- Protect intellectual property and legal rights;

The accomplishments of business objectives depend partially on the accomplishment of quality and security objectives.

2.5.3 Security Objectives

ISM3 requires an organisation to state its security objectives. These must be used as the basis for design, implementation and monitoring of the ISM system. Failure to meet a security objective will normally threaten achievement of a business objective. Security objectives may be expressed in fairly general terms using the information system model, such as:

- Use of services and access to repositories is restricted to authorized users;
  - Intellectual property is accessible to authorized users only;
  - Personal information of clients and employees is accessible for a valid purpose to authorized users only and is held for no longer than required;
  - Secrets are accessible to authorized users only;
  - Third party services and repositories are appropriately licensed and accessible only to authorized users;
  - Information repositories and systems are physically accessible only to authorized users.
- Availability of repositories, services and channels exceeds client needs;
- Reliability and performance of services and channels exceeds client needs;
- Existence of repositories and services is assured for exactly as long as client requirements;
- Expired or end of life-cycle repositories are permanently destroyed;
- Precision, relevance and consistency of repositories is assured;
- Accurate time and date is reflected in all records;
- Users are accountable for the repositories and messages they create or modify;
- Users are accountable for their use of services and acceptance of contracts and agreements.

An organization may vary its security objectives between logical environments, geographic locations or business units depending on local context. There must be a statement of security objectives for each logical environment; while these may be substantially the same between environments, there may also be differences, to reflect specific protection requirements, specific cost structures and specific use of technology.

Similarly, different organizations in the same sector are likely to have different security objectives.

2.5.4 Metrics

A Metric is a quantitative measurement that can be interpreted in the context of a series of previous equivalent measurements. In ISM3, metrics are used to determine whether security objectives are met, detect significant anomalies and to inform decisions to fix or improve the ISM processes. For a metric to be fully defined, the following items must be specified:

Metric	Name of the metric
Metric Description	Description of what is measured
Measurement Procedure	How is the metric measured
Measurement Frequency	How often is the measurement taken
Thresholds Estimation	How are the thresholds calculated
Current Thresholds	Current range of values considered normal for the metric
Target Value	Best possible value of the metric
Units	Units of measurement

In the ISM3 process model, only the metric description is given. This gives freedom for adopters to determine the nature, frequency and precision of measurement. It also means that for benchmarking purposes, metrics are not directly comparable between implementations unless the metric specifications are very similar.

2.5.4.1 Security Targets

A security target is the threshold of a metric that measures success in meeting business and security objectives, specifically, the number and cost of incidents due to failure to meet that business or security objective. The cost of incidents should consider:

- Direct costs:
  - Lost sales or service penalties;
  - Cost to return the system to the pre-incident state, including re-creation of the information;
  - Cost of maintaining business-as-usual during the incident;
  - Property damage and loss;
  - Others such as:
    - Financial penalties;
    - Higher insurance premiums;
    - Liability in the event of litigation.

- Indirect costs:
  - Damaged image or reputation;
  - Capital impairment, perhaps in the form of lost goodwill;
  - Loss of trust;
  - Treasury/cashflow implications;
  - Breach of contracts and other legal responsibilities;
  - Breach of social and moral obligations.

The threshold set for each security target depends on the logical environment. This allows a tighter set of targets to be established for more sensitive environments and helps to ensure that the ISM system is tailored to the needs of each environment in an organisation. The success or otherwise of an ISM system is measured in terms of achievement of its Security Targets. Some examples of security targets are:

Security & Business Objectives	Security Targets
Use of services and access to repositories is restricted to authorized users	• Fewer than two incidents every year • Loss is less than 0.1% of the accounting value of the company
Availability of repositories, services and channels exceeds client needs	• Fewer than twenty incidents per year. • Loss is less than 0.1% of the accounting value of the company
Existence of repositories and services is assured for exactly as long as client requires	• Fewer than two incidents per month. • Loss is less than 0.1% of the accounting value of the company
Intellectual property is accessible to authorized users only	• Fewer than two incidents every five years • Loss is less than 0.1% of the accounting value of the company
Personal information is accessible to authorized users only and is held for no longer than required	• Fewer than one incident every year. • Loss is less than 0.1% of the accounting value of the company
Secrets are accessible to authorized users only	• Fewer than one incident every five years • Loss is less than 0.1% of the accounting value of the company •
All records needed to pass any audit, such as a tax audit or a software licences audit, are available when required	• Less than one incident per ten years • Loss is less than 0.1% of the accounting value of the company
Prevention of information theft, fraud and corrupt practices.	• Fewer than one incident per two years. • Loss is less than 0.1% of the accounting value of the company.
Third party services and repositories are appropriately licensed and accessible only to authorized users	• Fewer than one incident per ten years. • Loss is less than 0.1% of the accounting value of the company.
Information systems are physically accessible only to authorized users	• Fewer than one incident per ten years. • Loss is less than 0.1% of the accounting value of the company.
Paying the payroll on the 1st of every month;	• Fewer than one incident per two years.
Paying taxes in time;	• Fewer than one incident per ten years. • Loss is less than 0.1% of the accounting value of the company.
Invoice all products and services provided;	• Fewer than ten incidents per year. • Loss is less than 0.1% of the accounting value of the company.
Deliver the products and services when and where committed by the organization;	• Fewer than ten incident per year. • Loss is less than 0.1% of the accounting value of the company.
Keep any records needed to pass successfully any audit, like a tax audit or a software licences audit.	• Fewer than one incident per five years. • Loss is less than 0.1% of the accounting value of the company.

2.5.4.2 Process Metrics

The success and performance of ISM3 processes is measured by process metrics. Process metrics assist management but do not themselves lead to the detection of incidents, which is the goal of OSP-23 Events Detection and Analysis.

Good process metrics help to detect abnormal conditions in a process, give a basis for comparison and aid management decision-making. Process metrics often vary between measurements and so the normal range and the trend are important qualities.

ISM3 specifies four basic types of process metric:

- Activity: The number of work products produced in a time period;
- Scope: The proportion of the environment or system that is protected by the process. For example, AV could be installed in only 50% of user PCs;
- Update: The time since the last update or refresh of process work products and related information system. It refers as well to how updated are the information systems that perform or support the process;
- Availability: The time since a process has performed as expected upon demand (uptime), the frequency and duration of interruptions.

The following performance metrics are also acknowledged by ISM3:

- Efficiency / Return on security investment (ROSI): Ratio of losses averted to the cost of the investment in the process. This metric measures the success of a process in comparison to the resources used.
- Efficacy /Benchmark: Ratio of work products produced in comparison to the theoretical maximum. Measuring efficacy of a process implies the comparison against a baseline.

2.5.4.3 Using Process Metrics and Security Targets

When the target for a process metric is set, it is compared with measured values and trends. Normal values are estimated from historic data. If the process metric has statistical variations, values within the arithmetic mean plus/minus twice the standard deviation may be considered "normal", as they make more than 95.4% of the values. Fluctuations within the “normal” range would not normally be investigated. Poor performance of a process will take process metrics outside normal thresholds. Managers may use process metrics to detect and diagnose the malfunction and take business decisions depending on the diagnosis.

Diagnosis	Business Decision
Fault in Plan-Do-Check-Act cycle leading to repetitive failures in a process	Fix the process
Weakness resulting from lack of transparency, partitioning, supervision, rotation or separation of responsibilities (TPSRSR)	Fix the assignment of responsibilities
Technology failure to perform as expected	Change / adapt technology
Inadequate resources	Increase resources or adjust security targets
Security target too high	Revise the security target if the effect on the business would be acceptable
Incompetence, dereliction of duty	Take disciplinary action
Inadequate training	Emergency and long term training of personnel

Representation of metrics will vary depending on the type of comparison and distribution of a resource. Bar charts, pie charts and line charts are most commonly used. Colours may help to highlight the meaning of a metric, such as the green-amber-red (equivalent to on-track, at risk and alert) traffic-light scale. Units and the period represented must always be given for the metric to be clearly understood. Rolling averages may be used to help identify trends.

2.6 Information System Model

2.6.1 Components

Information Systems are complex and have various tangible and intangible components. The components can be classed according to structural and transactional features.

Structural Features– the various assets from which an information system may be built:

- *Repositories*: Any temporary or permanent storage of information, including RAM, databases, file systems and any kind of portable media;
- *Interfaces*: Any input/output device, such as screens, printers and fax;
- *Channels*: Physical or logical pathways for the flow of messages, including buses, LAN networks, etc. A *Network* is a dynamic set of channels;
- *Borders* define the limits of the system.

Physical devices can host one or many logical components. Structural objects exist in every logical and physical level. The table below contains examples of each type of structural asset:

Repository	**Interface**	**Channel**
Payroll Database	Web-based interface	HTTPS
Database Replica	System call	TCP
File system	Monitor, keyboard and mouse	Frame relay PVC
Hard drive	Connector	Cable

When defining security requirements, policies or procedures, an organization should use asset description levels appropriate to the threats faced. The OSI model can be used to select an appropriate level of detail. For example, most organizations will draft policies relating to the security of high-level channels (such as OSI level 7 and above). Some organisations may be at risk from interception of a low level channel (OSI level 1), such as infra-red on a wireless keyboard, and have specific policies for infra-red channel.

Transactional Features – the various assets from which an information system produces actual results:

- *Services. Any value provider in an information system, including services provided by BIOS, operating systems and applications. A service can collaborate with other services or lower level services to complete a task that provides value, like accessing information from a repository;*
- *Messages*. Any meaningful information exchanged between two services or a user and an interface.

Transactional assets are dynamic, such as running processes and moving messages. Static assets such as mail or program files stored in a repository are not considered either a message or a service.

2.6.2 Properties

Several properties of information systems need to be defined in order to align the ISM system with organisational needs. These are classification, priority, durability, and information quality. Life-cycle is also an important factor which must be considered. These properties can be used to grade and categorize classes of asset into, for example, “high priority” and “normal priority”. As managing several categories is difficult and costly, the number of categories should be kept to the minimum required to describe the properties of the environment. Categorization must lead to distinctive treatment of the graded objects. If two objects are treated equally in all situations, they belong to the same categories.

2.6.2.1 Classification

Repositories and Messages can be classified according to security objectives for secrecy, privacy, licensing and protection of intellectual property. Classification is often used as the basis for access control, digital rights management and licensing controls. The specific terms of rights on intellectual property and licenses are relevant for their appropriate protection.

2.6.2.2 Priority

Services, interfaces and channels can be classified according to security objectives for priority. Three factors are relevant:

- Availability: the period of time when a service, interface of channel must be accessible and usable upon demand; e.g 9 hours a day every working day between 8 and 17h.
- Criticality: the longest time of the availability time a service, interface or channel can be interrupted; e.g 15 minutes a day during working hours.
- Volatility: the oldest recent messages and information that can be lost because of an interruption of service, channel or interface; e.g 5 minutes of information and transactions per interruption.

In a multi-tiered information system, the priority of higher level services is propagated to the lower level services they depend on.

2.6.2.3 Durability

The durability of a repository is the length of its planned life-cycle. Retention periods are often determined by business purpose or by legal and fiscal requirements. Two factors are relevant:

- Retention period: the minimum length of time a repository is kept; e.g 5 years since creation.
- Expiry: the date the repository should be destroyed reliably; e.g 10 years since end of use.

2.6.2.4 Information Quality

The information quality of a repository is a measure of how fit the repository is to fulfil security objectives. Two factors are relevant:

- Completeness: what information is available in comparison with the information needed; e.g. 98% of lines installed are in the invoicing database.
- Accuracy: what is the rate of errors in the information available; e.g 0,5% errors in customer addresses.

The information quality of Access Control records normally require the storage of usage, audit trail and other details.

2.6.2.5 Lifecycles and Environments

Depending on the mission, size and physical environment of an organization, there may be a number of different logical environments. Within these, systems go through the different states that make up their lifecycle.

In ISM3, a logical environment is a set of systems with a defined life-cycle under the same management / process owner. Life-cycle control processes are used to mitigate particular threats to systems and security measures. In particular, control processes are expected during the transitional period when a system is moving from one stage to another. Different environments will have their own security objectives and their own instances of ISM processes. Every process may have different thresholds for process metrics and security targets, which helps to adapt the process to the needs of the environment. This helps to optimize the drawbacks of targeting a high level of protection in all environments just because one of them needs that protection. The following are examples of common logical environments, with examples of the states that make up their lifecycles:

- User environment.
  - Reception;
  - Delivery;
  - Operation;
  - Change of ownership;
  - External maintenance;
  - Retirement;
  - Sale;
  - Theft.

- Server environment.
  - Concept;
  - Development or Selection & Acquisition;
  - Operation;
  - Maintenance;
  - Retirement.

- Security measures environment.
  - Concept;
  - Development or Selection & Acquisition;
  - Operation;
  - Maintenance;
  - Retirement.

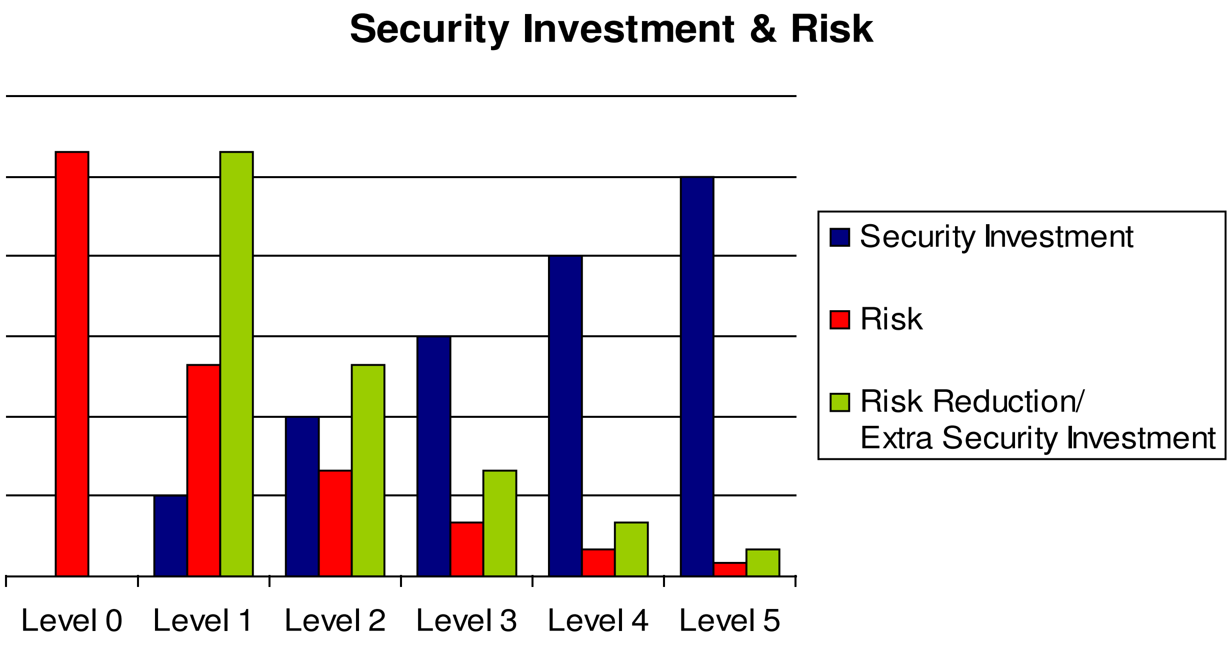
- Services development environment.
  - Requirements;
  - Analysis;
  - Design;
  - Build;
  - Test;
  - Configuration;
  - Deployment.

Lifecycles are not always linear or cyclical. Certain events can shift an object from one state to another, in a non-linear or non-cyclical fashion.

3 Using ISM3

3.1 Maturity Levels

Processes are allocated to maturity levels according to a spectrum, from a basic ISM system to an advanced one. Cost is taken into account since it is better to apply processes giving a high return on investment at earlier maturity levels.



(Risk reduction / Extra security investment x40 for better reading)

Mayfield's Paradox and a study from Carnegie Mellon[1] shows that as security posture improves, the marginal cost of further improvement also increases.

An organisation may choose to implement any of the defined processes at any stage of maturity. However, this should be related to specific security objectives. Similarly, it is possible to choose not to implement some required processes. For accreditation, this decision must be consistent with the organisation's security objectives.

ISM3 Level 1
This level should result in a significant risk reduction from technical threats, for a minimum investment in essential ISM processes. This level is recommended for organizations with low Information Security Targets in low risk environments that have very limited resources.

ISM3 Level 2
This level should result in further risk reduction from technical threats, for a moderate investment in ISM processes. It is recommended for organizations with normal Information Security Targets in normal risk environments that need to demonstrate good practice to partners and are keen to avoid security incidents.

ISM3 Level 3
This level should result in the highest risk reduction from technical threats, for a significant investment in Information Security processes. This level is recommended for organizations with high Information Security Targets in normal or high-risk environments, for example organisations dependent on information services and e-commerce.

[1] Carnegie Mellon University (2000) "The Survivability of Network Systems: An Empirical Analysis"

ISM3 Level 4

This level should result in the highest risk reduction from technical and internal threats, for a high investment in Information Security processes. This level is recommended for mature organizations affected by specific requirements for example highly regulated organisations, such as stock exchange listed corporations, government bodies and financial institution

ISM3 Level 5

The difference between this level and ISM3 Level 4 is the compulsory use of process metrics. Mature organizations that have some experience running a ISM3 Level 4 ISM system can optimize and continuously improve their ISM system at this level.

3.1.1 Levels Tables

General

	Level 1	Level 2	Level 3	Level 4	Level 5
GP-1 Document Management	Pass	Pass	Pass	Pass	Pass
GP-2 ISM System Audit	Pass	Pass	Pass	Pass	Pass

Strategic Management

	Level 1	Level 2	Level 3	Level 4	Level 5
SSP-1 Report to Stakeholders	Pass	Pass	Pass	Pass	Pass
SSP-2 Coordination	Pass	Pass	Pass	Pass	Pass
SSP-3 Strategic vision	Pass	Pass	Pass	Pass	Pass
SSP-4 Define TPSRSR rules				Pass	Pass
SSP-5 Check compliance with TPSRSR				Pass	Pass
SSP-6 Allocate resources for information security	Pass	Pass	Pass	Pass	Pass

Tactical Management

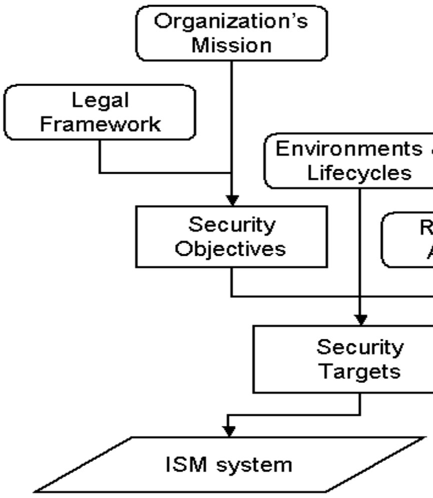
	Level 1	Level 2	Level 3	Level 4	Level 5
TSP-1 Report to strategic management	Pass	Pass	Pass	Pass	Pass
TSP-2 Manage allocated resources	Pass	Pass	Pass	Pass	Pass
TSP-3 Define Security Targets	Pass	Pass	Pass	Pass	Pass
TSP-4 Service Level Management			Pass	Pass	Pass
TSP-5 Define Properties Groups		Pass	Pass	Pass	Pass
TSP-6 Define environments and life-cycles		Pass	Pass	Pass	Pass
TSP-7 Background Checks				Pass	Pass
TSP-8 Security Personnel Selection				Pass	Pass
TSP-9 Security Personnel Training			Pass	Pass	Pass
TSP-10 Disciplinary Process		Pass	Pass	Pass	Pass
TSP-11 Security Awareness		Pass	Pass	Pass	Pass
TSP-12 Select Specific Processes	Pass	Pass	Pass	Pass	Pass

Operational Management

	Level 1	Level 2	Level 3	Level 4	Level 5
OSP-1 Report to tactical management	Pass	Pass	Pass	Pass	Pass
OSP-2 Select tools for implementing security measures		Pass	Pass	Pass	Pass
OSP-3 Inventory Management			Pass	Pass	Pass
OSP-4 Information Systems Environment Change Control		Pass	Pass	Pass	Pass
OSP-5 Environment Patching	Pass	Pass	Pass	Pass	Pass
OSP-6 Environment Clearing		Pass	Pass	Pass	Pass
OSP-7 Environment Hardening		Pass	Pass	Pass	Pass
OSP-8 Software Development Life-cycle Control			Pass	Pass	Pass
OSP-9 Security Measures Change Control		Pass	Pass	Pass	Pass
OSP-10 Backup & Redundancy Management	Pass	Pass	Pass	Pass	Pass
OSP-11 Access control		Pass	Pass	Pass	Pass
OSP-12 User Registration		Pass	Pass	Pass	Pass
OSP-14 Physical Environment Protection Management		Pass	Pass	Pass	Pass
OSP-15 Operations Continuity Management			Pass	Pass	Pass
OSP-16 Segmentation and Filtering Management	Pass	Pass	Pass	Pass	Pass
OSP-17 Malware Protection Management	Pass	Pass	Pass	Pass	Pass
OSP-18 Insurance Management				Pass	Pass
OSP-19 Attacks, Errors and Accidents Emulation (Internal Audit)		Pass	Pass	Pass	Pass
OSP-20 Incident Emulation			Pass	Pass	Pass
OSP-21 Information Quality Probing				Pass	Pass
OSP-22 Alerts Monitoring		Pass	Pass	Pass	Pass
OSP-23 Events Detection and Analysis				Pass	Pass
OSP-24 Handling of incidents and near-incidents			Pass	Pass	Pass
OSP-25 Forensics				Pass	Pass

3.2 Implementation Guidelines

The deployment of ISM3 differs depending on whether or not there is an existing ISM system. If an ISM system is in place, the first step should be to prepare a gap analysis of the systems and processes in place, against the target ISM3 maturity level. Implementation then ensures that quality management is strong, that the ISM system is aligned with the organisation's security objectives and that the required processes are documented and operated to the ISM3 standard.



The following considerations apply to a new implementation:

- Obtain management commitment;
- Name CISO and set up Executive Security Committee and Information Security Committee;
- Determine ISM3 target maturity level (if any);
- Determine any regulatory requirements;
- Determine implementation strategy;
- Set up Strategic Management processes;
  - Determine the security objectives;
  - Determine the information security budget;
- Set up selected Tactical Management processes;
  - Determine the logical environments and life-cycles;
  - Determine ISMS scope of accreditation and boundaries, with rationale for inclusion and exclusion;
  - Classify repositories and services, name system owners;
  - Set the security targets per environment;
  - Choose a process selection method;
  - Select appropriate operational processes per environment;
- Determine the process metrics;
- Set up operational ISM processes and assign responsibilities;
- Design and document the ISM3-based ISM system:
  - Agreements;
  - Policies;
  - Procedures;
  - Templates.
- Create and publish Information Security Policies;
- Train Management and Users on their ISMS responsibilities;
- Review operation of all processes;
- Revise security targets;
- Operate the ISM system;
- Define and refine the process metrics thresholds;
- Audit the ISM system periodically;
- Optionally, certificate the ISM system;
- Maintain and improve the ISM system;

3.3 Certification Guidelines

3.3.1 ISM3 Certification

ISM3 Levels may be accredited under ISO9001 and ISO27001 certification schemes:

	Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
ISO9001 certification	Yes	Yes	Yes	Yes	Yes[1]
ISO27001 certification	No	No	No	Yes	Yes[1]

(1): As neither the ISO27001 nor ISO9001 certification audits check for the use of metrics, accreditation of ISM3 Level 5 requires the certification of the ISM metrics by an accredited company.

The primary goal of a business-oriented ISM system should be the meeting of business objectives. For this reason, certification is optional and no preference is stated for any certification scheme.

To achieve certification of an ISM3 system, both the presence or the absence of every process must be justified.

3.3.2 Scope of Accreditation

All environments that host critical information systems of an organisation must be covered by the ISM system. As a rule of thumb, if the organization can survive for two weeks without the environment, the environment is considered not critical.

Any organisation that can survive two weeks without information systems is considered non IT-bound and is not eligible for accreditation.

3.4 Information Security Management Limitations

The performance of a well designed ISM system depends on the budget, the capability and the commitment of those involved in running it. The use of ISM3 does not guarantee that a process will perform properly; it only guarantees that the cause of faults is not poor process design. Accreditation may demonstrate that a process is in place, but it does not guarantee results. Being ISM3 compliant can be compared to earning an MBA. An MBA indicates that the holder is knowledgeable about business, but it does not guarantee success.

It is also important to note that some threats to organizations fall outside the scope of information security management. Some such threats are of internal origin and non-technical, often involving erroneous, malicious or fraudulent actions of staff. Such threats include:

- Human error;
- Incompetence;
- Fraud;
- Corruption.

Performance is the responsibility of management. However, the use of transparency, partitioning, supervision, rotation and separation of responsibilities (TPSRSR) on ISM and non-ISM processes can help to protect the organisation and information systems from these kinds of threat.

3.4 Relationships with Third Parties

ISM3 accreditation can be used to regulate the relationships with partners, customers and suppliers:

- As a way to evidence the organisation's stance on security;
- As part of a contract to ensure commitment by one of the parties to security management;
- As a selling point for vendors;
- As a requirement for outsourcing providers;
- As a mechanism to ensure mutual understanding of the services and work products obtained from an security outsourcing provider.

The following guidelines about outsourced ISM3 services may be used:

1. The service should be defined in a contract written and signed by legal representatives of both parties and should be governed by the laws of the client's country.
2. The contract should include procedures to vary the services provided and a pricing mechanism for agreed changes;
3. The service provider should:
    - Have a legal entity in the client's country, and have a physical address where it can receive legal notifications;
    - Provide the service in the language of the client;
    - Avoid and declare conflicts of interests;
    - Employ qualified, trained, experienced and committed commercial and technical personnel, whom should behave according to legal and ethical rules of conduct;
    - Manage personnel turnover through succession planning and minimal dependencies on key personnel;
    - Provide a customer care desk with a single point of contact and means to track the current state of incidents, change requests and inquiries;
    - Inform the client about:
        - Methodology used for the services provided;
        - Performance in relation to provision of the service;
        - Procedures in place to provide disaster recovery and business continuity;
        - Any subcontracting of all or part of the service. The service provider should be fully responsible for any mishap in the service caused by subcontracted parties;
        - Any circumstance that may affect the service negatively.
    - Allow the client to audit the service provided and co-operate as required with such auditors as the client appoints;
    - Provide information for benchmarking purposes at least once during the course of the contract;
    - Hand over gracefully to another service provider if required at the end of the contract.

4. The client should:
   - Designate a relationship manager for the contract;
   - Provide clear security objectives and timely and relevant outputs from in-house ISM processes;
   - Provide a contract help desk for its own employees to ensure that change requests to the service provider are managed, monitored and controlled;
   - Provide for regular meetings with the service provider to discuss performance.

The following may serve as an outline for the content of the outsourcing proposal:

1. Goals of the service
2. Methodology of provision of the service
3. Scope of the service
4. Budget
5. Organization and communication
6. Resources (service provider and client)
7. Security objectives and security targets relevant to the service
8. Schedule of tasks, including phase in and eventual phase out of the service
9. Description of the Service provided:
   - Scheduled service time (24x7, etc) with detailed start and end time. Special dates when the service is under certain limitation must be specified;
   - Overtime specified as time out of the scheduled service time, including the cost.
10. Underpinning Contract:
    - Bonuses and penalties specified in detail and unambiguously (a bail or insurance policy may serve as a guarantee on the penalties becoming effective if necessary);
    - A mechanism for the costing and pricing of contract variations and additional services;
    - A mechanism for metrics to be verified by an independent party.
11. Dependencies between the service provider and third parties, such as software and hardware distributors or makers.
12. Jurisdiction for the resolution of conflicts.

4 Information Security Management Model

4.1 Introduction

Security is the result of a process. The better the security process, the better the protection achieved from the resources available.

Using Security in Context, an incident is defined as a failure to meet the organization's Security Objectives. Since the definition is context dependent, ISM3 does not consider any single set of security measures or security management processes as compulsory or useful for all organizations.

To manage something means to define and achieve goals, while optimising the use of resources. Management activities normally include the requirements to plan, direct, control and coordinate.

There are three levels of Security Management:

- Strategic (Direct and Provide), which deals with broad goals, coordination and provision of resources;
- Tactical (Implement and Optimize), which deals with the design and implementation of the ISM system, specific goals and management of resources;
- Operational (Execute and Report), which deals with achieving defined goals by means of technical processes.

In a small to medium-sized organisation it is possible that the three levels may be compressed into two, with senior management taking on both Strategic and Tactical responsibilities. Junior management could have both Tactical and Operational roles.

4.2 Generic Goals

The generic goals of an ISM system are to:

- Prevent and mitigate incidents that could jeopardize the organization's property and the output of products and services that rely on information systems;
- Optimise the use of information, money, people, time and infrastructure.

4.3 Generic Work Products

The work products of an ISM system are:

- Incident prevention;
- Incident mitigation;
- *Risk reduction;*
- *Trust.*

The better the processes for assuring these products, the better security, and repeated meeting of the Security Objectives should result.

4.4 Generic Practices

4.4.1 Document Management

The Document Management process underpins the ISM System by defining document quality standards and contributes to keeping it up-to-date through the requirement for document expiry and review. It includes the following:

- Review and approval procedures when a document is created or updated;
- Distribution of current version and revocation of older versions;
- Version number and version date in every document;
- Document retrievability, expiry and retention policy;
- Document catalogue maintenance.

Generic Practice	**GP-1 Document management**
Description	The document management process covers organisation of the documents and records associated with specific processes.
Rationale	The robustness and repeatability of security processes is assured when associated documents are attributable, up-to-date, retrievable and subject to a review process.
Documentation	GP-011-Review and Approval Policy GP-012-Review and Approval Procedure GP-013-Distribution Policy GP-014-Distribution Procedure GP-015-Document Retrievability, Expiry and Retention Policy. GP-016-Catalogue Maintenance Procedure
Inputs	Process description, responsibilities and scope
Work Products	**Agreements**: Documents to specify commitments and responsibilities related to the process. For example: • Acceptable Use Policy: Informs users about their obligations when using the organization's information systems; • Third Party Code of Connection: Define mutual commitments at the organization's borders with others; • Insurance Policy. • Non Disclosure Agreements. **Reports**: Documents to reflect the results of a process. **Templates and Forms**: General layout and format of type of document. **Plans**: Documents to define the scope of a process and how to set it up.

Generic Practice	**GP-1 Document management**
Work Products (continued)	**Policies**: Documents to specify requirements and rules for the process: • Information Security Policy, which must include Information Security Objectives; • Lifecycle Control Policy; • Backup & Redundancy Management Policy; • Access Control Policy; • User Registration Policy; • Physical Protection Policy; • Operations Continuity Policy; • Segmentation and Filtering Controls Policy; • Malware Protection Policy. **Procedures**: Documents that reflect what a process does and how it relates to other processes. These documents normally specify: • What the procedure is for; • Who can apply it, who can change it; • Responsibilities for compliance with the procedure; • Scope of the procedure (who and where); • When the process starts and finishes; • Step by step description of tasks (who, what, when); • Acceptable task completion times; • How to solve and escalate conflicts/exceptions; • Related forms and communication channels. Metrics Report
Activity	Number of documents updated
Scope	Proportion of documents catalogued and subject to lifecycle
Update	Time since last document update Mean time between updates of documents
Availability	Percentage availability of the catalogue and of the systems where documents are stored.
Process owner	The individual who has responsibility for creating or updating the document.
Related Processes	All ISM3 processes.
Related Methodologies	ISO9001:2000

4.4.2 ISM System Audit

This can be carried out either internally or using external audit consultants. The scope and nature depends on the management level. Operational audit is concerned with how well operational processes perform. Tactical audit assesses how well resources are managed, and Strategic audit considers governance.

The auditor should be independent of the process owner and competent to carry out the work. The auditor should plan, document and carry out the audit to minimise the chance of reaching an incorrect conclusion. For external audits, professional guidelines issued by certification bodies should be followed.

Generic Practice	**GP-2 ISM System Audit**
Description	This process validates that the ISM system is implemented as defined. It can be applied to test all processes or a representative sample.
Rationale	Incidents arising from faults in the ISM system can be prevented by checking the system and taking action to address areas of improvement.
Documentation	GP-021-ISM Audit Manual GP-022-ISM Process Audit Program GP-023-ISM Audit Report Template
Inputs	Complete ISM documentation Work Products of every audited process
Work Products	ISM Audit Report Metrics Report
Activity	Number of ISM Audit Reports submitted
Scope	Percentage of ISM processes that have been audited at least once
Update	Time since last ISM Audit Report submission Mean time between ISM Audit Report submissions Mean time between ISM process audits
Availability	Not Applicable
Process owner	Information Security Management (Tester) Independent Auditor
Related Processes	All ISM3 processes.
Related Methodologies	ISACA IS Auditing Standards ISACA IS Control Professionals Standards

4.5 Specific Practice: Strategic Management

Strategic management are accountable to stakeholders for the use of resources through governance arrangements. The Clients of strategic management are therefore external (and possibly internal) stakeholders.

Specific Goals
Strategic management fulfils the following responsibilities in respect of security:

- Provides leadership and coordination of:
  - Information security;
  - Physical security;
  - Workplace security (outside scope of ISM3);
  - Interaction with organizational units.
- Reviews and improves the information security management system, including the appointment of Managers and internal and external auditors;
- Defines relationships with other organisations, such partners, vendors and contractors.
- Provides resources for information security;
- Defines Security Objectives consistent with organizational objectives, protecting stakeholders interests;
- Specify the Information Security Metrics to be Reported to the Board;
- Sets the organizational scheme of delegation.

4.5.1 Reporting

Process	**SSP-1 Report to stakeholders.**
Description	Annual or quarterly report to stakeholders of compliance with applicable regulations, and of performance in relation to budget allocations and Security Targets.
Rationale	In order to take decisions about future investment and activities of the organization, stakeholders require information about performance, including significant developments in information security.
Documentation	SSP-011-Strategic Information Security Report Template.
Inputs	Operational Information Security Report. Tactical Information Security Report Metrics Reports for the rest of Strategic Processes
Work Products	Strategic Information Security Report. Metrics Report
Activity	Number of Strategic Information Security Reports submitted
Scope	Not Applicable
Update	Time since last Strategic Information Security Report submission Mean time between Strategic Information Security Report submissions
Availability	Not Applicable
Process owner	Chief Executive Chief Information Officer
Related Processes	TSP-1 Report to strategic management.
Related Methodologies	Not Applicable

4.5.2 Coordination

Process	**SSP-2 Coordination**
Description	Coordination between leadership of the organization and leadership of the security function.
Rationale	Coordination between personnel responsible for security (information, physical, personal) and organizational leaders is required to ensure the support of the whole organization and help the organization achieve its goals and optimise resources.
Documentation	SSP-021-Meeting Minutes Template
Inputs	*Information Security and other Security objectives*
Work Products	Meeting Minutes Metrics Report *Information Security processes that support the organization.*
Activity	Number of Meeting Minutes submitted
Scope	Not Applicable
Update	Time since last Meeting Minutes submission Mean time between Meeting Minutes submissions
Availability	Not Applicable
Process owner	Chief Executive
Related Processes	Not Applicable
Related Methodologies	Not Applicable

4.5.3 Strategic Vision

Process	**SSP-3 Strategic vision**
Description	Identification of information Business Objectives. Scope includes the following areas: • Organizational mission and environment; • Statutory / regulatory compliance; • Privacy protection, both of employees and customers; • Intellectual property protection.
Rationale	Development of specific Business Objectives requires a strategic understanding of the organization’s environment and business goals. The Business Objectives provide the foundation for the Information Security Policy and the Information Security Targets.
Documentation	SSP-031-Information Security Policy Template
Inputs	*Organizational objectives and strategy*
Work Products	Information Security Policy Metrics Report
Activity	Not Applicable
Scope	Not Applicable
Update	Time since last Information Security Policy (reviewed) submission Mean time between Information Security Policy (reviewed) submissions
Availability	Not Applicable
Process owner	Chief Executive
Related Processes	SSP-4 Define rules for the division of duties: transparency, partitioning, supervision, rotation and separation of responsibilities (TPSRSR). TSP-3 Define Security Targets. TSP-12 Select Specific Processes.
Related Methodologies	Not Applicable

4.5.4 Scheme of Delegation

Process	**SSP-4 Define rules for the division of duties: transparency, partitioning, supervision, rotation and separation of responsibilities (TPSRSR).**
Description	In this process, rules are defined for the allocation and management of security responsibilities throughout the organization.
Rationale	Clear rules for the division of duties can improve the use of resources and reduce the risk of security incidents by helping protect the organization from internal threats.
Documentation	SSP-041-TPSRSR Policy Template
Inputs	*Organizational objectives and strategy*
Work Products	TPSRSR Policy Rules for transparency, partitioning, supervision, rotation and separation of responsibilities should be applied throughout the organization, such as: • Transparency: an audit trail should exist for all critical organizational processes that can be checked by supervisors and auditors; • Partitioning: all responsibilities should belong to one and only one role. No responsibility should be left unassigned; • Supervision: for every role there should be another role with the responsibility to check and supervise actively or passively; • Rotation: no person should hold a responsibility indefinitely (or even predictably). No person should hold certain critical roles for an unlimited span of time; • Separation of responsibilities: no person should carry out a sensitive process from end to end, or hold incompatible roles. Metrics Report
Activity	Not Applicable
Scope	Not Applicable
Update	Time since last TPSRSR Policy (reviewed) submission Mean time between TPSRSR Policy (reviewed) submissions
Availability	Not Applicable
Process owner	Chief Executive Business Unit Managers
Related Processes	SSP-5 Check compliance with TPSRSR rules.
Related Methodologies	Not Applicable

4.5.5 Testing and Auditing

Process	**SSP-5 Check compliance with TPSRSR rules**.
Description	This process ensures that the defined Scheme of Delegation is followed, so that personnel are not in a position to over-ride internal controls.
Rationale	To ensure that the rules for transparency, partitioning, supervision, rotation and separation of responsibilities (TPSRSR) rules are followed, there should be an audit process of independent verification.
Documentation	SSP-051-Compliance with TPSRSR Rules Template.
Inputs	Information Security Policy TPSRSR Policy
Work Products	Compliance with TPSRSR Rules Report. Metrics Report
Activity	Number of Compliance with TPSRSR Rules Reports submitted
Scope	Percentage of business processes that have been audited at least once
Update	Time since last Compliance with TPSRSR Rules Report submission Mean time between Compliance with TPSRSR Rules Report submissions Mean time between business process audits
Availability	Not Applicable
Process owner	Independent Auditor Tester
Related Processes	SSP-4 Define rules for the division of duties: transparency, partitioning, supervision, rotation and separation of responsibilities (TPSRSR).
Related Methodologies	Not Applicable

4.5.6 Resource Allocation

Process	**SSP-6 Allocate resources for information security**
Description	This process allocates resources for people, budget and facilities to tactical and operational management.
Rationale	Implementation of an ISM system requires investment in tactical and operational management processes.
Documentation	SSP-061-Information Security Budget Template
Inputs	Information Security Budget Request
Work Products	Information Security Budget *Resources allocated to Information Security Management* Metrics Report
Activity	Number of Information Security Budgets submitted
Scope	Percentage of ISM processes that have resources assigned
Update	Time since last Information Security Budget submission Mean time between Information Security Budget submissions
Availability	Not Applicable
Process owner	Chief Executive Business Unit Managers
Related Processes	All ISM3 processes.
Related Methodologies	Not Applicable

4.6 Specific Practice: Tactical Management

Strategic Management is the Client of Tactical Management in respect of ISM processes. Tactical management is accountable to strategic management for the performance of the ISM system and for the use of resources.

4.6.1 Specific Goals

Tactical Management has the following purposes:

- Provide feedback to Strategic Management;
- Define the environment for Operational Management:
    - Define Security Targets;
    - Define efficacy and efficiency metrics;
    - Define information classes, priorities, durability and quality groups;
    - Define environments and lifecycles;
    - Select appropriate processes to achieve the Security Targets;
- Manage budget, people and other resources allocated to information security.

4.6.2 Reporting

Process	**TSP-1 Report to strategic management.**
Description	A regular report of security outcomes and the use of allocated resources.
Rationale	A report to strategic management is required to demonstrate the performance, efficiency and effectiveness of the ISM system.
Documentation	TSP-011-Tactical Information Security Report Template.
Inputs	Metrics Reports from Tactical Processes Operational Information Security Report.
Work Products	Tactical Information Security Report - As tactical management deals mainly with resources management, this report should include efficiency information. Metrics Report
Activity	Number of Tactical Information Security Reports submitted
Scope	Not Applicable
Update	Time since last Tactical Information Security Report submission Mean time between Tactical Information Security Report submissions
Availability	Not Applicable
Process owner	Chief Information Officer Information Security Tactical Manager
Related Processes	OSP-1 Report to tactical management
Related Methodologies	Not Applicable

4.6.3 Resource Management

Process	**TSP-2 Manage allocated resources.**
Description	Tactical Management allocates resources to all Tactical and Operational Management processes.
Rationale	Planning and control in the allocation of resources is required to ensure the ISM is configured to achieve the Security Targets.
Documentation	TSP-021-Information Security Resources Assignment Template TSP-022-Information Security Resources Request Template
Inputs	Information Security Budget
Work Products	Information Security Resources Assignment Information Security Resources Request Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of ISM processes that have resources assigned
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Information Security Tactical Manager
Related Processes	SSP-6 Allocate resources for information security
Related Methodologies	Not Applicable

4.6.4 Security Targets

Process	**TSP-3 Define Security Targets and Security Objectives**
Description	This process specifies Security Targets for specific Business Objectives, Security Objectives per environment associated, and related policies.
Rationale	The definition of the Security Targets and Security Objectives per environment provides the basis for building the processes of the ISM system.
Documentation	TSP-031-Information Security Targets Template TSP-033-Acceptable Use Policy Template TSP-034-Third Party Code of Connection Agreement Policy Template Lifecycle Control Policy Template
Inputs	Information Security Policy
Work Products	Information Security Targets Acceptable Use Policy Third Party Code of Connection Agreement Policy Lifecycle Control Policy Metrics Report
Activity	Number of Work Products submitted
Scope	Not Applicable
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Chief Information Officer
Related Processes	SSP-3 Strategic vision
Related Methodologies	Not Applicable

4.6.5 Service Level Management

Process	**TSP-4 Service Level Management**
Description	Defines process metrics for other processes in the ISM. • Reviews the thresholds for every process metric. • Diagnoses and requests action on abnormal metric measurements. • Evaluates de cost of incidents.
Rationale	Information derived from metrics provides an objective way of assessing the ISM system and its component processes.
Documentation	TSP-041-Process Metrics Definition Template TSP-042-ISM Performance and Return on Investment Report Template TSP-043-Incident Valuation Report Template
Inputs	Information Security Targets Incident Valuation Report Intrusion Report Forensic Report Metrics Reports from all processes
Work Products	Process Metrics Definition ISM Performance and Return on Investment Report Incident Valuation Report *Remediation of errors and faults in the processes* Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of processes with fully defined and monitored process metrics
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Information Security Tactical Manager
Related Processes	TSP-3 Define Security Targets OSP-24 Handling of incidents and near-incidents OSP-25 Forensics
Related Methodologies	Not Applicable

4.6.6 Assets Classification

Process	**TSP-5 Define Properties Groups**
Description	In this process, the IS Model is applied to define rules for identifying critical assets. At the same time, an asset analysis is done to identify special requirements for classification, priority, durability and information quality.
Rationale	Rules for identifying critical assets and an associated asset grading scheme are required to ensure all important assets can be identified.
Documentation	TSP-051-Properties Groups Definition
Inputs	Information Security Targets
Work Products	Properties Groups Definition Metrics Report
Activity	Number of Work Products submitted
Scope	Not Applicable
Update	Time since last Work Products submission
Availability	Not Applicable
Process owner	Chief Information Officer
Related Processes	TSP-3 Define Security Targets TSP-12 Select Specific Processes OSP-3 Inventory Management
Related Methodologies	Not Applicable

4.6.7 Environments & Lifecycles Definition

Process	**TSP-6 Define environments and lifecycles.**
Description	This process identifies significant logical environments and the lifecycle of each environment. Within each environment, there may be a separate instance of some operational processes.
Rationale	Identification and definition of different environments and the systems grouped within them is required to ensure that appropriate environmental and life-cycle control processes are implemented.
Documentation	TSP-061-Environments and Lifecycles Definition Template
Inputs	Lifecycle Control Policy *Working environments in the organization* *States and Events that mark state transition in every environment*
Work Products	Environments and Lifecycles Definition Metrics Report *Note: UML state diagrams are recommended for lifecycle documentation.*
Activity	Number of Work Products submitted
Scope	Percentage of systems that belong to a defined Environment
Update	Time since last Work Products submission
Availability	Not Applicable
Process owner	Chief Information Officer
Related Processes	OSP4-7 Information Systems Lifecycle Management
Related Methodologies	ISO15228

4.6.8 Personnel Management

Process	**TSP-7 Background Checks**
Description	This process aims to ensure that new employees in sensitive roles do not pose a threat to the organization.
Rationale	Personnel trusted to carry out security processes must be competent, accountable and empowered. Background checks can be used to evaluate the suitability of potential employees.
Documentation	TSP-071-Background Check Procedure TSP-072-Background Check Report Template
Inputs	Job Definition Human Resources Policies Information Security Targets
Work Products	Background Check Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of selection processes where background check was performed
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Human Resources.
Related Processes	TSP-8 Security Personnel Selection
Related Methodologies	Not Applicable

Process	**TSP-8 Security Personnel Selection**
Description	This process aims to guarantee the commitment, competency, knowledge and experience of new employees through evidence-based assessment.
Rationale	Personnel trusted to carry out security processes must be competent, accountable and empowered. Evidence in the form of responses to competence-based interview questions, professional certifications and educational qualifications are needed to support selection decisions.
Documentation	TSP-081-Selection of Security Personnel Procedure TSP-082-Selection of Security Personnel Report Template TSP-083-Non Disclosure Agreement Template
Inputs	Job Definition Contracts of Employment Human Resources Policies Information Security Targets
Work Products	Selection of Security Personnel Report Non Disclosure Agreements Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of hiring where personnel selection was performed Turnover of security staff
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Human Resources.
Related Processes	TSP-7 Background Checks
Related Methodologies	P-CMM

Process	**TSP-9 Security Personnel Training**
Description	This process ensures that security personnel develop their competence and professional skills.
Rationale	Personnel trusted to carry out security processes must be competent, accountable and empowered. A planned and monitored training and development program is required to ensure that processes are performed by competent personnel.
Documentation	TSP-091-Training on Security Report Template TSP-092-Security Training Plan
Inputs	Human Resources Policies Information Security Policy
Work Products	Training on Security Report Metrics Report
Activity	Number of Work Products submitted Number of security personnel trained
Scope	Percentage of security personnel who have received training
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Human Resources.
Related Processes	Not Applicable
Related Methodologies	P-CMM

Process	**TSP-10 Disciplinary Process**
Description	Disciplinary procedures prevent and mitigate incidents resulting from employee misbehaviour.
Rationale	Personnel trusted to carry out security processes must be competent, accountable and empowered. A disciplinary process is required to enforce personal accountability and responsibility.
Documentation	TSP-101-Disciplinary Procedure TSP-102-Disciplinary Report Template
Inputs	Incident Report Contracts of Employment Information Security Policy Acceptable Use Policy
Work Products	Disciplinary Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of incidents leading to disciplinary process
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Human Resources.
Related Processes	OSP-24 Handling of incidents and near-incidents
Related Methodologies	P-CMM

Process	**TSP-11 Security Awareness**
Description	This process informs and educates users, raising the profile of information security throughout the organization.
Rationale	A high standard of security awareness throughout the organisation is required to prevent and mitigate security incidents.
Documentation	TSP-111-Security Awareness Report Template
Inputs	Information Security Policy Acceptable Use Policy
Work Products	Security Awareness Report Staff Training Manual Metrics Report
Activity	Number of Work Products submitted Number of non-security personnel trained
Scope	Percentage of non-security personnel who have received training
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Human Resources
Related Processes	Not Applicable
Related Methodologies	Not Applicable

4.6.9 Security Process Selection

The selection of the most appropriate processes for accomplishing Security Targets can be based on different types of assessment or analysis:

- Business Impact Assessment;
- ISM3 Maturity Target;
- Risk Assessment;
- ROSI Assessment.
- Threat Assessment;
- Vulnerability Assessment;

ISM3 advocates the use of process selection methods that show the following qualities:

- Repeatability. This means two different independent practitioners should get virtually the same work products and results. This requirement excludes the use of estimations of probability not based on historic data.
- Productivity. This means the work products should serve as inputs for:
  - Identify threats and weaknesses,
  - Choosing what processes are appropriate for fulfilling the security objectives.
  - Prioritizing investment in security processes.
  - Quantifying investment in security processes.
- Cost-effectiveness. Setting up a ISM system should be cheaper than operating it, just like the cost of choosing a security tool should be small in comparison with the cost of purchasing and using the tool.

Process	**TSP-12 Select Specific Processes**
Description	This process selects the most appropriate operational processes to achieve the Security Targets.
Rationale	Every organization has different Security Targets, acts in different environments and has different resources. An appropriate selection of processes will give a good return on the security investment.
Documentation	Not Applicable
Inputs	Information Security Targets Information Security Budget Inventory of Assets Incident Reports Intrusions Reports Forensics Reports Attacks Emulation Test Reports Incident Emulation Test Reports Operations Continuity Test Reports Alternative Inputs: • Business Impact Evaluation Report • ISM3 Maturity Target • Risk Evaluation Report • ROSI Evaluation Report • Threat Evaluation Report • Vulnerability Evaluation Report

Process	**TSP-12 Select Specific Processes**
Work Products	Information Security Management Processes Definition Threats to Insure Report Security Processes Policies: • Segmentation and Filtering Controls Policy; • Redundancy & Backup Management Policy; • Access Control Policy; • Access Request Concession Policy; • Malware Protection Policy; • Incident Investigation Policy; • Physical and Environmental Protection Policy; • Operations Continuity Policy. Environmental Lifecycle Control Policies. For example: • Services Development Lifecycle Control Policy; • Information System Lifecycle Control Policy; • Security Measures Lifecycle Control Policy. Metrics Report
Activity	Number of Work Products submitted
Scope	Not Applicable
Update	Time since last Work Products submission
Availability	Not Applicable
Process owner	Chief Information Officer
Related Processes	TSP-3 Define Security Targets. SSP-6 Allocate resources for information security OSP-3 Inventory Management OSP-24 Handling of incidents and near-incidents OSP-25 Forensics OSP-20 Incident Emulation OSP-19 Attacks Emulation
Related Methodologies	Vulnerability Assessment: OSSTMM Risk Assessment: CRAMM, MAGERIT, MEHARI, OCTAVE

4.7 Specific Practice: Operational Management

Operational Management reports to the Chief Information Officer and the Information Security Tactical Manager.

4.7.1 Specific Goals

Operational Management has the following responsibilities:

- Provide feedback to Tactical Management, including Incident Reports;
- Identify and protect assets;
- Protection and support of information systems throughout their lifecycle;
- Management of the security measures lifecycle;
- Apply allocated resources efficiently and effectively;
- Carry out processes for incident prevention, detection and mitigation (both real time and following an incident).

4.7.2 Reporting

Process	**OSP-1 Report to tactical management.**
Description	A regular report of process results and the use of allocated resources.
Rationale	A report to tactical management is required to show the performance and effectiveness of the specific processes in use.
Documentation	OSP-011-Operational Information Security Report Template
Inputs	Metrics Reports from Operational Processes
Work Products	Operational Information Security Report Metrics Report
Activity	Number of Work Products submitted
Scope	Not Applicable
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Information Security Operational Manager
Related Processes	OSP-3 Inventory Management OSP-20 Incident Emulation OSP-23 Events Detection and Analysis OSP-24 Handling of incidents and near-incidents
Related Methodologies	Not Applicable

4.7.3 Tool Selection

Process	**OSP-2 Select tools for implementing security measures**
Description	Selection of the specific products that best fit the Information Security Objectives and metrics within the budget assigned.
Rationale	Efficient use of resources results from effective selection of appropriate security tools.
Documentation	OSP-021-Product Selection Recommendations Report Template
Inputs	Published Comparatives Selection Criteria Best Practices (Updates, Metrics, Learning curve, etc) Information Security Targets Information Security Budget
Work Products	Product Selection Recommendations Report Metrics Report
Activity	Number of Work Products submitted
Scope	Not Applicable
Update	Time since last Work Products submission
Availability	Not Applicable
Process owner	Information Security Operational Manager.
Related Processes	TSP-12 Select Specific Processes
Related Methodologies	ISO15408 - Common Criteria

4.7.4 Inventory Management

Process	**OSP-3 Inventory Management**
Description	This process identifies, grades, and values the assets (repositories, interfaces, services and channels) to be protected. It should identify the Information System Owner for each information system, the environment it belongs to and the current state within that environment. To maintain a fully accurate inventory can be expensive and is exceedingly difficult in big organizations. ISM3 recognizes this difficulty, so this process may be performed either as a periodic or a real time (detection) process.
Rationale	Operation of the ISM system depends upon the identification of critical assets to protect and an appropriate grading using classification, priority, durability and quality.
Documentation	OSP-031-Inventory Procedure
Inputs	*Known Hardware* *Known Software* *Other Known Information Repositories* Properties Groups Definition
Work Products	Inventory of Assets. *Classified Repositories and Messages* *Prioritised Interfaces, Services and Channels* *Durability and Quality grouped Repositories* Metrics Report
Activity	Number of Classified Repositories and Messages Number of Repositories grouped by Durability and Quality Number of Prioritised Interfaces, Services and Channels
Scope	Percentage of Repositories and Messages Classified Percentage of Repositories grouped by Durability and Quality Percentage of Interfaces, Services and Channels prioritised
Update	Time since last Work Products submission Mean time between Work Products submissions Time since Repositories and Messages Classification Time since grouping of Repositories by Durability and Quality Time since prioritization of Interfaces, Services and Channels
Availability	Percentage of time the Inventory is available
Process owner	Information Systems Management
Related Processes	TSP-5 Define Properties Groups OSP-4 Information Systems Environment Change Control
Related Methodologies	Not Applicable

4.7.5 Information Systems Lifecycle Management

Lifecycle maintenance is normally a responsibility of the Information Systems department. The security role has the responsibility for protecting information systems through their lifecycle.

Process	**OSP-4 Information Systems Environment Change Control**
Description	This process prevents incidents caused by changes of state within an environment and by transitions between environments. Examples of environments are: • Server environment; • User environment; • Development environment. Examples of states within an environment are: • Reception; • Operation; • Change of ownership; • External maintenance; • Retirement; • Sale; • Theft. When a component changes state, its manager or the purpose for which it is used may change. Channels and Interfaces to other environments may be affected.
Rationale	Incidents, including loss of information and reliability, can result from poorly managed transition between states in an environment.
Documentation	Environments and Lifecycles Definition Lifecycle Control Policy OSP-041-Environment Transition Controls Procedure
Inputs	Information System Lifecycle Controls
Work Products	*Compliant interfaces in every environment.* *Compliant channels in every environment.* *Compliant services in every environment.* *Compliant repositories in every environment.* Metrics Report
Activity	Number of state changes subject to change control
Scope	Percentage of environments subject to change control Percentage of state changes subject to change control
Update	Time since last state change subject to change control Mean time between state changes subject to change control
Availability	No Applicable
Process owner	Information Systems Management
Related Processes	TSP-5 Define environments and lifecycles OSP-5 Environment Patching OSP-6 Environment Clearing OSP-7 Environment Hardening OSP-22 Alerts Monitoring
Related Methodologies	Not Applicable

Process	**OSP-5 Environment Patching**
Description	This process covers the on-going update of services to prevent incidents related to known weaknesses.
Rationale	Patching prevents incidents arising from the exploitation of known weaknesses in services.
Documentation	OSP-051-Services Update Level Report Template OSP-052-Services Patching Management Procedure
Inputs	Inventory of Assets. Alerts and Fixes Report
Work Products	*Up to date services in every environment.* Services Update Level Report. Metrics Report
Activity	Number of Work Products submitted Number of patching updates in information systems
Scope	Percentage of information systems covered by the process
Update	Time since last Work Products submission Mean time between Work Products submissions Update level, calculated as follows: 1. Every information system update level is equal to the sum of the number of days old that are all the security patches pending to apply. 2. The environment update level is equal to the sum of the individual update levels, divided by the number of information systems. The lower this metric, the better. This metric allows checking of the progress of the patching process, and comparison of the update level of different environments.
Availability	Percentage of time the patching systems are available
Process owner	Information Systems Management
Related Processes	OSP-4 Information Systems Environment Change Control OSP-22 Alerts Monitoring
Related Methodologies	Not Applicable

Process	**OSP-6 Environment Clearing**
Description	This process covers procedures for secure clearing of repositories to prevent disclosure of information.
Rationale	Clearing or destroying of repositories is required to prevent disclosure incidents when an information system leaves an environment or passes outside the control of the organization.
Documentation	OSP-061-Repository Clearing Procedure. OSP-062-Clearing Report Template
Inputs	Inventory of Assets Alerts and Fixes Report
Work Products	*Cleared Repositories* Clearing Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of information systems susceptible to be cleared when changing state in the environment
Update	Time since last Work Products submission Mean time between Work Products submissions Time since last information system clearing
Availability	Not Applicable
Process owner	Information Systems Management
Related Processes	OSP-4 Information Systems Environment Change Control OSP-22 Alerts Monitoring
Related Methodologies	Not Applicable

Process	**OSP-7 Environment Hardening**
Description	This process improves the configuration of channels, services, interfaces and repositories at borders and clears the presence of unused channels, services, interfaces and repositories.
Rationale	Environment hardening is required for assets at an environment border, where the assets are visible to zones of lower or unknown security. This is to protect information in the visible asset and prevent the visible zone from extending further than required within the organization.
Documentation	OSP-071-Service Hardening Procedure OSP-072-Interface Hardening Procedure OSP-073-Repository Hardening Procedure OSP-074-Channels Hardening Procedure OSP-075-Hardening Report Template
Inputs	Inventory of Assets. Alerts and Fixes Report
Work Products	*Hardened services, interfaces, repositories and channels* Hardening Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of information systems susceptible to be hardened when changing state
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Information Systems Management
Related Processes	OSP-4 Information Systems Environment Change Control OSP-22 Alerts Monitoring
Related Methodologies	CIS NSA

Process	**OSP-8 Software Development Lifecycle Control**
Description	Organizations may choose between developing software in-house, or procuring it externally. Structured processes and controls are needed to check each installed service and information system is compliant with Security Targets.
Rationale	An information system designed without regard to the Information Security Targets may require additional security measures, resulting in higher maintenance costs.
Documentation	OSP-081-Software Development Security Controls OSP-082-Information Security Requirements OSP-083-Information Security Requirements Test Report Template
Inputs	Information Security Targets Alerts and Fixes Report
Work Products	*Certified and Working Software.* Information Security Requirements Test Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of Information systems under development tested for compliance
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Information Systems Management
Related Processes	OSP-22 Alerts Monitoring
Related Methodologies	SSE-CMM OWASP SPSMM ISO12207

4.7.6 Security Measures Lifecycle Management

Security measures complement information system security features. The security organization must support security measures throughout their lifecycle from selection through installation, operation and decommissioning.

4.7.6.1 Security Measures Change Control

Process	**OSP-9 Security Measures Change Control**
Description	This process prevents incidents related to changes of state of security measures within an environment and transitions between environments. Examples of environments are: • Server environment; • User environment; • Development environment. Examples of states within an environment are: • Acquisition; • Commissioning; • Production; • Decommissioning. When a component changes state at least who manages it or what it is being used for must change.
Rationale	Changes in security personnel, new network devices and altered security measures pose a threat of opening unexpected weaknesses.
Documentation	Environments and Lifecycles Definition Lifecycle Control Policy OSP-091-Security Measures Change Control Procedures OSP-092-Security Measures Change Control Report Template
Inputs	Information Security Targets Security Measures Lifecycle Controls.
Work Products	*Compliant Security Measures in every environment.* Security Measures Change Control Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of security measures subject to change control Percentage of of security measures state changes subject to change control
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	No Applicable
Process owner	Information Security Management
Related Processes	TSP-5 Define environments and lifecycles OSP-5 Environment Patching OSP-6 Environment Clearing OSP-7 Environment Hardening OSP-22 Alerts Monitoring
Related Methodologies	Not Applicable

4.7.6.2 Backup and Redundancy Management

Process	**OSP-10 Backup & Redundancy Management**
Description	This is a set of security measures to reduce the impact of equipment loss and failure.
Rationale	Incidents arising from the loss of repositories and disruption to channels, interfaces and services can be mitigated by backup processes and elimination of single points of failure.
Documentation	OSP-101-Backup and Restore Test Procedure OSP-102-Backup Report Template OSP-103-Restore Report Template OSP-104-Redundancy Test Procedure OSP-105-Redundancy Test Report Template OSP-106-Repository Retention Policy Properties Groups Definition
Inputs	Inventory of Assets Incident Detection Report
Work Products	*Prevention of permanent information loss from repositories* *Prevention of interruption of channels, interfaces and services* Backup Report Restore Report Redundancy Test Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of repositories covered by backup Percentage of redundant channels Percentage of redundant services Percentage of redundant interfaces Percentage of information systems free of single points of failure
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Percentage of time the backup and restore systems are available
Process owner	Information Systems Management Information Security Management
Related Processes	OSP-2 Select tools for implementing security measures OSP-23 Events Detection and Analysis OSP-3 Inventory Management
Related Methodologies	Not Applicable

4.7.6.4 Access Control

Process	**OSP-11 Access control**
Description	Access control is the means by which access is provided to authorized users, while denied to unauthorized ones. Access Control includes Authentication of users or services, Authorization of users or services and Logging of access and use of services, repositories, channels and interfaces.
Rationale	Incidents like espionage, unlawful use of private and licensed information, repudiation of agreements, denial of authorship and unauthorized change of messages and repositories from can be prevented by access control procedures.
Documentation	OSP-111-Access Control Policy OSP-112-Unauthorized Access Attempts Report Template Properties Groups Definition
Inputs	Inventory of Assets Inventory of Premises
Work Products	*Grant of access to authorized users* *Denial of access to unauthorized users* *Logs of access to classified Repositories* *Logs of access to classified Premises* *Logs of use of classified Services and Interfaces* Unauthorized Access Attempts Report Metrics Report
Activity	Number of Work Products submitted Number of access attempts denied Number of access attempts successful Number of login failed Number of login successful Number of session expired Number of credentials changed
Scope	Percentage of repositories protected by access control Percentage of services protected by access control Percentage of user accounts with limited consecutive login failed Percentage of user accounts with configured delays between consecutive login failed Percentage of user accounts which sessions expire Percentage of user accounts which maximum number of simultaneous sessions is one. Percentage of user accounts which credentials expire Percentage of user accounts which password credentials quality is controlled
Update	Time since last Work Products submission Mean time between Work Products submissions Time since last access attempts denied Mean time between access attempts denied Time since last access attempts successful Mean time between access attempts successful Time since last beginning of session failed Mean time between beginning of session failed Time since last beginning of session successful Mean time between beginning of session successful Time since last session expired Mean time between sessions expired Time since last credential change Mean time between credential changes

Process	**OSP-11 Access control**
Availability	Percentage of time the access control systems are available
Process owner	Information Security Management
Related Processes	OSP-2 Select tools for implementing security measures OSP-3 Inventory Management OSP-12 User Registration
Related Methodologies	RBAC

4.7.6.5 User Registration

Process	**OSP-12 User Registration**
Description	This process covers enrolment and the granting, denial and revocation of access rights. The rights requested can be related to: • Access or use of services, repositories and interfaces; • Credentials and cryptographic keys; • Changes in the filtering of channels; • Physical Access. Four roles are considered in this process: • System Owner (a manager with a strategic role responsible for a business process reliant on an information system); • User (someone authorised to use an information system); • Authorizer (someone permitted by the System Owner to authorise system access requests); • Authority (the Systems Administrator of an access control system).
Rationale	Incidents arising from the inappropriate grant of access can be prevented and mitigated by user registration procedures.
Documentation	Properties Groups Definition OSP-121-Access Request Concession Policy OSP-122-Access Requests Procedure OSP-123-Access Request Template
Inputs	Inventory of Assets Access Request Personnel List of Leavers
Work Products	*Grant of Requests to trusted users to repositories, channels, interfaces and services* *Denial of Requests to distrusted users to repositories, channels, interfaces and services* Log of denied and granted Access Requests Metrics Report
Activity	Number of Work Products submitted Number of access rights granted Number of access rights revoked Number of user accounts created Number of user accounts removed Number of user unused accounts expired Number of user accounts blocked Number of user accounts unblocked

Process	**OSP-12 User Registration**
Scope	Percentage of access control systems which unused user accounts expire Percentage of access control systems which password credentials for first login are not predictable Percentage of access control systems which require password credentials change upon first login.
Update	Time since last Work Products submission Mean time between Work Products submissions Time since last access rights granted Mean Time between access rights granted Time since last access rights revoked Mean Time between access rights revoked Time since last accounts created Mean Time between accounts created Time since last user accounts removed Mean Time between user accounts removed Time since last unused user account expired Mean Time between unused user account expiries Time since last beginning of user accounts blocked Mean time between beginning of user accounts blocked Time since last beginning of user accounts unblocked Mean time between beginning of user accounts unblocked
Availability	Percentage of time the user registration system is available
Process owner	Information Security Management
Related Processes	OSP-2 Select tools for implementing security measures OSP-3 Inventory Management OSP-14 Physical Environment Protection Management OSP-16 Segmentation and Filtering Management
Related Methodologies	Not Applicable

4.7.6.6 Encryption Management

OSP-13 Encryption Management has been deprecated. The rationale is that encryption is a technique to perform access control.

4.6.7.7 Physical Security

Process	**OSP-14 Physical Environment Protection Management**
Description	This process covers control of access into secure areas containing important repositories or interfaces. It also covers protection of critical infrastructure from fire, flood, over-heating and other physical threats.
Rationale	Incidents caused by direct exploitation of assets and by physical damage resulting from environmental factors can be prevented and mitigated by effective physical security measures.
Documentation	OSP-141-Physical and Environmental Protection Policy OSP-142-Physical Access Procedure OSP-143-Environmental Control Procedure Properties Groups Definition
Inputs	Inventory of Assets
Work Products	*Prevention of environmental incidents* *Prevention of unauthorized passage of assets between environments* Physical Presence Logs Environmental Conditions Logs Metrics Report
Activity	Number of Work Products submitted Number of beginning of session failed Number of beginning of session successful Number of user accounts blocked Number of user accounts unblocked
Scope	Percentage of repositories protected by access control Percentage of services protected by access control Percentage of access control systems which credentials expire
Update	Time since last Work Products submission Mean time between Work Products submissions Time since last beginning of session failed Mean time between beginning of session failed Time since last beginning of session successful Mean time between beginning of session successful Time since last credential change Mean time between credential changes
Availability	Percentage of time the access control systems are available
Process owner	Facilities Manager
Related Processes	OSP-2 Select tools for implementing security measures OSP-23 Events Detection and Analysis OSP-3 Inventory Management OSP-12 User Registration
Related Methodologies	Not Applicable

4.7.6.8 Operations Continuity Management

Process	**OSP-15 Operations Continuity Management**
Description	This process aims to reduce the impact of incidents that threaten the existence of the organization.
Rationale	Events that might cause a sustained difficulty in providing service with subsequent loss of customers and goodwill can be mitigated by operations continuity management before viability of the organization is seriously affected.
Documentation	OSP-151-Operations Continuity Procedure OSP-152-Operations Continuity Test Plan OSP-153-Operations Continuity Test Report Template Properties Groups Definition
Inputs	Inventory of Assets Incident Detection Report
Work Products	*Protection of the existence of the organization* Operations Continuity Test Report Metrics Report
Activity	Number of Work Products submitted Number of restore tests of backups under emulated serious incident conditions Number of emergency test of environments under emulated serious incident conditions
Scope	Percentage of repositories backed up in the environment Percentage of emergency channels Percentage of emergency services Percentage of emergency interfaces Percentage of information systems free of single points of failure
Update	Time since last Work Products submission Mean time between Work Products submissions Time since last restore tests of backups under emulated serious incident conditions Time since last test restore of critical environments under simulated serious incident conditions
Availability	Percentage of time the restore systems are available Time to readiness of the operations continuity systems tested
Process owner	Information Security Management
Related Processes	OSP-2 Select tools for implementing security measures OSP-23 Events Detection and Analysis OSP-3 Inventory Management OSP-20 Incident Emulation
Related Methodologies	Not Applicable

4.7.6.9 Segmentation and Filtering Management

Process	**OSP-16 Segmentation and Filtering Management**
Description	This process defines technical policies for the passage of authorized messages between zones, while denying passage to unauthorized messages.
Rationale	Incidents arising from intrusion, vandalism and misuse of information systems can be prevented and mitigated by appropriate segmentation of environments and repositories and filtering of messages.
Documentation	OSP-161-Segmentation and Filtering Policy OSP-162-Internal Zones Filtering Procedure OSP-163-Border Filtering Procedure OSP-164-Filter Authorizations Report Template
Inputs	Environments & Lifecycles Definition Inventory of Assets Incident Detection Report Intrusion Detection Report
Work Products	*Prevention of unauthorized passage of messages between environments* Filter Authorizations Report Logs of use of channels Metrics Report
Activity	Number of Work Products submitted Number of Drops Number of Pass Number of filtering rules changes
Scope	Percentage of connections to other environments that are protected
Update	Time since last Work Products submission Mean time between Work Products submissions Update level, calculated as follows: 1. Update level of each filtering system is equal to the number of days old of updates notified but not yet applied. 2. The overall update level is equal to the sum of the individual update levels, divided by the number of filtering systems. The lower this metric, the better. This metric provides a check on the appropriateness of the current filtering arrangements, and allows comparison of the update level of different environments.
Availability	Percentage of time the filtering systems are available
Process owner	Information Security Management
Related Processes	OSP-2 Select tools for implementing security measures OSP-23 Events Detection and Analysis OSP-3 Inventory Management OSP-12 User Registration
Related Methodologies	Not Applicable

4.7.6.10 Malware Protection

Process	**OSP-17 Malware Protection Management**
Description	This is a set of security measures to provide protection against technical threats such as viruses, spy ware, trojans, backdoors, key loggers and other unauthorised services.
Rationale	Incidents relating to the infection of internal assets with Malware can be prevented and mitigated by an appropriate Malware protection process.
Documentation	OSP-171-Malware Protection Procedure OSP-172-Malware Detection and Cleaning Report Template OSP-173-Malware Protection Deployment and Update Level Report Template
Inputs	Inventory of Assets Incident Detection Report
Work Products	*Protection of information systems from Malware* Malware Detection and Cleaning Report Malware Protection Deployment and Update Level Report Metrics Report
Activity	Number of Work Products submitted Number of malware items Cleaned Number of malware items Cleaning Errors
Scope	Percentage of systems covered by malware protection
Update	Time since last Work Products submission Mean time between Work Products submissions Update level, calculated as follows: 1.Malware update level for each information system is equal to the number of days old of malware signatures updates notified but not yet applied. 2.The overall environment malware update level is equal to the sum of the individual malware update levels, divided by the number of information systems. The lower this metric, the better. This metric measures the degree of readiness against new malware, and allows comparison of the update level of different environments. Note: Depending on the particular malware protection technology used, there might be more than one component to measure. Some malware protection technologies don't use signatures at all.
Availability	Percentage of time the malware protection systems are available
Process owner	Information Security Management
Related Processes	OSP-2 Select tools for implementing security measures OSP-23 Events Detection and Analysis OSP-3 Inventory Management
Related Methodologies	Not Applicable

4.7.6.11 Insurance Management

Process	**OSP-18 Insurance Management**
Description	This measure uses insurance to transfer risk to a third party, in exchange for payment of a fixed fee or premium.
Rationale	The financial impact of serious incidents can be mitigated by sharing of the risk with others through taking out an appropriate insurance policy.
Documentation	OSP-181-Insurance Management Policy
Inputs	Threats to Insure Report Inventory of Assets.
Work Products	*Threats Insured* Insurance Contracts Metrics Report
Activity	Number of Work Products submitted Number of information systems covered by insurance
Scope	Percentage of information systems covered by insurance
Update	Time since last Work Products submission
Availability	Not Applicable
Process owner	Information Security Management
Related Processes	TSP-12 Select Specific Processes
Related Methodologies	Not Applicable

4.7.7 Testing and Auditing

4.7.7.1 Attack Emulation

Process	**OSP-19 Attacks Emulation**
Description	This process validates the effectiveness of vulnerability reduction measures. It can be applied to all possible targets or a representative random sample. When performed from internal systems, it is commonly called internal vulnerability testing. When performed from external systems, is commonly known as penetration testing.
Rationale	Incidents arising from the exploitation of configuration weaknesses around the borders of an organisation can be prevented by attacks emulation and subsequent environment hardening, investment and improved monitoring.
Documentation	OSP-191-Information Security Targets OSP-192-Attacks Emulation Procedure OSP-193-Attack Emulation Report Template
Inputs	Inventory of Assets.
Work Products	Attack Emulation Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of information systems that have been tested in the environment
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Information Security Management (Tester) Independent Auditor
Related Processes	OSP-5 Environment Patching OSP-6 Environment Clearing OSP-7 Environment Hardening OSP-8 Software Development Lifecycle Control OSP-11 Access control over services, repositories channels and interfaces OSP-12 User Registration OSP-14 Physical Environment Protection Management OSP-16 Segmentation and Filtering Management OSP-17 Malware Protection Management
Related Methodologies	OSSTMM

4.7.7.2 Incident Emulation

Process	**OSP-20 Incident Emulation**
Description	This process validates the effectiveness of impact reduction security measures, which protect against accidents, errors and the failure of vulnerability reduction measures. This process can be carried out by testing all the possible targets or a representative random sample of them. It is often used to test operational continuity plans.
Rationale	The impact of major incidents can be mitigated by incident emulation in which planned testing is used to simulate an incident, walk-through its consequences and improve emergency response and impact reduction measures.
Documentation	OSP-152-Operations Continuity Test Plan OSP-153-Operations Continuity Test Report Template OSP-201-Incident Emulation Procedure OSP-204-Incident Emulation Test Report
Inputs	Information Security Targets.
Work Products	*Impact Reduction Controls Tested* Incident Emulation Test Report Operations Continuity Test Report Metrics Report
Activity	Number of Work Products submitted Number of incident emulations performed
Scope	Percentage of information systems tested under incident emulation in each environment
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Information Systems Management (Tester) Information Security Management (Tester) Independent Auditor
Related Processes	OSP-10 Backup & Redundancy Management OSP-15 Operations Continuity Management OSP-18 Insurance Management
Related Methodologies	Not Applicable

4.7.7.3 Information Quality

Process	**OSP-21 Information Quality Probing**
Description	Periodic review of information held to give assurance that it is accurate, up-to-date and held for a specific purpose. For example, logs normally have specific accuracy requirements and private information must be held only when necessary of a specific purpose. This process can be carried out by testing all the possible targets or a representative random sample of them.
Rationale	Incidents arising from the use or storage of information that is inaccurate, expired or wrongly labelled can be mitigated by an appropriately targeted quality probing process.
Documentation	OSP-211-Information Audit plan OSP-212-Information Update Report OSP-213-Information Erasure Report OSP-214-Information Archiving Report Fair Data Processing Legislation
Inputs	Inventory of Assets Information Surveys
Work Products	*Disclosures to public and commercial partners;* Information Update Report Information Erasure Report Information Archiving Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of repositories probed for quality
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Not Applicable
Process owner	Information Systems Management (Tester) Independent Auditor
Related Processes	OSP-3 Inventory Management
Related Methodologies	National data and privacy protection legislation EU European Directives USA HIPAA USA Safe Harbour USA. Privacy Act

4.7.8 Monitoring

4.7.8.1 Alerts Monitoring

Process	**OSP-22 Alerts Monitoring**
Description	This process checks that Information Security Management is aware of new weaknesses and fixes and is enabled to make an informed decision about whether or not to change information system configuration or patch level. Both employees and third parties can contribute to the discovery of weaknesses.
Rationale	Incidents resulting from the exploitation of published weaknesses in products and software can be prevented by timely application of appropriate corrective measures. Weakness in production systems discovered by employees or third parties need corrective action.
Documentation	OSP-221-Alerts Monitoring Procedure OSP-222-Employee Weakness Reporting Procedure OSP-223-Third Party Weakness Reporting Procedure (Public Document) OSP-224-Alerts and Fixes Report Template OSP-225-Corrective Actions on Alerts and Weaknesses Report Template
Inputs	Alerts Weakness and Fixes Report Inventory of Assets
Work Products	*Reviewed Alerts, Fixes and Weaknesses Reports* Alerts and Fixes Report Template Corrective Actions on Alerts and Weaknesses Report Template Metrics Report
Activity	Number of Work Products submitted Number of alerts and fixes reviewed
Scope	Percentage of systems which alerts and fixes are monitored
Update	Time since last Work Products submission Mean time between Work Products submissions
Availability	Percentage availability of the alerting information sources
Process owner	Information Security Management
Related Processes	OSP-4 Information Systems Environment Change Control OSP-9 Security Measures Change Control OSP-8 Software Development Lifecycle Control
Related Methodologies	SVRRP

4.7.8.2 Event Analysis

Process	**OSP-23 Events Detection and Analysis**
Description	This process covers the conversion into information of the data captured in event logs [information system, physical access, and environmental conditions] and other sources. This information may lead to the detection of incidents or intrusions. Employees can contribute to the discovery of incidents and intrusions.
Rationale	Incidents must be detected before a response can be made in mitigation. Detection can depend upon monitoring and analysis of events. If an incident is not detected, it may recur, or lead to incidents with a higher impact, resulting in chronic damage to information systems and failure to meet Security Targets.
Documentation	OSP-231-Incident and Intrusion Detection Procedure. OSP-232-Incident Detection Report Template OSP-233-Intrusion Detection Report Template
Inputs	*Events* Inventory of Assets
Work Products	*Incidents and Intrusions Detected* Incident Detection Report Intrusion Detection Report Metrics Report
Activity	Number of Work Products submitted Number of events detected
Scope	Percentage of events in the environment that are analysed
Update	Time since last Work Products submission Mean time between Work Products submissions Time since last event detected Mean time between events detection
Availability	Availability of event detection systems
Process owner	Information Security Management
Related Processes	OSP-10 to OSP-17 processes OSP-24 Handling of incidents and near-incidents
Related Methodologies	Not Applicable

4.7.9 Handling of Incidents

4.7.9.1 Incident Handling

Process	**OSP-24 Handling of incidents and near-incidents**
Description	This process aims to limit the impact of incidents and to gather information. The goals of incident management are to: • Contain the effects of the incident, including the recovery of repositories and information systems; • Gather data for forensics; • Gather information to learn from the incident; • Gather data to evaluate the impact and the security investment efficiency.
Rationale	Clear procedures for incident handling can help to mitigate the effects of an incident and prevent future recurrence. Information on incidents, intrusions and attacks should be used to improve the operation of security measures, take decisions on security investment and measure the efficiency of security measures.
Documentation	OSP-241-Incident Investigation Policy OSP-242-Incident Response Procedure OSP-243-Incident Report Template OSP-244-Intrusion Report Template
Inputs	Incident Detection Report Intrusion Detection Report
Work Products	*Incidents and near-Incidents Handled* Incident Report Intrusion Report Metrics Report
Activity	Number of Work Products submitted Number of incidents and near-incidents handled Number of intrusions handled
Scope	Percentage of incidents and near-incidents handled by this process Percentage of intrusions handled by this process
Update	Time since last Work Products submission
Availability	Not Applicable
Process owner	Information Security Management
Related Processes	OSP-23 Events Detection and Analysis OSP-25 Forensics
Related Methodologies	ISO18044

4.7.9.2 Incident Probing

Process	**OSP-25 Forensics**
Description	This process analyses the sequence and impact of incidents.
Rationale	Incident investigation helps to prevent and mitigate future incidents by improving security processes. Forensic analysis of the information gathered in the incident handling phase can be used to: • Evaluate the incident; • Identify corrective measures; • Support prosecution of attackers, if appropriate;
Documentation	OSP-251-Forensics Assessment Procedure. OSP-252-Forensic Report Template
Inputs	Incident Report Intrusion Report
Work Products	*Investigated Incidents and Intrusions* Forensic Report Metrics Report
Activity	Number of Work Products submitted
Scope	Percentage of incidents analysed
Update	Time since last Work Products submission
Availability	Not Applicable
Process owner	Information Security Management
Related Processes	OSP-24 Handling of incidents and near-incidents
Related Methodologies	Not Applicable

5 Responsibilities Management

Information Security Management (ISM) is no different from any other organizational process. Therefore, division of duty rules for transparency, partitioning, supervision, rotation and separation of responsibilities (TPSRSR) should be followed. The following are some Best Practice Guidelines:

Transparency
Responsibilities and reporting channels should be clearly defined, documented and communicated. In addition:

- Strategic ISM reports should be available to stakeholders, to the extent deemed appropriate to the laws, regulations and governance requirements of the organization;
- Operational ISM reports should be available to tactical and strategic ISM managers;
- Tactical ISM Reports should be available to strategic ISM managers.

Transparency is recommended for all maturity levels.

Partitioning
All instances of ISM processes should have one and only one Process Owner. The process owner may delegate a process, but still bears responsibility for the competency and due diligence with which it is performed.

Partitioning is recommended for all maturity levels.

Supervision
All ISM processes should have at least one supervisor.

- Stakeholders may act as supervisors of strategic ISM vision, to the extent deemed appropriate to the laws, regulations and governance requirements of the organization;
- Strategic ISM managers may act as supervisors of tactical ISM processes;
- Tactical ISM managers may act as supervisors of operational ISM processes.

Supervision is recommended for maturity levels 3 and above.

Rotation
All sensitive processes, especially audits, should be transferred periodically to another competent process owner, even if it is just to cover a 3-4 week holiday period. It should be difficult or impossible to forecast who the next process owner might be.

Rotation is recommended for maturity level 4 and above.

Separation
Separation of responsibilities helps to prevent internal fraud. In combination with Transparency, Separation brings accountability to business processes, making clear who is responsible for the outcomes of the process.

To ensure Separation works in practice, it will normally be necessary to designate an appropriate back-up to every participant in the process, so that if key people are away, the system does not break down.

The following related roles should be kept separate:

Incompatibility	ISM3 Level
Process auditor & Process Owner (PO)	1 and above
Incident victim & Forensics investigator	1 and above
Incident whistleblower & Forensics investigator	1 and above
ISM3 Auditor & any other PO	1 and above
Strategic PO & Operational PO (this incompatibility guarantees supervision)	2 and above
Authorizer & System Administrator	2 and above
Physical access control PO & Logical access control PO	3 and above
Request personnel & Select personnel (to prevent nepotism)	3 and above
Repository classifier & Repository user	3 and above
Information System Owner & System Administrator	3 and above
Weakness whistleblower & Patching management PO	3 and above
System Administrator & User	3 and above
Repository backup operator & Tape librarian	4 and above
Logs administrator & Logs keeper	4 and above

6 References

Paradigms

- Shewhart Cycle or Deming Wheel (Plan, Do, Check, Act)
- Le Moigne Triangle (Strategy, Tactics, Operations)
- People - Process – Technology.
- KISS (Keep It Simple, Stupid)

Papers

- “Towards maturity of information maturity criteria: six lessons learned from software quality criteria” Mikko Siponen, 2002.
- “Designing secure information systems and software: Critical evaluation of the existing approaches and a new paradigm” Mikko Siponen, 2002
- “Information Security Governance: Toward a Framework for Action” Business Software Alliance, 2003.
- CISWG Report of the Best Practices and Metrics Teams, http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661
- Federal Information Security Management Act 2002
- InfoSecGov4_04.pdf, http://www.cyberpartnership.org/InfoSecGov4_04.pdf
- University of New Haven "Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security"
- Carnegie Mellon University “The Survivability of Network Systems: An Empirical Analysis”

Standards

- BSI BS7799-2:2002, http://www.bsi-global.com/
- BSI BS ISO/IEC 27001:2005, http://www.bsi-global.com/
- BSI BS ISO/IEC 17799:2000, http://www.bsi-global.com/
- SEI CMMI, http://www.sei.cmu.edu/cmmi/
- ISACA COBIT, http://www.isaca.org/
- EA 7/03, http://www.european-accreditation.org
- ISO 13335, http://www.iso.org/
- ISO 19011:2002, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=31169
- ITSM, ITIL, http://www.itil-itsm-world.com/
- ISSA GAISP, http://www.issa.org/gaisp/_pdfs/v30.pdf
- IETF RFC2119, http://rfc.net/rfc2119.html
- NIST SP800-53, http://csrc.nist.gov/publications/nistpubs/
- NIST SP800-55, http://csrc.nist.gov/publications/nistpubs/

Related Methodologies and Certifications

- AEDI CAYSER http://www.aedi.es/asp/ACYS-0001.asp
- CIS, http://www.cisecurity.org/
- ISACA CISA, http://www.isaca.org/
- ISC2 CISSP, http://www.isc2.org/
- CORAS, http://coras.sourceforge.net
- CRAMM, http://www.cramm.com/
- ISO 9001:2000, http://www.iso.org/
- ISO 12207, http://www.iso.org/
- ISO 15408, http://www.iso.org/
- ISO 15228, http://www.iso.org/
- ISO 18044, http://www.iso.org/
- MAP MAGERIT, http://www.csi.map.es/csi/pg5m20.htm
- CLUSIF MEHARI https://www.clusif.asso.fr/fr/production/mehari/3.asp
- NSA, http://nsa2.www.conxion.com/
- NIST RBAC, http://csrc.nist.gov/rbac/
- ISECOM SPSMM, http://www.isecom.org/
- SSE-CMM, http://www.sse-cmm.org/
- OIS SVRRP, http://www.oisafety.org/
- CERT OCTAVE, http://www.cert.org/octave/
- ISECOM OPSA, OPST, http://www.isecom.org/
- ISECOM OSSTMM, http://www.isecom.org/
- ISECOM OWASP, http://www.owasp.org/
- SEI P-CMM, http://www.sei.cmu.edu/cmm-p/

7 Terminology

- Processes are coded with the following format: ***XY*P**, where **X** can be **S**trategical, **T**actical or **O**perational and **Y** can be **G**eneric or **S**pecific. **P** stands for **P**rocess.
- Words followed by an acronym in brackets [ ], are referenced to an existing publication or standard.
- Work Products in italics are *non-documentary* work products.

8 Glossary

Access
Any exchange of a message between an interface, a repository or a service.

Access right
A class of access to a repository, a service or an interface that can be granted or revoked.

Accident
A class of incident with non-human natural causes. (There is no ISO equivalent)

Alarm
A set of events likely to be caused by an incident.

Alert
A warning of a possible weakness. (Not equivalent to [ISO] Alert)

Assessment
All activities related to the certification/ registration of an organisation to determine whether the organisation meets all the requirements of the relevant clauses of the specified standard necessary for granting certification/ registration, and whether they are properly implemented, including documentation review, audit, preparation and consideration of the audit report and other relevant activities necessary to provide sufficient information to allow a decision to be made as to whether certification/ registration shall be granted.

Asset
Any valuable property of the organization.

Attack
An a class of incident with an intentional human cause. (Not equivalent to [ISO] Attack “An attempt to exploit a vulnerability”)

Audit
Systematic, independent and documented process for obtaining Audit Evidence and evaluating it objectively to determine the extent to which the Audit Criteria are fulfilled

Audit Criteria
Set of policies, procedures or requirements. Audit criteria are used as a reference against which Audit Evidence is compared.

Audit Evidence
Records, statements of fact or other information, which are relevant to the Audit Criteria and verifiable. Audit evidence may be qualitative or quantitative

Auditor
Person external to the organization with the Competence to conduct an Audit on behalf of a Process Owner or a Client

Authentication
Validation of the credentials presented to an information system at the moment the system is used.

Authorizer
A delegate of an Information System Owner who can approve or deny access requests to interfaces, repositories, channels and services of an information system.

Authorization
Ability to designate what services can be used and what information can be accessed by an authenticated user.

Authority
The technical person who implements approved access requests.

Availability

1. The period of time when a process must performed as expected upon demand with minimal or no interruptions.
1. The period of time when a service, interface of channel must be accessible and usable upon demand with minimal or no interruptions.

Border
A boundary between two environments or information systems having different characteristics.

Catastrophe
Any incident that could result in an organization's demise.

Certification Body / Registration body
A third party that assesses and certifies/ registers the ISMS of an organisation with respect to published ISMS standards, and any supplementary documentation required under the system.

Certification Document / Registration Document
Document indicating that an organisation's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system.

Certification System / Registration System
System having its own rules of procedure and management for carrying out the assessment leading to the issuance of a certification/ registration document and its subsequent maintenance.

Channel
A channel is the medium used by services to exchange messages transparently, without explicit help from other lower level services. This collaboration is normally needed for creating and closing logical channels.

Client
The client of a process who provides the resources and sets the requirements for the process.

Competence
Demonstrated personal attributes and demonstrated ability to apply knowledge and skills

Credential
An item used for authentication of a user account in an access control system.

Critical
A service is critical in a time span if the interruption of the service for a that span of time is highly likely to jeopardize general business objectives, for example:

- Achieving its mission;
- Continuing to exist;
- Maintain and grow its revenue;
- Maintain and grow its brand and reputation;
- Complying with regulations and contracts;

Device
Instrument, software, measurement standard, reference material, auxiliary apparatus or combination thereof used to measure a process metric.

Disaster
See Catastrophe

Environment

1. All the physical, logical and organizational factors external to the organization.
2. A technical zone of the organization with a defined purpose, like the Server environment, User environment, Development environment, etc.
3. Any subdivision of a logical, technical or organizational partition under a single management.

Error
A class of incident caused by a human because of a mismatch between the intended and the effective results of a task, or because of incorrect or missing information needed for the task. (There is no [ISO] Equivalent).

Event
Any fact that can lead to the detection of an incident. (Equivalent to [ISO] Alert).

Expectation
Any hope for the future state of assets, organizational processes or information systems.

Generic Goal
A goal achieved when a set of specific goals are achieved.

Generic Practice
An auxiliary process to a specific practice to achieve a generic goal.

Incident
A failure to meet a security objective resulting from accidents, errors or attacks. (There is no ISO Equivalent).

Intellectual property
Information which an organisation has rights over under copyright, trade mark or patent law.

Identification
Ability to identify a user of an information system at the moment he is granted credentials to that system.

Indicative Equipment
A Device that delivers qualitative information.

Interface
A means of information input or output between a user and an information system.

Information System
A human and technical infrastructure for the storage, processing, transmission, input and output of information.

Information System Owner
The Client [ITIL] of an information system, who has all the rights to the system, including discontinuation.

Intrusion
The theft of information about from a target by an attacker.

Impact
The direct and indirect cost of an incident including the cost of restoring the assets to the pre-incident state.

Licence
An agreement that details the rights granted by an intellectual property owner to use certain information.

Lifecycle
The set of states that make up a series of operational conditions of an information system.

Logging
Recording of the services have been used by an authorized user and what information has been accessed, created, modified or erased including details such when, when, where from, etc.

Login
Beginning of a session, normally using a credential for authentication. Also called Logon.

Logo
A symbol used by a body as a form of identification, usually stylised. A logo may also be a mark.

Logout
End of a session by the user account of by expiration. Also called Logoff.

Mark
A legally registered trade mark or otherwise protected symbol which is issued under the rules of an accreditation body or of a certification/ registration body indicating that adequate confidence in the systems operated by a body has been demonstrated or that relevant products or individuals conform to the requirements of a specified standard.

Management
To manage something is to define and achieve goals while optimising the use of Resources.

Measurement
Considers the determination of a physical quantity, magnitude or dimension (using Measuring Equipment).

Measuring Equipment
A Device that delivers quantitative information.

Message
Meaningful data exchanged between services in a hierarchical or peer-to-peer fashion.

Monitoring
Implies observing, supervising, keeping under review (using monitoring devices); it can involve measuring or testing at intervals, especially for the purpose of regulation or control

Network
A set of physical or logical channels connecting repositories and interfaces.

Node
An information system whose primary function is relay messages between channels (Not Equivalent to [ISO] Node).

Nonconformity
The absence of, or the failure to implement and maintain, one or more required management system elements, or a situation which would, on the basis of objective evidence raise significant doubt as to the capability of the ISMS to achieve the business objectives of the organisation.

Non repudiation
Ability to assert the authorship of a message or information authored by a second party, preventing the author to deny his own authorship.

Operational Level Agreement (OLA)
SLA between a process provider and a Client from the same organisation who is a process provider to other Clients.

Operational Process (OP)
A process that delivers the requirements set by tactical management.

Opportunity
The combination of an asset, a threat and an occasion that may give rise to an incident.

Organisation
Company, corporation, firm, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public or private, that has its own functions and administration.

Partition
Any subdivision of a whole that does not intersect totally or partially any other subdivision

Private information
Information that can identify a person.

Process
A organised set of tasks that uses resources and inputs to produce work products.

Provider
The process owner of a process that delivers its work products.

Process Owner
The person or team responsible for a process, including prioritizing, planning for growth, and accounting for costs.

Quality
The meeting or surpassing of expectations.

Registration Body
See Certification Body.

Registration Document
See Certification Document.

Registration System
See Certification System.

Reliability
The percentage of the Availability time a service, interface of channel must behave and produce results as intended.

Resource
A resource is anything needed to complete a task. Most resources stop being available to other tasks while they are being used. Some resources are exhausted after the task and can not be reused.

Some fundamental resources are:

- Time;
- Money;
- People;
- Logistics and Infrastructure;
- Information.

Repository
Any permanent or transient storage of information.

Responsibility
An assignment of a task, with power and resources, to a competent individual or a team accountable for the proper execution of the task.

Risk
The loss expectancy as a function of a set of incidents' vulnerability and impact, measured in monetary units per year. The maximum risk the certainty of losing the total value of the organization within a year or less.

Role
A set of responsibilities. (Equivalent to [ISO/IEC 15408-1] Role)

Secret
Information shared in a controlled way between a group of people.

Security
The repeated meeting of security objectives. (Not equivalent to [ISO] Security)

Security Objective
A business expectation or requirement that is dependent on a security process.

Security Target
A frequency and financial threshold for a metric derived from a security objective. (Not equivalent to [ISO] Security Target)

Service
Any code or program that provides value for users, via messages exchanged with other services and access to repositories.

Session
The set of successful and failed accesses to repositories and uses of services between the time a user account is authenticated and the time the authentication expires or the authentication is terminated.

Service Level Agreement (SLA)
Quality agreement between a process provider and a Client specified using a set of metrics.

Service Level Objective (SLO)
See Threshold

Specific Goal
An objective of a set of specific practices.

Specific Practice
A process.

Strategic Processes (SP)
Processes that determine the objectives of lower level processes.

Tactical Processes (TP)
Processes that provide a framework for operational delivery. These processes normally involve resources management (people, time, money, information, infrastructure, etc).

Target
The information asset which may be the victim or potential victim of an attack.

Tester
Someone in the organization testing on behalf of a Process Owner

Threat
Any potential cause of an Attack, an Accident or an Error.

Threshold
Value against which a measurement is benchmarked or evaluated. In the context of Service Level Agreements is called a Service Level Objective.

TPSRSR
Acronym for Transparency, Partitioning, Supervision, Rotation and Separation of Responsibilities.

Underpinning contract (UC)
A SLA between a external process or product provider with a Client.

User
The person who uses an information system.

User account
Representation of a user in an information system. A user account can be linked to a person or a group of persons.

Visibility
The degree to which information assets at a border present an interfaces or provide services to information systems outside the organization.

Vulnerability
The likelihood of an incident, measured as real instances against possible attacks, accidents and errors per year. These attacks, accidents and errors can be triggered by one or several threats. (Not equivalent to [ISO] Vulnerability)

Weakness
Any fault in services, messages, channels, repositories, interfaces, organizational processes or responsibilities assignment that provides an opportunity for an error, attack or accident. (Equivalent to [ISO] Vulnerability)