
ISM3
INFORMATION_SECURITY_MANAGEMENT_MATURITY_MODEL

ISBN: 978-84-613-0539-1

CONTACT INFORMATION

Calle Olímpico Francisco Fernández Ochoa, 9
28923 Alcorcón (Madrid) Spain
Mail: consortium@ism3.com
Phone:+ 34 620 527 478

LEGAL DISCLAIMER

This is an informational document, and it doesn't represent legal or professional advice from the ISM3 Consortium, the authors or reviewers of this document. This document is offered as is without any warranty of completeness, accuracy or timeliness. The ISM3 Consortium, the authors and reviewers of this document disclaim any implied warranty or liability.

LICENSE AND COPYRIGHT

ISM3 Consortium Members

ESTEC Security (http://www.security.estec.com/) - Canada

First Legion Consulting (http://www.firstlegion.net/) - India

Global4 (http://www.g4ii.com/) - Spain

M3 Security (http://www.m3-security.net/) - USA

Seltika (http://www.seltika.com) – Colombia

Valiant Technologies (www.valiant-technologies.com) - India

Acknowledgements

The ISM3 Consortium would like to thank the people who contributed with work, organization or valuable comments to the development of ISM3:

Principal Author (all versions):
Vicente Aceituno, ISM3 Consortium

Editor and principal reviewer and contributor (all versions):
Edward Stansfeld, Audit Scotland

Organization of v1.2 and later versions:
ISM3 Consortium

Organization of v1.0:
Lorenzo Cavassa, Sicurante
Pete Herzog, ISECOM
Balwant Rathore, Oissg
Marco Clemente, Sicurante (Intern)

Reviewers of v2.11 (November 2007):
Alex Hutton, Riskanalys.is
Scott Mitchell, Open Compliance and Ethics Group
Anthony B. Nelson, Estec Security
Kelly Ray, Open Compliance and Ethics Group
K Rama Subramaniam, Valiant Technologies Pvt Ltd
Jeff Warren, DHS – Government of Victoria / Australia

Reviewers of v2.0 (February 2007):
Krishna Kumar, DNV
Anup Narayanan, First Legion Consulting
Anthony B. Nelson, Estec Security

Reviewers of v1.2 (March 2006):
Gustavo Lozano, SIA
Anup Narayanan, First Legion Consulting

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

Processes Index

Processes Change Log

- OSP-13 Encryption Management deprecated since v1.20.
- OSP-18 Insurance Management renamed since v1.90 to TSP-13 Insurance Management.
- SSP-5 Check compliance with TPSRSR rules included since v1.90 in GP-2 ISM System and Business Audit
- TSP-5 Define Properties Groups deprecated since v1.90 is now part of TSP-3 Define Security Targets.
- TSP-12 ISM Design and Evolution renamed since v2.00 to GP-3 ISM Design and Evolution
- SSP-4 Define rules for the division of duties: transparency, partitioning, supervision, rotation and separation of responsibilities (TPSRSR) renamed since v2.00 to SSP-4 Define Division of Duties rules.
- TSP-8 Security Personnel Selection renamed since v2.10 to TSP-8 Personnel Security
- OSP-2 Select tools for implementing security measures renamed since v2.10 to OSP-2 Security Procurement

Documents Index

1 Executive Summary

The Information Security Management Maturity Model (ISM3, or ISM-cubed) extends ISO9001 quality management principles to information security management (ISM) systems. Rather than focussing on controls, it focusses on the common processes of information security, which are shared to some extent by all organizations.

Under ISM3, the common processes of information security are formally described, given performance targets and metrics, and used to build a quality assured process framework. Performance targets are unique to each implementation and depend upon business requirements and resources available. Altogether, the performance goals for security become the Information Security Policy. The emphasis on the practical and the measurable is what makes ISM3 unusual, and the approach ensures that ISM systems adapt without re-engineering in the face of changes to technology and risk.

Implementations of ISM3 are compatible with ISO27001 (Information Security Management Systems – Requirements), which establishes control objectives for each process. Implementations use management responsibilities framework akin to the IT Governance Institute's CobIT framework model, which describes best practice in the parent field of IT service management. ITIL users can employ ISM3 process orientation to strengthen ITIL security process seamlessly. Using ISM3 style metrics, objectives and targets it is possible to create measurable Service Level Agreements for outsourced security processes.

ISM3 describes five basic ISM system configurations, equivalent to maturity levels, and these are used to help organizations choose the scale of ISM system most appropriate to their needs. The maturity spectrum relates cost, risk and threat reduction and enables incremental improvement, benchmarking and long term targets.

ISM3 systems and products are accreditable through the ISM3 Consortium, and it is the intention of the ISM3 Consortium to strengthen linkages and compatibility with existing ISO standards, so that existing investment in ISM systems is protected as ISM systems are improved.

In summary, ISM3 aims to:

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

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.

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 organization 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. Some information security terminology has different meaning in different standards and methods. To reduce ambiguity, the information security terminology used in this document is defined in the Terms and Definitions section, and the similarity or difference in use with other standards is stated when possible.

ISM3 is designed with all kinds of organization in mind. In particular, businesses, non-governmental organizations 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, (CMMI, Cobit, ISM3, ISO9001, ISO20000, ITIL/ITSM);
- Controls oriented (BSI-ITBPM, ISO27001, ISO13335-4);
- Product oriented (Common Criteria / ISO15408);
- Risk management oriented (AS/NZS 4360, CRAMM, EBIOS, ISO 27005, MAGERIT, MEHARI, OCTAVE, SP800-30, SOMAP);
- Best practice oriented (ISO/IEC 27002, ISF-SoGP).

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 organization'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 are appropriate to achieve the process objectives and outputs.

3 Concepts – Processes and Metrics

3.1 Processes

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, their frequency or which events would trigger them. Some processes are triggered by specific events, while others are periodic or continuous.

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.
- Inputs to the process;
- Outputs 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 organization under different process owners or in different logical environments.

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 (like goods, energy or even money) or services and these may be produced automatically or not.

The structure of the process definition template is as follows (next page):

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. **(List of processes that generate this input)** Inputs in *italics* are obtained from sources other than documents.
Outputs	Results of the process. **(List of processes that use this output)** Outputs in *italics* are Outputs other than documents. **Note I**: Metrics Reports should normally be available to the CIO, CEO, CSO, and a representative of the Users.
Activity	Metric description of the volume of Outputs produced.
Scope	Metric description showing how much of the organization or the environment is covered by the process.
Update	Metric description of the frequency of update of the process 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.
Responsibilities	An example of a process owner is given in this row. Every process should have one and no more than one process owner. The supervisor of the process will normally be a process owner of a higher level process; operational processes are supervised by tactical managers, tactical processes are supervised by strategic managers and strategic managers are supervised by the Board. The auditor of the process will normally be an internal or external auditor, or a quality assurance specialist. Auditor and the supervisor role, the process owner role, or performing any other process related duties are incompatible. Auditor independence should be safeguarded, for example by rotation. **Note II**: Some practitioners may find useful the RACI model for responsibilities distribution from Cobit
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.

Note III: The process code is just an identifier. ISM3 Process Model presents gaps and out of numeric order processes because of deprecated or renamed processes.
Note IV: Processes mentioned in the text can be found using the Process Index.

3.1 Metrics

A Metric is a quantitative measurement that can be interpreted in the context of a series of previous or equivalent measurements. In ISM3, metrics are used to:

- Determine whether security objectives are met;
- Show how security objectives contribute to business objectives;
- Measure how changes in a process improve the ISM system;
- Detect significant anomalies;
- 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.

It is optional to add Accuracy and Precision to the Metric Definitions, as these are important when small differences in the value of the metric will trigger very different management decisions. Estimating accuracy and precision might be resource consuming, as it is necessary to have a baseline measurement system with a known high accuracy and precision to compare with.

Measurements from different sources and different periods need to be normalized before integration in a single metric.

3.3 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 the process 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 Outputs 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 Outputs and related information systems.
- Availability: The time since a process has performed as expected upon demand (uptime), the frequency and duration of interruptions, and the time interval between 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 Outputs produced in comparison to the theoretical maximum. Measuring efficacy of a process implies the comparison against a baseline.
- Load: Ratio of available resources in actual use, like CPU load, repositories capacity, bandwidth, licenses and overtime hours per employee.

3.4 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. Metrics are best interpreted using Shewhart-Deming control charts, with a threshold estimation between 2 and 3 standard deviations (sigma). (Values within the arithmetic mean plus/minus twice or thrice 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 malfunctions and make business decisions based 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.	Institute immediate and/or 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.

The process that uses Metrics in high maturity levels to manage ISM3 process is TSP-4 Service Level Management.

3.5 Formal Management Practices

Management systems normally evolve to fit the purposes of the organization they serve. Several management practices contribute to this evolution:

- Implementation. Practice performed when no pre-existing management system or management process. This practice uses information from an assessment of the organization's goals and informal management practices in place to design an appropriate management system or process. As GP-3 ISM Design and Evolution is the process used to implement other processes, it is used to underpin management systems.
- Operation. Practice routinely performed that normally implies in addition to execution
    - Testing. Checking whether we get the expected outputs from invented or selected inputs purposefully fed into the process. This is performed using TSP-4 Service Level Management.
    - Monitoring. Checking whether the outputs of the process and the resources used are within normal ranges. This is performed using TSP-4 Service Level Management with metrics.
    - Improving. Making changes in the process to make it better fit the purpose, or to lead to a saving in resources. This management practice needs information gained from testing, monitoring or diagnosing the process. The gains from the changes (if any) can be diagnosed with subsequent testing, monitoring or auditing. GP-3 ISM Design and Evolution is the process used to improve other processes.
- Evaluation. Practice performed periodically or as required.
    - Assessment. Checking whether the existing process matches the organization's needs and compliance goals, or if it performs better and with better use of resources than it used to. This practice is performed using GP-3 ISM Design and Evolution.
    - Audit. Checking whether the process inputs, activities and results match their documentation. This practice is performed using GP-2 ISM System and Business Audit.
    - Certify. Checking whether process documentation, inputs, outputs and activities comply with a pre-defined standard, law or regulation. The certificate is a proof of compliance that third parties can trust. This practice is performed using GP-2 ISM System and Business Audit.

  Evaluating the current state of the organization will normally imply making a model of the organization. As organizations evolve, and modelling can be time and resource consuming, the model's scope and depth are normally tuned for the task at hand.

4 Concepts - Security in Context Model

4.1 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 classified as an incident at one organization may not be classified as an incident at another. For example, an organization, or a logical environment that handles no confidential information may not classify the viewing of its files by an unauthorized party as an incident.

4.2 Business Objectives

Every organization exists for a certain purpose, not always fully formalized. There are also likely to be formal business objectives, such as growing revenue, providing a service, and paying bills on time. Generally speaking, organizations have the following business goals:

- Achieving a vision and mission;
- Continuing to exist;
- Maintaining and growing revenue;
- Attracting, maintaining and fostering talent;
- Maintaining and growing brand and reputation;
- Complying with internal ethics and social responsibility goals;
- Complying with regulations and contracts;

A key feature of the ISM3 approach is linkage of business objectives with security objectives. The achievement of the business objectives depend on several factors, such quality issues, the skills and commitment of staff, competition and other market conditions. Business objectives depend increasingly on information security as well. Business 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;
- Invoicing all products and services provided;
- Delivering the products and services when and where committed by the organization;
- Keeping all necessary records to pass any audit successfully (i.e., tax audit, software license audit, etc.)
- Preventing breach of contractual agreements;
- Protecting intellectual property and legal rights;

Achieving business objectives consistently is both a quality and a security issue. Quality will help meeting or surpassing customer's expectations, while Security will keep Quality consistent in time despite errors, accidents and attacks.

Examples of Business Objective and related Security Targets:

Business Objectives	Sample Business Security Targets
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 incidents per year. • Loss is less than 0.1% of the accounting value of the company.
On-line booking Availability	• Fewer than five incidents every year where availability is reduced in one hour or more between 8 and 17h or simultaneous users are reduced to 50 or less. • Loss is less than 0.1% of the accounting value of the company.
On-line booking Reliability	• Fewer than two incidents where interruption are more than 2 or add up to more than 15 minutes any working day. • Loss is less than 0.1% of the accounting value of the company.
On-line booking Volatility	• Fewer than two incidents a month where more than 5 minutes of transactions are lost because of a service interruption • Loss is less than 0.1% of the accounting value of the company.
Tax Information Retention	• Fewer than one incident every year where more than 1% of data with a 5 years retention requirement is lost. • Loss is less than 0.1% of the accounting value of the company.
Old customers information Expiry	• Fewer than two incidents every year where more than 1% of expired data is not irrecoverably deleted. • Loss is less than 0.1% of the accounting value of the company.
Installed lines Completeness	• Fewer than four incidents every year where number of installed lines in the invoicing database drops below 98% any working day. • Loss is less than 0.1% of the accounting value of the company.

Business Objectives	Sample Business Security Targets
Customer addresses Precision	• Fewer than two incidents every year where more than 0,5% of customer addresses are wrong or outdated any working day. • Loss is less than 0.1% of the accounting value of the company.

4.2.1 Incidents and success of ISM systems

ISM3 uses business objectives and security targets as the criteria to determine if there has been an incident and to determine if an ISM system is successful or otherwise. When a business objective is not met, an incident has occurred. Security targets are the defined thresholds of metrics associated to specific business and security objectives. When a security target is not met, the ISM system has failed.

Security targets are defined normally as the number and cost of incidents due to failure to achieve business objectives. Security targets can be thought as a way to specify the Risk Appetite of an organization.

Determining the 'cost' of an incident should include both:

- 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 contract, statutory or regulatory legal obligations;
  - Breach of ethical codes of conduct;
  - Breach of social and moral obligations;
  - Breach of professional, regulatory or statutory responsibilities.

The threshold value set for each security target depends on the logical environment (as defined in 10.3). 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 organization.

4.2.2 Personnel Responsibilities

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

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

Division of duty rules for transparency, partitioning, supervision, rotation and separation of responsibilities prevent conflict of interest, collusion to commit fraud and impunity from committing fraud:

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

- Strategic ISM reports should be available to stakeholders and their representatives, 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.

Partitioning
All instances of ISM processes should have one and only one Process Owner. All process owners should be employees of the organization. An owner may contract out some activities related to the process, but ownership should always be held in-house. The process owner may delegate a process, but still bears responsibility for the competency and due diligence with which it is performed.

Supervision
All ISM processes should have at least one supervisor.
Stakeholder representatives 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.

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.

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.

An appropriate distribution of responsibilities, provision of resources and the use of ISM3 Processes TSP-7 to TSP-11 help to improve personnel performance.

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); Roles normally involve: to perform, to supervise, to audit, or being informed about tasks.
- Organizational chart: diagram of the responsibilities for supervision between roles;
- Border: defines the limits of the organization.

The following roles have special importance in ISM3:

- Customer: as in the ITIL definition a customer is the role 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 organization, 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 organization, 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 organizational 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 Customer).

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.

As a guideline, the following related roles should be kept separate:

Incompatibility	ISM3 Level
Process Owner and Stakeholder Representative	1 and above
Process auditor & Process Owner (PO)	1 and above
Incident victim & Forensics investigator	1 and above
Incident whistle-blower & Forensics investigator	1 and above
GP-2 & any other PO	1 and above
Strategic PO & Operational PO (this incompatibility guarantees supervision)	2 and above
Authorizer & System Administrator	2 and above
OSP-19 & any other PO	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 whistle-blower & Patching management PO	3 and above
System Administrator & User	3 and above
OSP-20 & any other PO	3 and above
Repository backup operator & Tape librarian	4 and above
Logs administrator & Logs keeper	4 and above
OSP-21, OSP-25 & any other PO	4 and above

4.3 Security Objectives

ISM3 requires an organization 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 is called an incident and will normally threaten the achievement of a business objective.

Security objectives and security targets should balance business, compliance and technical needs and limitations, like cost, functionality, privacy, liability and risk. The expression of security objectives using Information Assurance Markup Language v1.0 is recommended (see: 9 References)

The following goals, objectives, needs and limitations...	...depend total or partially on...
Business Goals	**Business Objectives**
Business Objectives	**Market Conditions,** **Competition,** **Seasonal changes,** **Costs,** **Pricing,** **Workforce skill and commitment,** **Innovation...** **Quality Objectives** **Security Objectives**
Security Objectives	**Compliance Needs and Limitations** **Technical Needs and Limitations** **Business Needs and Limitations**
Compliance Needs and Limitations	Process OSP-21 Information Quality and Compliance Probing (among others)
Technical Needs and Limitations	Process OSP-5 Environment Patching Process OSP-7 Environment Hardening Process OSP-16 Segmentation and Filtering Management Process OSP-17 Malware Protection Management (among others)
Business Needs and Limitations	**Access Control Objectives** **Priority Objectives** **Durability Objectives** **Information Quality Objectives**
Access Control Objectives	Process OSP-3 Inventory Management Process OSP-11 Access control Process OSP-12 User Registration Process OSP-14 Physical Environment Protection Management (among others)
Priority Objectives	Process OSP-26 Enhanced Reliability and Availability Management Process OSP-15 Operations Continuity Management (among others)
Durability Objectives	Process OSP-6 Environment Clearing Process OSP-10 Backup Management Process OSP-27 Archiving Management (among others)
Information Quality Objectives	Process OSP-21 Information Quality and Compliance Probing (among others)

4.3.1 Businesses Needs and Limitations

While these may be substantially similar, security objectives may vary between environments, geographic locations or business units depending on local context, specific protection requirements, cost structures and use of technology. Similarly, different organizations in the same sector are likely to have different security objectives. As a result, there must be a statement of security objectives for each logical environment of the organization.

The following is a list of generic or implicit security objectives that will be common to many organizations. The security objectives are expressed using the Terms and Definitions.

a) Use of services and physical and logical access to repositories and systems is restricted to authorized users;
    i. Intellectual property (licensed, copyrighted, patented and trademarks) is accessible to authorized users only;
    ii. Personal information of clients and employees is accessible for a valid purpose to authorized users only, preserves their anonymity if necessary, and is held for no longer than required;
    iii. Secrets (industrial, trade) are accessible to authorized users only;
    iv. Third party services and repositories are appropriately licensed and accessible only to authorized users;
a) Users are accountable for the repositories and messages they create or modify;
b) Users are accountable for their acceptance of contracts and agreements.
c) Users are accountable for their use of services.
d) Accurate time and date is reflected in all records;
e) Availability of repositories, services and channels exceeds Customer needs;
f) Reliability and performance of services and channels exceeds Customer needs;
g) Volatility of services and channels within Customer needs;
h) Repositories are retained at least as long as Customer requirements;
i) Expired or end of life-cycle repositories are permanently destroyed;
j) Precision, relevance (up-to-date), completeness and consistency of repositories exceeds Customer needs;

Business Objectives are achieved using a variety of techniques and security management processes. **Security Objectives** “a” to “e” are achieved using access control techniques. The Access Control paradigm represents users in information systems using user accounts or certificates and implements digital equivalents to guarded doors, records and signatures. (**Note V**: While user accounts sometimes represent services or information systems instead of people, the term user will be used alone for simplicity) For Access Control to be effective, some processes need to be implemented in a as robust and non tamperable manner as possible:

l) The User Registration Process links user accounts and certificates to identifiable users, and manages the lifecycle of user accounts, certificates and access rights. When protecting the anonymity of users is more important than making them accountable, registration must guarantee that user accounts and certificates **are not** linked to identifiable users.
m) The Authentication Process links the use of user accounts with their owner and manages the lifecycle of sessions.
n) The Authorization Process grants the use of services and interfaces and access to repositories to authorized users and denies it to unauthorised users.

o) The Signing Process records the will and intent about a repository of the owner of the user account or certificate concerning a repository, such as agreeing, witnessing or claiming authorship of repositories and messages like original works, votes, contracts and agreements. Digital signatures are a special kind of record.
p) The Recording Process registers accurately the results of the registration, authentication, authorization, use of systems and signing processes, so these can be investigated and will and intent or responsibilities determined, within the limits set by Anonymity business objectives. The recording process will normally have to meet business objectives for accurate recording, including date and time. Depending on the security objectives of Anonymity, the recording process normally registers;
    - Interface ID and Location;
    - User account or certificate ID;
    - Signature;
    - Type of Access Attempt (login, logout, change password, change configuration, connect/disconnect systems, repositories I/O interfaces, enabling/disabling admin access or logging, etc)
    - Date and Time of Access attempt;
    - Access attempt result;
    - Repository, Interface, Service or Message accessed.

Depending on the identity of the information system owner and the audience (set of authorized users) of the information, the User Registration and the Authorization processes are normally simplified using secrecy, privacy, intellectual property, and licensing categories. As managing several categories is difficult and costly, the number of categories should be kept to a minimum. Classification must lead to distinctive treatment of the graded objects. If two objects are treated equally in all situations, they belong to the same categories.

During the lifecyle of information, it can change from one secrecy, privacy, intellectual property or licensing category to another. Secret information is not secret forever and trademarked and licensed information is so for the period of contract, or can even have upper limits set by law, for example.

Access Control Objectives

These security targets are rates of accidents, errors and attacks and the cost of those incidents in the user registration, authentication, authorization, signing and recording processes:

Access Control Security Objectives	Sample Access Control Security Targets
Personal information preserves the anonymity of the information subjects if necessary, for example not linking user accounts or certificates to an identifiable user;	• Fewer than 15 incidents per year • Loss is less than 0.1% of the accounting value of the company.
Links the use of user accounts with their owners;	• Fewer than 20 incidents per year • Loss is less than 0.1% of the accounting value of the company.
Granting the use of services and interfaces and access to repositories to authorized users.	• Fewer than 25 incidents per year • Loss is less than 0.1% of the accounting value of the company.
Denying the use of services and interfaces and access to repositories to unauthorized users.	• Fewer than 10 incidents per year • Loss is less than 0.1% of the accounting value of the company.
Express the will and intent about a repository of the owner of a user account or certificate.	• Fewer than 20 incidents per year • Loss is less than 0.1% of the accounting value of the company.

Access Control Security Objectives	Sample Access Control Security Targets
Inaccurate recording, of: • Interface ID and Location; • User account or certificate ID; • Signature; • Type of Access Attempt • Date and Time of Access attempt; • Access attempt result; • Repository, Interface, Service or Message accessed.	• Fewer than 10 incidents per year • 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 20 incidents per year • Loss is less than 0.1% of the accounting value of the company.
Secrets are accessible to authorized users only	• Fewer than 3 incidents per year • 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 5 incidents per year • Loss is less than 0.1% of the accounting value of the company.
Information systems are physically accessible only to authorized users	• Fewer than 5 incidents per year • Loss is less than 0.1% of the accounting value of the company.
Repositories are accessed by authorised users only	• Fewer than 10 incidents per year • Loss is less than 0.1% of the accounting value of the company.

Priority Security Objectives

Security Objectives “f” to “h” are normally achieved using backup and enhanced reliability techniques. Protected services, interfaces and channels can be classified according to security objectives for priority. In a multi-tiered information system, the priority of higher level services is propagated to the lower level services they depend on.

Priority Security Objectives	Sample Priority Security Targets
Availability: the period of time when a service, repository, interface or channel must exist, be accessible and usable (perform according to customer needs) upon demand according to or exceeding customer needs.	• 9 hours a day every working day between 0800 and 1700 hours for ten years serving 100 simultaneous users.
Reliability: the longest time and the number of times in the availability (performance) time a service, repository, interface or channel can be interrupted according to or exceeding customer needs.	• 2 times for a total time of 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 according to or exceeding customer needs.	• 1000 transactions lost per interruption. • 5 minutes of information and transactions per interruption.

Durability Security Objectives

Security Objectives "i" and "j" are normally achieved using archival and clearing techniques. 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.

Retention of repositories implies either keeping available the systems used to access them or copying the data to newer repositories and format that are accessible by available systems.

Durability Security Objectives	Sample Durability Security Targets
Retention period: the minimum length of time a repository is kept (preserved) according to or exceeding customer and regulatory requirements	• 5 years since creation.
Expiry: the date the expired or end of life-cycle repositories and records should be permanently and reliably destroyed according to or exceeding customer and regulatory requirements. Those with personal information of customers and employees often require a specific expiry date.	• 10 years since end of use.

Information Quality Security Objectives

Security Objective "k" is normally achieved using quality control techniques. The information quality of a repository is a measure of how fit the repository is to fulfil security objectives. Two factors are relevant:

Information Quality Security Objectives	Sample Information Quality Security Targets
Completeness: The extent to which a repository is populated (available and consistent) with the information required to meet or exceed customer needs. The lower limit is usually set by business or customer needs, and the upper limit by regulatory needs	• 98% of lines installed are in the invoicing database.
Precision: The maximum rate of erroneous and outdated information in the information available according to or exceeding customer and regulatory needs. Customers require especially high levels of accuracy in some types of records. **Note VI**: When random data is used, its accuracy is related to how fit is the data to the statistical distribution needed.	• 0.5% incorrect or out-of-date customer addresses.

4.3.2 Compliance Needs and Limitations

There are voluntary security objectives, security targets and obligations set by the business and other set by laws or regulations (which are normally mandatory) and certifications sought by the organization on contractual, ethical and fair use grounds, for example:

q) Third party services and repositories need to be appropriately licensed.
r) Personal information completeness must be proportional to its use.
s) Personal information can't be kept for longer than needed.
t) Tax records must be kept for a minimum number of years.
u) Personal information must be protected using certain security measures depending on the type of personal information.
v) The owner of Personal information must agree for it to be collected and he has the right to check it, fix it and approve how it will be used or ceded.
w) Repositories with Personal information have to be registered with a Data Protection agency.
x) Encryption must be used under legal limitations.
y) Secrets must be kept according to the terms of agreed Non Disclosure Agreements.
z) The owner of Personal information will be given notice when his data is being collected, including who is collecting the data.
aa) Personal information must be used for the purpose agreed with the information owner..
ab) Personal information must not be disclosed without the agreement of the information owner..
ac) Personal information owners will have means to make data collectors accountable for their use of his personal information.

The same techniques used to control information quality can be used to control compliance, but business related and compliance related security objectives don't necessarily match.

Examples of Compliance related Security Objectives and related Security Targets:

Compliance Security Objectives	Sample Compliance Security Targets
Third party services and repositories need to be appropriately licensed.	• Fewer than ten incidents every year where an improperly licensed service or repository is used.. • Loss is less than 0.1% of the accounting value of the company.
Personal information completeness must be proportional to its use.	• Fewer than two incidents every year where more any personal datum is collected without a business case for it. • Loss is less than 0.1% of the accounting value of the company.
Personal information is held for no longer than required	• Fewer than two incidents every year where more than 0,1% of personal records are retained beyond their expiry date. • Loss is less than 0.1% of the accounting value of the company.
Tax records must be kept for a minimum number of years.	• Fewer than two incidents every year where more than 0,1% of tax records are lost. • Loss is less than 0.1% of the accounting value of the company.
Personal information must be protected using certain security measures.	• Fewer than five incidents every year where mandatory security measures are found to be missing. • Loss is less than 0.1% of the accounting value of the company.

Compliance Security Objectives	Sample Compliance Security Targets
The owner of Personal information must agree for it to be collected, and he has the right to check it and fix it and approve how it will be used of ceded.	• Fewer than ten incidents every year where a personal record is not handled accordingly. • Loss is less than 0.1% of the accounting value of the company.
Repositories with Personal information have to be registered with a Data Protection agency.	• Fewer than one incident every two years where a Repository is not registered. • Loss is less than 0.1% of the accounting value of the company. •

Industrial and trade secrets, licensing and protection of intellectual property (copyrights, patents and trademarks) have special compliance protection needs. There are some compliance rules as well that restrict the specified function of the ISM system. Security objectives and targets must reflect these restrictions.

Privacy, the right to keep right to secrecy, to be unknown to others what we do not know, or we do, which forbids third, whether private or public authorities decide what are the boundaries of our private life, setting aside an area sheltered from the curiosity of others, whatever the content of that space, is especially protected by specific laws in many countries.

4.3.3 Technical Needs and Limitations

Technical needs are related to weaknesses and requirements of using information systems based on the Von-Neumann architecture. Most weaknesses in modern systems are related to the following facts:

- A byte can be either data, an address or a machine instruction. This is exploited, for example by buffer overflow attacks;
- User systems consider by default that all code sitting in their repositories, or even remotely is legitimate. This is exploited by malware;
- Mobile repositories are essentially passive and can be read without any access control from any system;
- Once a repository is written, the information remains for long after it stopped being used.

These needs are not directly linked to businesses objectives, but are a fact of life of the use of information systems. Information systems need electricity and certain temperature and humidity conditions to work properly. New weaknesses are discovered all the time, and patches are released fix those weaknesses. For these reasons there are security objectives related to keeping information systems as free as possible of visible weaknesses to potential attackers, and within proper environmental conditions:

ad) Systems are as free of weaknesses as possible.
ae) Systems are visible to trusted systems only.
af) Systems that need to be visible to not trusted systems are the least visible possible.
ag) Systems run trusted services only.
ah) The electricity, temperature and humidity where systems operate exceeds the systems needs.

Examples of Technical related Security Objectives and related Security Targets:

Technical Security Objectives	Sample Technical Security Targets
Systems are as free of weaknesses as possible.	• Average update level in the production environment of 1 week.
Systems that need to be visible to not trusted systems are the less visible possible.	• Less than 10 unused ports discovered during penetration testing per year.
Systems run trusted services only.	• The medium update level of anti virus is below 1 day.
The electricity, temperature and humidity where systems operate exceeds the systems needs.	• Electricity reliability is over 99,9999% • Temperature doesn't exceed 25 degrees more than 5 minutes a day. • Humidity is over 80% for less than 10 minutes a day.

5 Requirements - Certification

5.1 Maturity and Capability Levels

Two types of maturity are considered; coverage and capability.

Capability maturity levels are:

- **Undefined**. The process might be used, but it is not defined.
- **Defined**. The process is documented and used.
- **Managed**. The process is Defined and the results of the process are used to fix and improve the process.
- **Controlled**. The process is Managed and milestones and need of resources is accurately predicted.
- **Optimized**. The process is Controlled and improvement leads to a saving in resources

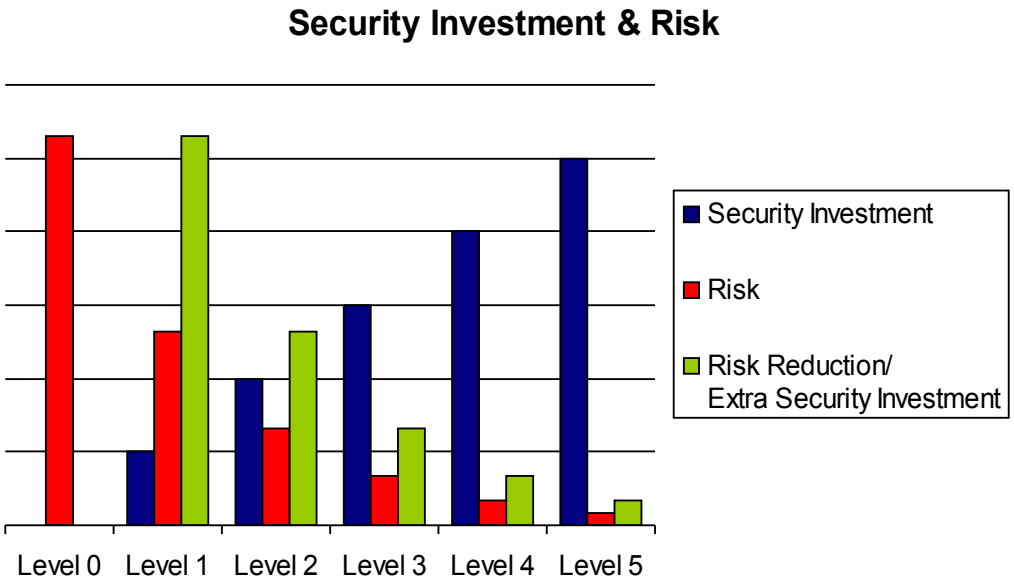
For a process to pass a ISO9001-style audit, it must reach the "Managed" level. Capability is a property of how a process is managed, not a property of the process itself. The capability achieved by every organization will depend on:

- The distribution of responsibilities.
- The motivation, skills, accountability and empowerment of the personnel.
- The resources available.

Continuous improvement toward higher capability levels can be reached implementing the process TSP-4 Service Level Management and using metrics.

While capability levels beyond Managed are not accreditable as it would be misleading to suggest that any past success forecasting the need of resources, or optimizing their use will be repeated in the future, GP-2 ISM System and Business Audit can research the current capability of processes.

Processes are allocated to coverage 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. Normally, higher capability of the implemented processes will render a higher return of investment. Note that return of investment increase is not linear with the investment increase and that an excessive investment in security, beyond the the risk cost, can give a negative return.



(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.

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

An organization may choose to implement any of the defined processes at any stage of maturity. However, this should be related to specific security objectives. While it is possible to choose not to implement some required processes, for accreditation purposes it is not possible to leave out any of the required processes of the chosen maturity level.

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. Process metrics are not compulsory for this level.

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. Process metrics are not compulsory for this level.

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 organizations dependent on information services and e-commerce. Process metrics are not compulsory for this level.

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 organizations, such as stock exchange listed corporations, government bodies and financial institutions. Process metrics are not compulsory for this level.

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.

5.1.1 Levels Tables

These tables specify the minimum capability level per process required to achieve every maturity level.

General

	Level 1	Level 2	Level 3	Level 4	Level 5
GP-1 Document Management	Managed	Managed	Managed	Managed	Managed w/ Metrics
GP-2 ISM System and Business Audit	Managed	Managed	Managed	Managed	Managed w/ Metrics
GP-3 ISM Design and Evolution	Managed	Managed	Managed	Managed	Managed w/ Metrics

Strategic Management

	Level 1	Level 2	Level 3	Level 4	Level 5
SSP-1 Report to Stakeholders	Managed	Managed	Managed	Managed	Managed w/ Metrics
SSP-2 Coordination	Managed	Managed	Managed	Managed	Managed w/ Metrics
SSP-3 Strategic vision	Managed	Managed	Managed	Managed	Managed w/ Metrics
SSP-4 Define TPSRSR rules				Managed	Managed w/ Metrics
SSP-6 Allocate resources for information security	Managed	Managed	Managed	Managed	Managed w/ Metrics

Tactical Management

	Level 1	Level 2	Level 3	Level 4	Level 5
TSP-1 Report to strategic management	Managed	Managed	Managed	Managed	Managed w/ Metrics
TSP-2 Manage allocated resources	Managed	Managed	Managed	Managed	Managed w/ Metrics
TSP-3 Define Security Targets	Managed	Managed	Managed	Managed	Managed w/ Metrics
TSP-4 Service Level Management			Managed	Managed	Managed w/ Metrics
TSP-6 Define environments and life-cycles		Managed	Managed	Managed	Managed w/ Metrics
TSP-13 Insurance Management				Managed	Managed w/ Metrics
TSP-7 Background Checks				Managed	Managed w/ Metrics
TSP-8 Personnel Security				Managed	Managed w/ Metrics
TSP-9 Security Personnel Training			Managed	Managed	Managed w/ Metrics
TSP-10 Disciplinary Process		Managed	Managed	Managed	Managed w/ Metrics
TSP-11 Security Awareness		Managed	Managed	Managed	Managed w/ Metrics

Operational Management

	Level 1	Level 2	Level 3	Level 4	Level 5
OSP-1 Report to tactical management	Managed	Managed	Managed	Managed	Managed w/ Metrics
OSP-2 Security Procurement		Managed	Managed	Managed	Managed w/ Metrics
OSP-3 Inventory Management			Managed	Managed	Managed w/ Metrics
OSP-4 Information Systems Environment Change Control		Managed	Managed	Managed	Managed w/ Metrics
OSP-5 Environment Patching	Managed	Managed	Managed	Managed	Managed w/ Metrics
OSP-6 Environment Clearing		Managed	Managed	Managed	Managed w/ Metrics
OSP-7 Environment Hardening		Managed	Managed	Managed	Managed w/ Metrics
OSP-8 Software Development Life-cycle Control			Managed	Managed	Managed w/ Metrics
OSP-9 Security Measures Change Control		Managed	Managed	Managed	Managed w/ Metrics
OSP-16 Segmentation and Filtering Management	Managed	Managed	Managed	Managed	Managed w/ Metrics
OSP-17 Malware Protection Management	Managed	Managed	Managed	Managed	Managed w/ Metrics
OSP-11 Access control		Managed	Managed	Managed	Managed w/ Metrics
OSP-12 User Registration		Managed	Managed	Managed	Managed w/ Metrics
OSP-14 Physical Environment Protection Management		Managed	Managed	Managed	Managed w/ Metrics
OSP-10 Backup Management	Managed	Managed	Managed	Managed	Managed w/ Metrics
OSP-26 Enhanced Reliability and Availability Management				Managed	Managed w/ Metrics
OSP-15 Operations Continuity Management			Managed	Managed	Managed w/ Metrics
OSP-27 Archiving Management				Managed	Managed w/ Metrics
OSP-19 Internal Technical Audit		Managed	Managed	Managed	Managed w/ Metrics
OSP-20 Incident Emulation			Managed	Managed	Managed w/ Metrics
OSP-21 Information Quality and Compliance Probing				Managed	Managed w/ Metrics
OSP-22 Alerts Monitoring		Managed	Managed	Managed	Managed w/ Metrics
OSP-23 Events Detection and Analysis				Managed	Managed w/ Metrics
OSP-24 Handling of incidents and near-incidents			Managed	Managed	Managed w/ Metrics
OSP-25 Forensics				Managed	Managed w/ Metrics

5.2 ISM3 Certification

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.

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

- As a way to evidence the organization'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 Outputs obtained from an security outsourcing provider.

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[2]
ISO27001 certification	No	No	No	Yes	Yes[2]

(2): 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 the ISM3 Consortium.

5.2.1 Scope of Accreditation

To achieve certification of an ISM3 system all processes for the certified level must be implemented, at least in the environments that hold the critical information of the business. As a rule of thumb, if the organization can survive any two weeks of a year without the environment, the environment is considered not critical.

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

5.2.2 Accreditable 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.

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 organization and information systems from these kinds of threat.

6 Information Security Management Process Model

6.1 Introduction

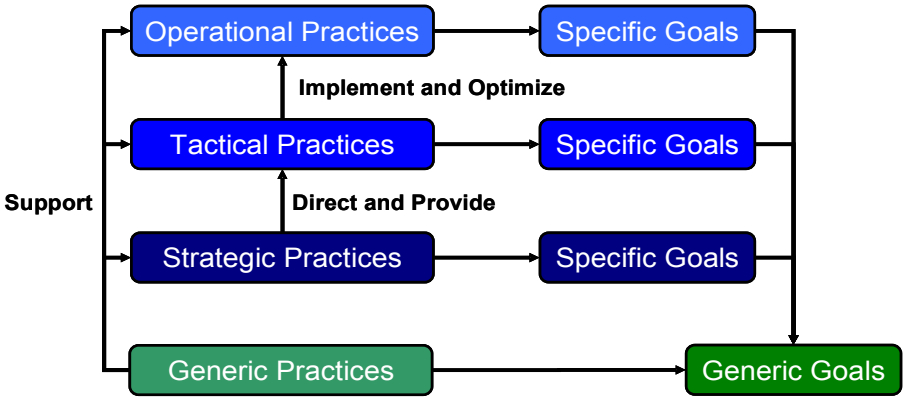
Security is the result of a process. The better the security process, the better the protection achieved from the resources available.

Using Security in Context, an incident is defined as a failure to meet the organization's business or 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 organization 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.

The Operational level reports to the Tactical level, which in turn reports to the Strategic level, which in turn reports to the organization's stakeholders.

6.2 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.

The Outputs 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 Business and Security Objectives should result.

6.3 Generic Practices

6.3.1 Document Management

Generic Practice	**GP-1 Document management**
Description	This process underpins the ISM System by defining document quality standards, organization and distribution of the documents and records associated with specific processes and contributes to keeping them up-to-date through the requirement for document expiry and review.
Rationale	Security processes are implemented in a robust and repeatable way 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
Outputs	List of Reviewed documents List of Approved new and updated documents List of Distributed and Retired document versions (including version number and date) Metrics Report (TSP-4) **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. **Templates and Forms:** General layout and format of type of document.

Generic Practice	GP-1 Document management
Outputs (continued)	**Plans:** Documents to define the scope of a process, the resources necessary to establish and perform it and how to set it up. **Policies**: Documents to specify requirements, priorities and rules for the process: • GP-024-Information Security Policy, which must include Information Security Objectives; • GP-017-Lifecycle Control Policy; • GP-018-Access and Environmental Control Policy (including Third Party Code of Connection Agreement); • GP-019- Availability Management Policy; • GP-022-Testing and Auditing Policy; • GP-01B-Monitoring Policy; • GP-01A-Incident Handling Policy; • GP-01D-Personnel Management Policy. • GP-01E-Acceptable Use 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. **Reports:** Documents that reflect a summary and interpretation of the results of a process.
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.
Responsibilities	Process Owner: The individual who has responsibility for creating or updating the document.
Related Processes	All ISM3 processes.
Related Methodologies	ISO9001:2000

6.3.2 ISM System Audit

Generic Practice	GP-2 ISM System and Business Audit
Description	This process validates: • If the process documentation, inputs, outputs and activities complies with standards, laws, regulations and internal policies; • If the existing scheme of delegation follows TPSRSR rules; • If the processes inputs, activities and results match their documentation; It can be applied to test all processes compliance and capability or a representative sample. The auditor should plan, document and carry out the audit to minimise the chance of reaching an incorrect conclusion, following relevant Professional Guidelines.
Rationale	Incidents arising from faults in the ISM system can be prevented by checking the system and taking action to address areas of improvement, for example: • Compliance of business processes with applicable regulations. • Scheme of delegation following TPSRSR rules. • Implementation of ISM system as defined.
Documentation	GP-021-Audit Policy (Criteria, Scope, Rules) GP-022-Audit Procedure (Method)
Inputs	GP-024-Information Security Policy SSP-041-TPSRSR Policy ISM documentation of the audited process Outputs of every audited process Results of previous audits
Outputs	Audit Report TPSRSR Rules Report Metrics Report (TSP-4)
Activity	Number of ISM Audit Reports submitted
Scope	Percentage of ISM processes that have been audited at least once Percentage of business processes that have been audited at least once
Update	Time since last Audit Report submission Mean time between Audit Report submissions Mean time between ISM process audits Mean time between business process audits
Availability	Not Applicable
Responsibilities	Supervisor: CEO Process Owner: Internal or external Auditor. The Audit Report must be communicated to the process owner of the audited process.
Related Processes	All ISM3 processes.
Related Methodologies	ISACA IS Auditing Standards ISACA IS Control Professionals Standards

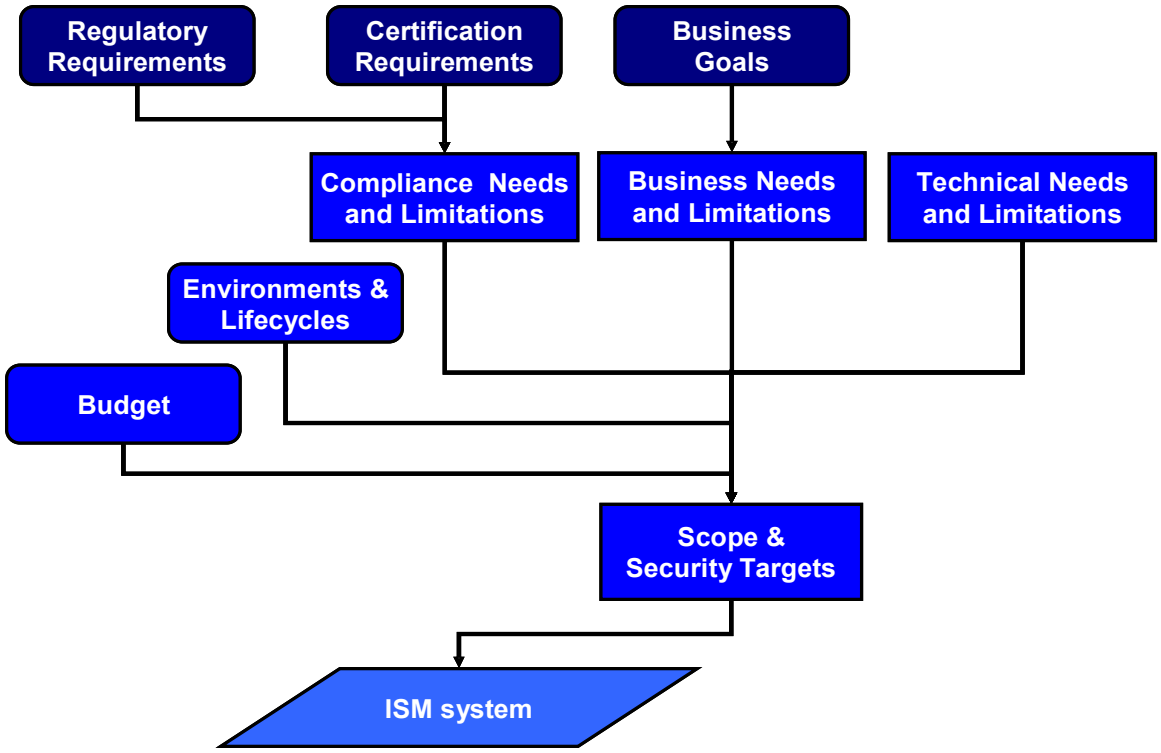
6.3.3 Establishing and improving the ISMS

The following steps should be taken for initial 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 (e.g. Basel II, USA SoX, Spain LOPD);
- Determine additional certification requirements (e.g. ISO27001, SAS70);
- Assessment of the current ISM system / ISM3 based ISM system.
- Set up GP-1 Document Management (it can be based on current ISO9001 infrastructure);
- Determine implementation strategy;
- Set up Strategic Management processes;
    - Determine the Business, Personnel and Compliance security objectives based on regulatory, certification and business goals.
    - Determine the information security budget;
- Set up selected Tactical Management processes, including GP-3 ISM Design and Evolution;
    - Determine the Access Control, Priority, Durability, Information Quality and Technical related security objectives;
    - Determine the logical environments and life-cycles;
    - If accreditation is sought, determine ISMS scope of accreditation and boundaries, with rationale for inclusion and exclusion;
    - Classify repositories and services according to security objectives, name system owners;
    - Set the security targets per environment;
    - Choose a process selection method, like e.g. risk assessment;
    - Select appropriate operational processes per environment;
- Determine metrics for each process;
- Set up or outsource operational ISM processes;
- Assign responsibilities;
- Design and document (using GP-1 Document Management) the ISM3-based ISM system.
    - Agreements, including SLAs for outsourced processes;
    - Policies;
    - Procedures;
    - Templates;
    - Reports.
- Create and publish Information Security Policies using SSP-3 Strategic vision;
- Train Management and Users on their ISMS responsibilities using TSP-9 Security Personnel Training;
- Review operation of all processes using TSP-4 Service Level Management;
- Revise security targets using TSP-3 Define Security Targets;
- Operate the ISM system;
- Define and refine the process metrics thresholds using TSP-4 Service Level Management;
- Audit the ISM system periodically using GP-2 ISM System and Business Audit;
- Optionally, certificate the ISM system;
- Maintain and improve the ISM system using GP-3 ISM Design and Evolution;

GP-3 ISM Design and Evolution and GP-1 Document Management are the main processes necessary to “boot” a ISM3 ISM.

ISM Design can be summarized as follows:



Generic Practice	GP-3 ISM Design and Evolution
Description	This process selects the most appropriate operational processes to achieve the Security Targets. There are a variety of techniques for ISM assessment, amongst them: • ISM3 Maturity Level choice; • ROSI Evaluation; • Threat Evaluation; • Vulnerability Evaluation • Business Impact Evaluation. • Risk Evaluation (Threat, Vulnerability and Impact Evaluation). This process validates whether the existing process matches or not the organization's needs and compliance goals or if it performs better and with better use of resources than it used to. Modelling the organization is helpful for doing Risk, Threat, Vulnerability and Business Impact Evaluation. Depending on the scope and depth of the evaluation, models of the following types are useful: • Information system Model; • Financial model • Logistic Model (Transport, Supplies, Waste); • Infrastructure Model (Energy, Space, Environmental conditions); • Personnel and Responsibilities Model; • Organizational Reputation Model; These techniques should add value producing reproducible results in a cost-effective way. The smallest units considered by a ISM3 focused Risk Evaluation are business objectives, security objectives and environments.

Generic Practice	GP-3 ISM Design and Evolution
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. Processes efficiency and effectiveness can degrade in time unless there is a continuous effort in the organization towards higher levels of capability.
Documentation	GP-030-Internal and External Threats and Vulnerabilities to Business and Security Objectives per Environment Template GP-031-Recommended Investment in Existing and New ISM Processes per Environment Template GP-032-ISM Design and Evolution Methodology GP-01G-Risk Management Policy
Inputs	GP-017-Lifecycle Control Policy GP-024-Information Security Policy Information Security Targets (TSP-3) Information Security Budget (SSP-6) Inventory of Assets (OSP-3) Incident Reports (OSP-24) Intrusions Reports (OSP-24) Forensics Reports (OSP-25) Backup Test Report (OSP-10) Enhanced Reliability and Availability Test Report (OSP-26) Operations Continuity Test Report (OSP-15)
Outputs	Internal and External Threats and Vulnerabilities to Business and Security Objectives per Environment Acceptable Internal and External Threats and Vulnerabilities to Business and Security Objectives per Environment Threats to Insure Report (TSP-13) Recommended Investment in Existing and New ISM Processes per Environment (SSP-6) Information Security Management Processes Definition (including priorities and investments needed) Security Processes Policies: • GP-017-Lifecycle Control Policy; • GP-018-Access and Environmental Control Policy; • GP-019- Availability Management Policy; • GP-01C-Testing and Auditing Policy • GP-01B-Monitoring Policy • GP-01A-Incident Handling Policy; • GP-01D-Personnel Management Policy. Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of Threats in environments, security objectives and business objectives identified Number of Vulnerabilities in environments, security objectives and business objectives determined Number of Business Impacts determined
Scope	Percentage of Environments examined Percentage of Business Objectives examined Percentage of Security Objectives examined
Update	Time since last Outputs submission

Generic Practice	GP-3 ISM Design and Evolution
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. Process Owner: Chief Information Officer
Related Processes	SSP-6 Allocate resources for information security TSP-3 Define Security Targets. TSP-13 Insurance Management OSP-3 Inventory Management OSP-24 Handling of incidents and near-incidents OSP-25 Forensics OSP-20 Incident Emulation OSP-19 Internal Technical Audit
Related Methodologies	ISO 544R Business Impact Assessment; Risk Assessment, Threat Assessment, Vulnerability Assessment: AS/NZS 4360, CRAMM, EBIOS, ISO 27005, MAGERIT, MEHARI, OCTAVE, SP800-30

6.4 Specific Practice: Strategic Management

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

6.4.1 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 organizations, such partners, vendors and contractors.
- Provides resources for information security;
- Defines Security Objectives consistent with business goals and objectives, protecting stakeholders interests;
- Sets the organizational scheme of delegation.

6.4.2 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 (OSP-1) Tactical Information Security Report (TSP-1) Metrics Reports (From the rest of Strategic Processes)
Outputs	Strategic Information Security Report (For the stakeholders) Metrics Report (For the stakeholders)
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
Responsibilities	Supervisor: stakeholder representatives. Process Owner: Chief Executive and Chief Information Officer
Related Processes	TSP-1 Report to strategic management.
Related Methodologies	Not Applicable

6.4.3 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*
Outputs	Meeting Minutes Metrics Report (SSP-1) *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
Responsibilities	Supervisor: stakeholder representatives. Process Owner: Chief Executive
Related Processes	Not Applicable
Related Methodologies	Not Applicable

6.4.4 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	GP-024-Information Security Policy Template
Inputs	*Organizational objectives and strategy*
Outputs	GP-024-Information Security Policy Metrics Report (SSP-1)
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
Responsibilities	Supervisor: stakeholder representatives. Process Owner: Chief Executive
Related Processes	SSP-4 Define Division of Duties rules. TSP-3 Define Security Targets. GP-3 ISM Design and Evolution.
Related Methodologies	Not Applicable

6.4.5 Scheme of Delegation

Process	SSP-4 Define Division of Duties rules
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 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.
Inputs	*Organizational objectives and strategy*
Outputs	SSP-041-TPSRSR Policy Metrics Report (SSP-1)
Activity	Not Applicable
Scope	Not Applicable
Update	Time since last TPSRSR Policy (reviewed) submission Mean time between TPSRSR Policy (reviewed) submissions
Availability	Not Applicable
Responsibilities	Supervisor: stakeholder representatives. Process Owner: Chief Executive and Business Unit Managers
Related Processes	GP-2 ISM System and Business Audit
Related Methodologies	Not Applicable

6.4.6 Provision of Resources

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	Recommended Investment in Existing and New ISM Processes per Environment (GP-3) Incident Valuation Report (TSP-4) ISM Performance and Return on Investment Report (TSP-4)
Outputs	*Resources allocated to Information Security Management* Information Security Budget (TSP-2, GP-3, OSP-2) Metrics Report (SSP-1)
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
Responsibilities	Supervisor: stakeholder representatives. Process Owner: Chief Executive and Business Unit Managers
Related Processes	All ISM3 processes.
Related Methodologies	Not Applicable

6.5 Specific Practice: Tactical Management

Strategic Management is the Customer 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.

6.5.1 Specific Goals

Tactical Management has the following purposes:

- Provide feedback to Strategic Management;
- Define the environment for Operational Management:
  - Define Security Targets;
  - Define metrics;
  - Define information Business, Personnel, Compliance, Access Control, Priority, Durability, Information Quality and Technical related security objectives;
  - Define environments and lifecycles;
  - Select appropriate processes to achieve the Security Targets;
- Manage budget, people and other resources allocated to information security.

6.5.2 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	Operational Information Security Report (OSP-1) Metrics Reports (From all Tactical Processes) ISM Performance and Return on Investment Report (TSP-4)
Outputs	Tactical Information Security Report (SSP-1)
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
Responsibilities	Supervisor: SSP-3 Process Owner. Process Owner: Chief Information Officer or Information Security Tactical Manager
Related Processes	OSP-1 Report to tactical management
Related Methodologies	Not Applicable

6.5.3 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 (SSP-6) Information Security Resources Request (From Tactical and Operational Processes)
Outputs	Information Security Resources Assignment (To Tactical and Operational Processes) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of ISM processes that have resources assigned
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. Process Owner: Information Security Tactical Manager
Related Processes	SSP-6 Allocate resources for information security
Related Methodologies	Not Applicable

6.5.4 Security Targets and Assets Classification

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. Business, Compliance, Personnel, Access Control, Priority, Durability, Information Quality and Technical related requirements are taken into account.
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-032-Information Requirements and Classification Template GP-01E-Acceptable Use Policy Template TSP-034-Third Party Code of Connection Agreement Policy Template GP-017-Lifecycle Control Policy
Inputs	GP-024-Information Security Policy (SSP-3)
Outputs	Information Security Targets (TSP-4, GP-3, OSP-2, OSP-8, OSP-9, OSP-20) Information Requirements and Classification (Documentation) Acceptable Use Policy (TSP-10, TSP-11) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Not Applicable
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. Process Owner: Chief Information Officer
Related Processes	SSP-3 Strategic vision
Related Methodologies	Not Applicable

6.5.5 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	GP-017-Lifecycle Control Policy (Documentation) *Working environments in the organization* *States and Events that mark state transition in every environment*
Outputs	TSP-061-Environments and Lifecycles Definition (Documentation) Metrics Report (TSP-4) **Note VII***: UML state diagrams are recommended for lifecycle documentation.*
Activity	Number of Outputs submitted
Scope	Percentage of systems that belong to a defined Environment
Update	Time since last Outputs submission
Availability	Not Applicable
Process owner	Chief Information Officer
Related Processes	OSP4-7 Information Systems Lifecycle Management
Related Methodologies	ISO15228

6.5.6 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. Monitors metric measurements and requests action on observation of abnormal metric measurements. Feeds inputs for testing purposes to other processes and requests action if they fail to produce the expected outputs. Suggests fixes and improvement of the processes. Suggests improvement in the use of resources of the processes. Evaluates the 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 (TSP-3) Physical Presence Logs (OSP-14) Environmental Conditions Logs (OSP-14) Security Awareness Report (TSP-4) Log of denied and granted Access Requests (OSP-12) Unauthorized Access Attempts Report (OSP-11) Malware Protection Deployment and Update Level Report (OSP-17) Filter Rules Report (TSP-4) Intrusion Report (OSP-24) Forensic Report (OSP-25) Metrics Reports (From all Operational Processes)
Outputs	*Remediation of errors and faults in the processes* Process Metrics Definition (For every Operational Process) Incident Valuation Report (SSP-6) ISM Performance and Return on Investment Report (TSP-1, SSP-6) Metrics Report (TSP-1)
Activity	Number of Outputs submitted
Scope	Percentage of processes with fully defined and monitored process metrics
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. 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	Six Sigma DMAIC process

6.5.7 Insurance Management

Process	TSP-13 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	GP-01G-Risk Management Policy
Inputs	Threats to Insure Report (GP-3) Inventory of Assets (OSP-3)
Outputs	*Threats Insured* Insurance Contracts (OSP-15) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of information systems covered by insurance Number of incidents mitigated by insurance
Scope	Percentage of information systems covered by insurance
Update	Time since last Outputs submission
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. Process Owner: Information Security Management
Related Processes	GP-3 ISM Design and Evolution
Related Methodologies	Not Applicable

6.5.8 Personnel Security

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 (from Human Resources) Human Resources Policies (from Human Resources)
Outputs	Background Check Report (for Human Resources) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of selection processes where background check was performed
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. Process Owner: Human Resources.
Related Processes	TSP-8 Personnel Security
Related Methodologies	Not Applicable

Process	TSP-8 Personnel Security
Description	This process aims to assure the commitment, competency, knowledge and experience of employees while their liaison with the organization lasts through evidence-based assessment. This process is closely linked with OSP12 so that changes in personnel role or status are promptly reflected by access rights
Rationale	Personnel trusted to carry out security processes must be competent, accountable and empowered. Evidence in the form of responses to Skills-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 (from Human Resources) Contracts of Employment (from Human Resources) Human Resources Policies (from Human Resources) Personnel/professional development schemes (from Human Resources)
Outputs	Selection of Security Personnel Report (to Human Resources) Non Disclosure Agreements (to Human Resources) Metrics Report (TSP-4) Personnel Status Changes (OSP-12 User Registration)
Activity	Number of Outputs submitted
Scope	Turnover of security staff Turnover of staff
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. 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 Skills 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 (from Human Resources)
Outputs	Training on Security Report (to Human Resources) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of security personnel trained
Scope	Percentage of security personnel who have received training
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. 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 (OSP-24) Contracts of Employment (from Human Resources) GP-01E-Acceptable Use Policy (TSP-3)
Outputs	Disciplinary Report (to Human Resources) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of incidents leading to disciplinary process
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. 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 organization is required to prevent and mitigate security incidents.
Documentation	TSP-111-Security Awareness Report Template TSP-112-Staff Training Manual
Inputs	GP-024-Information Security Policy GP-01E-Acceptable Use Policy (TSP-3)
Outputs	Security Awareness Report (TSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of non-security personnel trained
Scope	Percentage of non-security personnel who have received training
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: SSP-3 Process Owner. Process Owner: Human Resources.
Related Processes	Not Applicable
Related Methodologies	Not Applicable

6.6 Specific Practice: Operational Management

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

6.6.1 Specific Goals

Operational Management has the following responsibilities:

- Provide feedback to Tactical Management, including Incident and Metrics 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).

6.6.2 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 (*The same TSP-4 has*)
Outputs	Operational Information Security Report (TSP-1, TSP-4)
Activity	Number of Outputs submitted
Scope	Not Applicable
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner 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

6.6.3 Tool Selection

Process	OSP-2 Security Procurement
Description	Selection of the specific products, providers and outsourcing providers 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, providers and outsourcing services.
Documentation	OSP-021- Procurement Recommendations Report Template
Inputs	Published Comparatives (Publications) Selection Criteria Best Practices (Updates, Metrics, Learning curve, etc) Information Security Targets (TSP-3) Information Security Budget (SSP-6)
Outputs	Procurement Recommendations Report (GP-3) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Not Applicable
Update	Time since last Outputs submission
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Operational Manager.
Related Processes	GP-3 ISM Design and Evolution
Related Methodologies	ISO15408 - Common Criteria

6.6.4 Lifecyle Control

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-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. • The authorized audience of important removable repositories keeping an inventory of copies and who owns them. • The licensing of installed and uninstalled software. • The licensing of copyrighted information in use. 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 for example the Information Assurance Markup Language.
Documentation	OSP-031-Inventory Procedure OSP-032-Asset Naming Policy OSP-033-Asset Labeling Procedure TSP-032-Information Requirements and Classification
Inputs	*Known Hardware* *Known Software* *Other Known Information Repositories* Clearing Report (OSP-6)
Outputs	Inventory of Assets (Multiple Processes) *Classified Repositories and Messages* *Prioritised Interfaces, Services and Channels* *Durability and Quality grouped Repositories* Metrics Report (TSP-4)
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 Outputs submission Mean time between Outputs 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
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management
Related Processes	TSP-3 Define Security Targets OSP-4 Information Systems Environment Change Control
Related Methodologies	Not Applicable

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	OSP-041-Environments and Lifecycles Definition OSP-042-Lifecycle Control Policy
Inputs	Alerts, Fixes and Threats Report (OSP-22) Attack Emulation Report (OSP-19) Services Update Level Report (OSP-5) Clearing Report (OSP-6) Hardening Report (OSP-7) Information Completeness, Precision, Update and Fair-Use Report (OSP-21)
Outputs	*Compliant interfaces in every environment.* *Compliant channels in every environment.* *Compliant services in every environment.* *Compliant repositories in every environment.* Metrics Report (TSP-4)
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
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management
Related Processes	TSP-6 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, enhancing the Reliability of the updated systems.
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 (OSP-3)
Outputs	*Up to date services in every environment.* Services Update Level Report (OSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of patching updates in information systems
Scope	Percentage of information systems covered by the process
Update	Time since last Outputs submission Mean time between Outputs 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
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management
Related Processes	OSP-4 Information Systems Environment Change Control OSP-9 Security Measures Change Control
Related Methodologies	Not Applicable

Process	OSP-6 Environment Clearing
Description	This process covers procedures for clearing whole repositories or previous versions information or changed parts of repositories to prevent disclosure of information. Clearing might affect licensed software and copyrighted information.
Rationale	Clearing or destroying of repositories is required to prevent disclosure incidents when an information system or repository is changed leaving previous versions information behind, or when it 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 (OSP-3)
Outputs	*Cleared Repositories* Clearing Report (OSP-4, OSP-3) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of information systems susceptible to be cleared when changing state in the environment
Update	Time since last Outputs submission Mean time between Outputs submissions Time since last information system clearing Time since last repository clearing
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management
Related Processes	OSP-4 Information Systems Environment Change Control OSP-9 Security Measures Change Control OSP-3 Inventory Management OSP-27 Archiving Management
Related Methodologies	Not Applicable

Process	OSP-7 Environment Hardening
Description	This process improves the configuration of channels, services, interfaces and repositories at borders, enhancing their Reliability 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 (OSP-3)
Outputs	*Hardened services, interfaces, repositories and channels* Hardening Report (OSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of information systems susceptible to be hardened when changing state
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management
Related Processes	OSP-4 Information Systems Environment Change Control OSP-9 Security Measures Change Control
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 Security Objectives and 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 OSP-194-Source Code Review Procedure OSP-195-Source Code Review Report Template
Inputs	Information Security Targets (TSP-3) Alerts, Fixes and Threats Report (OSP-22) Source Code Review Report (OSP-19)
Outputs	*Certified and Working Software.* Information Security Requirements Test Report (For the development team) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of Information systems under development tested for compliance
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management
Related Processes	OSP-22 Alerts Monitoring
Related Methodologies	SSE-CMM OWASP SPSMM ISO12207

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	TSP-061-Environments and Lifecycles Definition GP-017-Lifecycle Control Policy OSP-091-Security Measures Change Control Procedures OSP-092-Security Measures Change Control Report Template
Inputs	Information Security Targets (TSP-3) Alerts, Fixes and Threats Report (OSP-22)
Outputs	*Compliant Security Measures in every environment.* Security Measures Change Control Report (TSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs 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 Outputs submission Mean time between Outputs submissions
Availability	No Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management
Related Processes	TSP-6 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-16 Segmentation and Filtering Management
Description	This process defines technical policies for the passage of authorized messages and electromagnetic waves between zones, while denying passage to unauthorized messages and EM waves. Messages and EM waves can be filtered at any abstraction level, ranging from level-7 firewalls to spam filtering, Instant Messaging filtering, TCP/IP traffic filtering, VoIP filtering, electromagnetic pulse filtering etc. Third party connections involve at least one of the organization's zones and an external zone. An alternative to flatly denying access is using a quarantined environment with limited access.
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-162-Internal Zones Filtering Procedure OSP-163-Border Filtering Procedure OSP-164-Filter Authorizations Report Template GP-018-Access and Environmental Control Policy (including Third Party Code of Connection Agreement)
Inputs	Environments & Lifecycles Definition Inventory of Assets (OSP-3) Incident Detection Report (OSP-23) Intrusion Detection Report (OSP-23)
Outputs	*Prevention of unauthorized passage of messages between environments* Filter Rules Report (TSP-4) Logs of Drops (OSP-23) Logs of Pass (OSP-23) Metrics Report (TSP-4)
Activity	Number of Outputs 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 Outputs submission Mean time between Outputs 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
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management
Related Processes	OSP-2 Security Procurement OSP-23 Events Detection and Analysis OSP-3 Inventory Management OSP-12 User Registration
Related Methodologies	Not Applicable

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, rootkits and other unauthorised services. An alternative to cleaning or deleting the unauthorised service is to put it in a quarantined sandbox.
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 GP-017-Lifecycle Control Policy
Inputs	Inventory of Assets (OSP-3) Incident Detection Report (OSP-23)
Outputs	*Protection of information systems from Malware* Malware Detection and Cleaning Report (OSP-23) Malware Protection Deployment and Update Level Report (TSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of malware items Cleaned Number of malware items Cleaning Errors
Scope	Percentage of information systems covered by malware protection
Update	Time since last Outputs submission Mean time between Outputs 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 VIII**: 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
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management
Related Processes	OSP-2 Security Procurement OSP-23 Events Detection and Analysis OSP-3 Inventory Management
Related Methodologies	Not Applicable

6.6.5 Access and Environmental Control

Note IX: Code Obfuscation, Watermarking, Digital Rights Management, Licensing controls and related techniques are a form of Access Control, but these techniques are not a part of the ISMS as they control the use of intellectual property in third party information systems.

Process	**OSP-11 Access control**
Description	Access control is the means by which access to classified information is provided to and by authorized users, while denied to unauthorized ones. Access Control includes Authentication of users or services, Authorization of users or services, Signing of repositories and Recording of access and use of services, repositories, channels and interfaces. • Authentication links the use of user accounts with their owners and manages the lifecycle of sessions. • Authorization grants the use of services and interfaces and access to repositories to authorized users and denies it to unauthorised users. An alternative to denying access is providing limited (quarantined) access rights instead. • Signing records the will and intent about a repository of the owner of the user account or certificate concerning a repository, such as agreeing, witnessing or claiming authorship of repositories and messages like original works, votes, contracts and agreements.. • Recording registers accurately the results of the user registration, authentication, authorization, use of systems and signing processes, so these can be investigated and will and intent or responsibilities determined, within the limits set by Anonymity business objectives.
Rationale	To make users accountable for their use of services, interfaces and access to repositories, it is necessary to link the use of user accounts with their owner, grant or deny access to to services, interfaces and repositories in real time, and record it. Incidents like espionage, unlawful use of Personal 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 GP-018-Access and Environmental Control Policy
Inputs	Inventory of Assets (OSP-3) Inventory of Premises (From Facilities) User Registration and Access Control Review Report (OSP-19)
Outputs	*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 (TSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs 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

Process	OSP-11 Access control
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 Outputs submission Mean time between Outputs 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
Availability	Percentage of time the access control systems are available
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management
Related Processes	OSP-2 Security Procurement OSP-3 Inventory Management OSP-12 User Registration
Related Methodologies	RBAC ISO 15489: 2001

Process	OSP-12 User Registration
Description	This process covers enrolment that can link user accounts and certificates to their identifiable or anonymous owners and manages the lifecycle of certificates and user accounts, and the granting, denial and revocation of access rights. An alternative to denying access rights is providing limited (quarantined) access rights instead. When protecting the anonymity of users is more important than making them accountable, registration must guarantee that user accounts **are not** linked to identifiable users. The rights requested can be related to: • Access, use or connection 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, User, Authorizer, and Authority. This process is closely linked with TSP8, so that access rights are promptly updated when personnel change role or status.
Rationale	To make users accountable for their use of services, interfaces and access to repositories, it is necessary to link user accounts to identifiable users. Incidents arising from the inappropriate grant of access or concession of user accounts can be prevented and mitigated by user registration procedures.
Documentation	TSP-032-Information Requirements and Classification GP-018-Access and Environmental Control Policy OSP-122-Access Requests Procedure OSP-123-Access Request Template
Inputs	Inventory of Assets (OSP-3) Access Request (From users) Personnel List of Leavers (From Human Resources) User Registration and Access Control Review Report (OSP-19) Personnel Status Changes (TSP-8)
Outputs	*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 (TSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs 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 Outputs submission Mean time between Outputs 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
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management
Related Processes	OSP-2 Security Procurement OSP-3 Inventory Management OSP-14 Physical Environment Protection Management OSP-16 Segmentation and Filtering Management
Related Methodologies	Not Applicable

Process	OSP-14 Physical Environment Protection Management
Description	This process covers guarantee access and control of access into secure areas containing important repositories or interfaces, and alternate facilities. It also covers protection of critical infrastructure from fire, extreme temperatures, extreme humidity flood, electromagnetic anomalies and other physical threats. An alternative to flatly denying access is using a quarantined area with limited access.
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	GP-018-Access and Environmental Control Policy OSP-142-Physical Access Procedure OSP-143-Environmental Control Procedure TSP-032-Information Requirements and Classification
Inputs	Inventory of Assets (OSP-3)
Outputs	*Prevention of environmental incidents* *Prevention of unauthorized passage of assets between environments* Physical Presence Logs (TSP-4) Environmental Conditions Logs (TSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs 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 Outputs submission Mean time between Outputs 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
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Facilities Manager
Related Processes	OSP-2 Security Procurement OSP-23 Events Detection and Analysis OSP-3 Inventory Management OSP-12 User Registration OSP-15 Operations Continuity Management
Related Methodologies	Not Applicable

6.6.6 Availability Control

Availability Management is the collective name for the Availability, Reliability, Volatility, Retention Period and Expiry security objectives and targets related processes.

Process	**OSP-26 Enhanced Reliability and Availability Management**
Description	This is a set of redundancy, diversity and dispersion based security measures to reduce the impact of equipment loss and failure, achieving service level requirements for a short mean time to information systems recovery, checkpoint date and time. **Note X**: Real time detection and quick remediation of partial failures are essential to keep MTTR within Security Targets.
Rationale	Incidents arising from the loss of repositories and disruption to channels, interfaces and services can be mitigated by elimination of single points of failure and built-in resilience to total or partial failures.
Documentation	OSP-264-Reliability and Availability Test Plan OSP-265-Reliability and Availability Test Report Template GP-019- Availability Management Policy TSP-032-Information Requirements and Classification
Inputs	Inventory of Assets (OSP-3) Incident Detection Report (OSP-23) Enhanced Reliability and Availability Test Report (OSP-20)
Outputs	*Prevention of permanent information loss from repositories* *Prevention of interruption of channels, interfaces and services* Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of system failures mitigated by high reliability systems
Scope	Percentage of protected information systems in the environment Percentage of single points of failure (services, interfaces and channels) in protected information systems Percentage of in protected information systems free of single points of failure Percentage of points of failure in protected information systems that lose current transactions when failing Percentage of redundant points of failure in protected information systems currently operating without redundancy.
Update	Time since last Outputs submission Mean time between Outputs submissions Time since last partial failure – MFOP
Availability	Percentage of time the enhanced reliability and availability systems are available Meant Time between partial failures (MTBF) Annualized Failure Rate (AFR) Meant Time to Recovery (per protected information system) (MTTR) Best case time from Recovery Point per protected information system of failure tested Worst case time from Recovery Point per protected information system of failure tested
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management or Information Security Management
Related Processes	OSP-2 Security Procurement OSP-3 Inventory Management OSP-20 Incident Emulation OSP-23 Events Detection and Analysis
Related Methodologies	Not Applicable

Process	OSP-10 Backup Management
Description	This process reduces the impact of information loss, achieving service level requirements for time to information systems recovery, Recovery Point date and time and Recovery Time. Keeping several Recovery Points increases de chances of finding a known good state of the information or information system being backed up. Additional information and changes like files deleted or moved not present in Recovery Points might be salvaged using Data Recovery techniques. Some backup systems require that no changes are made on the repository being backed up during back up. In these systems, a conflict might arise between the required availability of the repository and the duration of the backup. Recovering a system normally requires backing up file's meta data, permissions, file system layout and settings.
Rationale	Incidents arising from the loss of repositories can be mitigated by backup processes.
Documentation	OSP-101-Backup and Restore Test Plan OSP-102-Backup Report Template OSP-103-Restore Report Template GP-019- Availability Management Policy TSP-032-Information Requirements and Classification
Inputs	Inventory of Assets (OSP-3) Incident Detection Report (OSP-23) Backup Test Report (OSP-20)
Outputs	*Prevention of permanent information loss from repositories* Backup Report (OSP-15) Restore Report (OSP-15) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of repositories covered by backup. Percentage of the non-availability windows of the repository used for backup. Best case Number of Recovery Points Best case time from Recovery Point Worst case time from Recovery Point Best case Time to Recovery Worst case Time to Recovery
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Percentage of time the backup and restore systems are available Time to partial restore of backups tested Time to full restore of backups tested
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management or Information Security Management
Related Processes	OSP-2 Security Procurement OSP-3 Inventory Management OSP-20 Incident Emulation
Related Methodologies	Not Applicable

Process	OSP-15 Operations Continuity Management
Description	This process uses redundancy (like redundant systems and communications, spare parts), dispersion (like alternate facilities and off-site backup storage) to reduce the impact of incidents that threaten the existence of the organization, achieving regulatory and business requirements for mean time to business processes recovery, checkpoint date and time and degree of redundancy.
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 GP-019- Availability Management Policy TSP-032-Information Requirements and Classification
Inputs	Inventory of Assets (OSP-3) Insurance Contracts (TSP-13) Incident Detection Report (OSP-23) Backup Report (OSP-10) Restore Report (OSP-10) Backup Test Report (OSP-20) Archival Restore Report (OSP-27) Archival Restore Report (OSP-27) Enhanced Reliability and Availability Test Report (OSP-20) Operations Continuity Test Report (OSP-20)
Outputs	*Protection of the existence of the organization* Metrics Report (TSP-4)
Activity	Number of Outputs 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 off-site 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 Best case time from Recovery Point Worst case time from Recovery Point Best case Time to Recovery Worst case Time to Recovery Number of off-site Recovery Points
Update	Time since last Outputs submission Mean time between Outputs 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
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management

Process	OSP-15 Operations Continuity Management
Related Processes	OSP-2 Security Procurement OSP-3 Inventory Management OSP-20 Incident Emulation OSP-23 Events Detection and Analysis
Related Methodologies	PAS 56 Guide to Business Continuity Management BS25999

Process	OSP-27 Archiving Management
Description	This is a set of security measures to achieve requirements of expiry date and long periods of retention. Strategies to guarantee information retrievablility include copying information from old media and formats to current ones or keeping obsolete systems in working order and monitoring storing media quality.
Rationale	Incidents arising from the loss of repositories before their defined retention period or keeping them beyond their expiry date can be mitigated storing, cataloguing and monitoring retrievability periodically.
Documentation	OSP-271-Archival and Archival Restore Test Plan OSP-272-Archival Report Template OSP-273-Archival Restore Report Template GP-019- Availability Management Policy TSP-032-Information Requirements and Classification
Inputs	Inventory of Assets (OSP-3)
Outputs	*Prevention of permanent information loss from repositories* Archival Storage Report (OSP-15) Archival Restore Report (OSP-15) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of repositories with defined retention periods covered by archival
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Percentage of time the archival systems are available Percentage of physical repositories older that end-of-life Percentage of physical repositories replaced
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management, or Information Security Management
Related Processes	OSP-3 Inventory Management This process relies on OSP-6 Environment Clearing for deletion of expired information.
Related Methodologies	Not Applicable

6.6.7 Testing and Auditing

Process	OSP-19 Internal Technical Audit
Description	This process validates: • The effectiveness of vulnerability reduction measures. • The effectiveness of access control measures. • The effectiveness of user registration measures. • The quality of the software developed in-house. It can be applied to all possible targets or a representative random sample. When performing emulated attacks from internal systems, it is commonly called internal "vulnerability" testing. When performing emulated attacks from external systems, is commonly known as penetration testing.
Rationale	Incidents arising from the exploitation of weaknesses in software and configuration weaknesses around the borders of an organization can be prevented by attacks emulation and subsequent software mending, environment hardening, investment and improved monitoring.
Documentation	OSP-192-Attacks Emulation Procedure OSP-193-Attack Emulation Report Template OSP-194-Source Code Review Procedure OSP-195-Source Code Review Report Template OSP-196-User Registration and Access Control Review Procedure OSP-197- User Registration and Access Control Review Report Template GP-01C-Testing and Auditing Policy
Inputs	Inventory of Assets (OSP-3).
Outputs	Attack Emulation Report (OSP-4) Source Code Review Report (OSP-8) User Registration and Access Control Review Report (OSP12, OSP-11) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of information systems that have been tested in the environment
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management (Tester), or Independent Auditor
Related Processes	OSP-4 Information Systems Environment Change Control OSP-9 Security Measures Change Control OSP-8 Software Development Lifecycle Control OSP-11 Access Control OSP-12 User Registration OSP-14 Physical Environment Protection Management OSP-16 Segmentation and Filtering Management OSP-17 Malware Protection Management
Related Methodologies	OSSTMM OWASP

Process	OSP-20 Incident Emulation
Description	This process validates the effectiveness of OSP-10 Backup Management, OSP-26 Enhanced Reliability and Availability Management, OSP-15 Operations Continuity Management, 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.
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-101-Backup and Restore Test Plan OSP-103-Restore Report Template OSP-152-Operations Continuity Test Plan OSP-153-Operations Continuity Test Report Template OSP-264-Reliability and Availability Test Plan OSP-265-Reliability and Availability Test Report Template OSP-201-Incident Emulation Procedure OSP-204-Incident Emulation Test Report GP-01C-Testing and Auditing Policy
Inputs	Information Security Targets (TSP-3)
Outputs	Backup Test Report (OSP-10, OSP-15) Enhanced Reliability and Availability Test Report (OSP-26, OSP-15) Operations Continuity Test Report (GP-3, OSP-15) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of incident emulations performed
Scope	Percentage of information systems tested under incident emulation.
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management (Tester), or Information Security Management (Tester), or Independent Auditor
Related Processes	OSP-10 Backup Management OSP-26 Enhanced Reliability and Availability Management OSP-15 Operations Continuity Management TSP-13 Insurance Management
Related Methodologies	Not Applicable

Process	OSP-21 Information Quality and Compliance Probing
Description	Periodic review of classified information, held to give assurance that it is complete, accurate, up-to-date and held for a specific purpose according to the law and the company ethics and contracts. For example, records normally have specific accuracy requirements and Personal information must be held only when necessary for 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 incomplete, inaccurate, expired, wrongly labelled or unethically or unlawfully held can be mitigated by an appropriately targeted quality probing process.
Documentation	OSP-211-Information Audit plan OSP-212-Information Completeness, Precision, Update and Fair-Use Report Template GP-01C-Testing and Auditing Policy Fair Data Processing Legislation
Inputs	Inventory of Assets (OSP-3)
Outputs	*Disclosures to public and commercial partners;* Information Completeness, Precision, Update and Fair-Use Report (OSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Percentage of information that belongs to a repository actually in the repository Percentage of records in a repository accurate enough for their business purpose. Percentage of records in a repository updated enough for their business purpose. Percentage of repositories probed for fair use found held for a purpose and compliant with law and ethics.
Scope	Percentage of repositories probed for completeness Percentage of repositories probed for accuracy Percentage of repositories updating probed Percentage of repositories probed for fair use
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Systems Management (Tester), or Independent Auditor
Related Processes	OSP-3 Inventory Management OSP-4 Information Systems Environment Change Control OSP-8 Software Development Lifecycle Control
Related Methodologies	National data and privacy protection legislation, for example: • EU European Directives • USA HIPAA • USA Safe Harbour • USA Privacy Act

6.6.8 Monitoring

Process	OSP-22 Alerts Monitoring
Description	This process checks that Information Security Management is aware of new threats, weaknesses and fixes and is enabled to make informed decisions whether or not to change information system configuration or patch level, or even evolution of the management system. 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. New threats might require changes in the information security management system.
Documentation	OSP-221-Alerts Monitoring Procedure OSP-222-Employee Weakness Reporting Procedure OSP-223-Third Party Weakness Reporting Procedure (Public Document) OSP-224-Alerts, Fixes and Threats Report Template GP-01B-Monitoring Policy
Inputs	Weakness, Fixes and Threats Reports (From External and internal sources) Inventory of Assets (OSP-3)
Outputs	*Reviewed Alerts, Fixes and Weaknesses Reports* Alerts, Fixes and Threats Report (OSP-4) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of alerts and fixes reviewed
Scope	Percentage of systems which alerts and fixes are monitored
Update	Time since last Outputs submission Mean time between Outputs submissions
Availability	Percentage availability of the alerting information sources
Responsibilities	Supervisor: TSP-14 Process Owner: 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

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 like decoys (e.g. honeypots). This information may lead to the detection of incidents, intrusions and partial failures in redundant systems. 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 GP-01A-Incident Handling Policy
Inputs	*Events* Logs of Drops (OSP-16) Logs of Pass (OSP-16) Malware Detection and Cleaning Report (OSP-17) Inventory of Assets (OSP-3)
Outputs	*Incidents and Intrusions Detected* Incident Detection Report (OSP-24, OSP-16, OSP-17, OSP-26, OSP-15, OSP-10) Intrusion Detection Report (OSP-24, OSP-16) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of events detected
Scope	Percentage of events in the environment that are analysed
Update	Time since last Outputs submission Mean time between Outputs submissions Time since last event detected Mean time between events detection
Availability	Availability of event detection systems
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management
Related Processes	OSP-16 , OSP-17, OSP-26 and OSP-10 OSP-24 Handling of incidents and near-incidents
Related Methodologies	Not Applicable

6.6.9 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, **not** including the recovery of repositories and information systems which is responsibility of OSP-10, OSP-15 and OSP-26; • 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-242-Incident Response Procedure OSP-243-Incident Report Template OSP-244-Intrusion Report Template GP-01A-Incident Handling Policy
Inputs	Incident Detection Report (OSP-23) Intrusion Detection Report (OSP-23)
Outputs	*Incidents and near-Incidents Handled* Incident Report (OSP-25, TSP-10) Intrusion Report (OSP-25) Metrics Report (TSP-4)
Activity	Number of Outputs submitted Number of incidents and near-incidents handled Number of intrusions handled Number of Incident Detection Report that are false positives Number of Intrusion Detection Report that are false positives
Scope	Percentage of incidents and near-incidents handled by this process Percentage of intrusions handled by this process
Update	Time since last Outputs submission
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner:Information Security Management
Related Processes	OSP-23 Events Detection and Analysis OSP-25 Forensics
Related Methodologies	ISO18044

Process	OSP-25 Forensics
Description	This process investigates and diagnoses the sequence, authorship, classification, underlying cause 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 GP-01A-Incident Handling Policy
Inputs	Incident Report (OSP-24) Intrusion Report (OSP-24)
Outputs	*Investigated Incidents and Intrusions* Forensic Report (TSP-10, TSP-4, and for legal proceedings) Metrics Report (TSP-4)
Activity	Number of Outputs submitted
Scope	Percentage of incidents analysed
Update	Time since last Outputs submission
Availability	Not Applicable
Responsibilities	Supervisor: TSP-14 Process Owner Process Owner: Information Security Management
Related Processes	OSP-24 Handling of incidents and near-incidents
Related Methodologies	Not Applicable

7 Risk Assessment Method ISM3-RA

ISM3-RA is a method that uses ISM3 concepts to provide a way to make an assessment of risk that is reproducible by different practitioners, useful and cost effective. ISM3-RA outputs can be used as inputs for:

- Gauging how safe the organization is;
- Identifying threats and weaknesses;
- Choosing what processes are appropriate for fulfilling the security objectives;
- Prioritizing investment in security processes.

The scope of an ISM3-RA assessment is the whole business and all the information systems in use. Smaller scopes normally do not lead to significant savings.

Two objects are used: Business Functions and Environments (see 10.3). These objects preserve a depth level that is low enough to represent the features of the organization and the information systems used, while remaining meaningful for management.

Business functions are performed by one or several individuals, teams or even business units depending of the scale of the company. Sixteen business functions are defined, which are common to all kinds of organizations. Some of them are often outsourced, like the legal business function for example:

1. Governance: Definition of the organization's goals, steering of the organization by rules, instruction and challenge rules and instructions.
2. Research. Creation of new knowledge in every area of interest to the organization.
3. Advertising. Promotion of the organization's services and products to potential customers, suppliers and investors.
4. Business Intelligence. Maintenance and delivery of knowledge.
5. Human Resources. Finding, selecting and procuring, promoting and releasing personnel.
6. Information Technology. Finding, filtering and procuring information and communication systems.
7. Legal. Claiming legally binding obligations from third parties and fulfilling the organization's own.
8. Relationships. Creating and maintaining trust, association and familiarity with customers, suppliers, and investors.
9. Administration. Management of paperwork associated with all business functions..
10. Financing / Accounting. Finding, selecting and procuring financial instruments like e.g. money, bonds, etc.
11. Infrastructure. Management of real estate, air conditioning, heating, water supply, energy supply, furniture, food supply, waste , recycling , physical access control, etc
12. Logistics. Delivery of physical products or services.
13. Maintenance. Preventing and repairing faults and the general dilapidation of infrastructure, tools, etc
14. Procurement. Finding, comparing, choosing, selecting and procuring information, tools, supplies, assets and professional services.
15. Production. Production of products and services.
16. Sales: Sale of products or services.

Using these sixteen business functions to model an organization guarantees that a risk assessment is still valid even if the organization undergoes a redistribution of functions among business units.

Every information system belongs to one and only one environment. Many Business functions depend on information systems. A business function can depend on one or several environments differently:

1. No dependency: There are cost effective alternatives to using the information system from that environment and it is not a real time dependency.
2. Partial: There are cost effective alternatives to using the information system from that environment and it is a real time dependency
3. Relative: There are no cost effective alternatives to using the information system from that environment and it is not a real time dependency .
4. Absolute: There are no cost effective alternatives to using the information system from that environment and it is a real time dependency.

The threat taxonomy, which treats environments as a set of information systems, classifies threats depending on the effects of the threat, not the causes. For example interruption of valid service can be caused by someone unplugging a power cable by mistake, the power going out, or a denial of service attack. Seven types of threat significant at a management level are considered:

1. Destruction, Corruption or Loss of valid information or systems
2. Failure to destroy expired information or systems & Failure to stop systems at will
3. Improper use of authorized access to information or systems
4. Improper recording of access to information or systems
5. Unauthorized access, eavesdropping, theft and disclosure of information or systems
6. Underperformance or Interruption of valid system services & Failure of authorized access.
7. Aging of information & Outdated systems

Every threat can be given a probability greater than 0 and smaller than 1 in a given period.

The control taxonomy used is the list of ISM3 processes. Optionally other lists of controls (e.g: ISO27001 controls) can be used as well. Controls can protect one or several environments, to a greater or lesser degree. Some controls can protect against one or several threats.

The more protected an environment is and the less likely a threat is considered, the smaller the risk for that environment.

Where

- *ENVr* = Environment's risk;
- *TP* = Total possible Protection;
- Tp = Threat probability associated to the type of protection;
- *Pp* = Particular Protection of an environment.

Impact is measured scoring the relative importance of each business function and the dependency between each business function and the environments.

Where

- *BFr*: Business Function risk;
- *BFd* = Business Function dependency on environment;
- *ENVrs* = Environment's risk share.

The risk of every environment is then split fairly between all the business functions that depend on that environment. The risk of every business function is the aggregated risk from all the environments it depends on.

Where *BFi* = Business Function impact.

To get a risk figure, numbers have to be assigned to business function importance, dependency between business functions and environments, how protected the environments are, and how likely the threats considered are for each environment. The risk figure is associated with a period of time when all the values used for the calculus are valid.

The total risk is the sum of the risk of all the business functions:

1 Outsourcing

8.1 Service Level Agreements

A Service Level Agreement is a quality agreement between a process provider and a customer specified using a set of metrics. Service level agreements are often used to monitor and improve the quality of service provided by an outsourcing provider. A service level agreement should specify:

Service	A description of the service offered by the outsourcing provider.
Scope	Specific limitations to the service offered, like location, dates and times, lower and higher load limits, language, etc.
Metrics	List of metrics.
Bonuses and Penalties	List of bonuses and penalties to apply for every metric staying or straying from service level objectives.
Escalation Procedures	Procedures to follow in case of service level objectives being missed.
Reporting	Frequency and content of service level reports.
Operation Procedures	Procedures to follow for requests, queries, warnings and incident reports.

For example the following metric can be part of a service level agreement for an outsourced OSP-17 Malware Protection Management process. The SLA should be completed with activity, scope, availability, efficiency, efficacy and load metrics.

Metric	PC antivirus update level
Metric Description	This metrics measures how updated are the computers with Microsoft Windows and corporative antivirus software installed.
Measurement Procedure	The operator uses the query “updatelevel.sql” to extract the current values from the corporative antivirus server AVCORP. (Check Annex XX – Queries.). The query gives as an output the number of PC with every antivirus signature file installed. The counts of all the PC with a signature file older than 3 days are aggregated. The update level is calculated as the number of PC multiplied for how many days old is the signature installed, divided by the total of PC.
Measurement Frequency	Every Monday at 8:00 a.m. local time.
Service Level Objective	Update Level < 2.5 days
Target Value	1 day
Units	0.0 days

TSP-4 Service Level Management uses Service Level Agreements to manage outsourced ISM3 processes.

8.2 Guidelines

The following guidelines about outsourced ISM3 services may be used:

1. The service should be defined in a contract and signed by legal representatives of both parties who shall determine and agree on which country's laws shall govern the contract.
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 notification, if appropriate. Else, the client should be in possession of a registered address of the service provider, the service to which address will satisfy the requirement of legal notification being sufficiently served;
    - Provide the service in the language of the customer;
    - Avoid and declare conflicts of interests;
    - Employ qualified, trained, experienced and committed commercial and technical personnel whom should behave according to all applicable legal requirements and adhere to a formally announced and agreed upon 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 customer 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 customer to audit the service provided and co-operate as required with such auditors as the customer 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.

1. The customer 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 customer)
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.

1. 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.

1. Dependencies between the service provider and third parties, such as software and hardware distributors or producers.

2. Jurisdiction for the resolution of conflicts.

1 References

Paradigms

- Shewhart Cycle or Deming Wheel (Plan, Do, Check, Act)
- Le Moigne Triangle (Strategy, Tactics, Operations)
- People, Process & Technology.
- Keep it Simple, Stupid
- Minimum Privilege
- Need to Know
- Prevention, Detection & Response
- Defence in Depth

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: Towards a Framework for Action" Business Software Alliance, 2003.
- CISWG Report of the Best Practices and Metrics Teams, http://www.educause.edu/ir/library/pdf/CSD3661.pdf
- Federal Information Security Management Act (USA) 2002
- 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"
- OCEG Measurement & Metrics Guide, http://www.oceg.org/view/mmg

Standards

- BSI BS ISO/IEC 27001:2005, http://www.bsi-global.com/
- BSI BS ISO/IEC 27002, http://www.bsi-global.com/
- EA 7/03, http://www.european-accreditation.org
- ELML, http://www.ism3.com
- IETF RFC2119, http://rfc.net/rfc2119.html
- IAML, http://www.ism3.com
- ISACA CObIT , http://www.isaca.org
- ISO 13335, http://www.iso.org/
- ISO 19011:2002, http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=31169
- ISSA GAISP http://all.net/books/standards/GAISP-v30.pdf
- ITSM, ITIL, http://www.itil-itsm-world.com/
- NIST SP800-53, http://csrc.nist.gov/publications/nistpubs/
- NIST SP800-55, http://csrc.nist.gov/publications/nistpubs/
- SEI CMMI, http://www.sei.cmu.edu/cmmi/

Related Methodologies and Certifications

- AEDI CAYSER http://www.aedi.es/cayser/CAYSER.asp
- AICPA Generally Accepted Privacy Principles, http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles/
- AS/NZS 4360, http://www.riskmanagement.com.au/
- Business Process Improvement, http://en.wikipedia.org/w/index.php?title=Business_Process_Improvement&oldid=162199279
- CERT OCTAVE, http://www.cert.org/octave/
- CIS, http://www.cisecurity.org/
- CLUSIF MEHARI http://www.clusif.asso.fr
- CRAMM, http://www.cramm.com/
- EBIOS, http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html
- ISACA CISA, http://www.isaca.org/
- ISACA CISM, http://www.isaca.org
- ISECOM OSSTMM, http://www.isecom.org/
- ISC2 CISSP, http://www.iso.org/
- ISO 544R, http://www.iso.org/
- ISO 9001:2000, http://www.iso.org/
- ISO 12207, http://www.iso.org/
- ISO 15228, http://www.iso.org/
- ISO 15408, http://www.iso.org/
- ISO 18044, http://www.iso.org/
- ISSA GAISP http://all.net/books/standards/GAISP-v30.pdf
- MAP MAGERIT, http://www.csi.map.es/csi/pg5m20.htm
- NIST RBAC, http://csrc.nist.gov/rbac/
- NIST SP800-30, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf#search=%22sp800-30%22
- NSA, http://www.nsa.gov/snac
- Motorola Six Sigma http://www.motorola.com/motorolauniversity.jsp
- OIS SVRRP, http://www.oisafety.org/
- OWASP, http://www.owasp.org/
- SEI P-CMM, http://www.sei.cmu.edu/cmm-p/version2/
- SSE-CMM, http://www.sse-cmm.org/
- Shewhart-Deming control charts, http://en.wikipedia.org/w/index.php?title=Control_chart&oldid=161945932

1 Terms and Definitions

10.1 Processes and Documents Codes

- Processes are coded with the following format: ***XYP***, 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.
- Documents are coded with the following format: **XYP-NNN**, where **XYP** is the process code and **NNN** an integer.
- Words followed by an acronym in brackets [ ], are referenced to an existing publication or standard.
- Outputs in italics are *non-documentary* Outputs.

10.1 Components of Information Systems

Information Systems are complex and have various tangible and intangible components. The components can be classed at the chosen level of abstraction 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 organizations 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;
- *Sessions*. A temporary relationship of trust between services. The establishment of this relationship can require the exchange of Credentials.
- *Messages*. Any meaningful information exchanged between two services or a user and an interface. *Requests* are special messages used by services to change the state of information system components. Requests fall into one of the following categories:

Component State Transition:	Initiate	Finalize	Freeze	Unfreeze	Query State	Change State
Repository	create	delete	block	unblock	read	write
Interface	connect	disconnect	interrupt	continue	read	write
Channel	open	close	hold	release	read	write
Session	login	logout	suspend	resume	read	write
Message	send	listen	retain	forward	read	write
Service	start	stop	pause	go	read	write

Note XI: The request “listen” can be understood as “receive” or “detect”, but for simplicity, only the word “listen” is used.
Note XII: If the repository is RAM-like “block” and “unblock” are equivalent to “allocate” and “free”.

Transactional assets are dynamic, such as running processes, moving messages and live sessions. Static assets such as mail, program files or credentials stored in a repository are not considered either a message or a service. Transactional objects exist in every logical and physical level. The table below contains examples of each type of transactional asset:

Service	Message	Session
Bank Account	Transfer from another account	Work session between user and application
SOAP API Interface	SOAP Call	Session between processes
Port	TCP Packet	TCP Transmission session
Ethernet Port	Ethernet Packet	Frame transmission session

10.3 Lifecycles and Environments

Depending on the mission, size and physical environment of an organization, there may be a number of different logical environments. Systems going through the different states that make up their lifecycle often change the structure of the environment.

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:

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

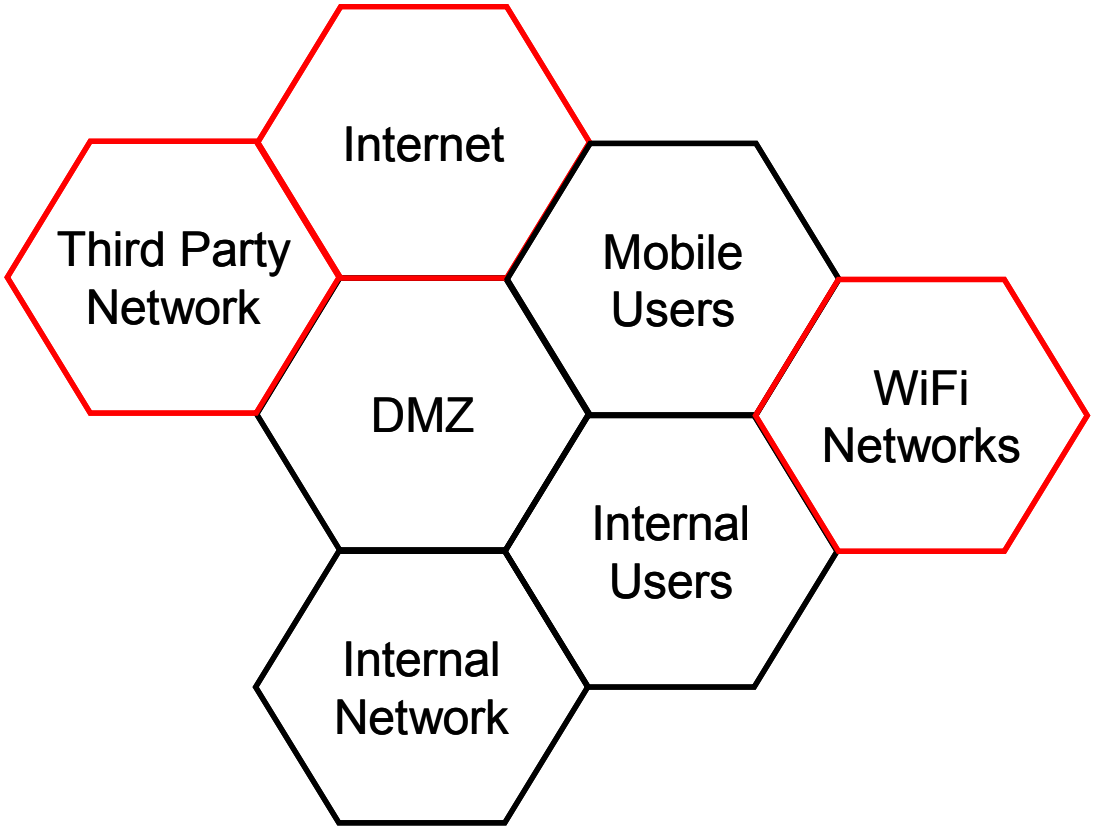
- Mobile / Remote User environment
  - Reception;
  - Delivery;
  - Operation;
  - Change of ownership;
  - Change of location and connection;
  - External maintenance;
  - Retirement;
  - Sale;
  - Theft.

- Internal / Server 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.

The following graph represents very common environments. The environments in black are trusted, the environments in red are not trusted. While the boundary between the DMZ and the third party network is a third party connection, the boundary between Users and WiFi Networks is a physical one (external WiFi networks across the street). Mobile Users can sometimes connect directly to the internal network through the DMZ, and can sometimes access Internet directly.



10.1 Glossary

Term	Glossary Definitions
Access	Any exchange of a message between an interface, a repository or a service.
Access Control	The set formed by the User registration, Authentication, Authorization, Signing and Recording processes.
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)
Activity	Set of actions performed to achieve a particular result.
Agreement	A documented understanding between two or more parties.
Alarm	A set of events likely to be caused by an incident.
Alert	A warning of a possible weakness or type of weakness, a new threat or a measured value of a metric going beyond defined thresholds. (Not equivalent to [ISO] Alert, Similar to [ITIL] Alert)
Assessment	Checking if an organization meets all the requirements specified in a standard or regulation to be accredited or audited.
Asset	Any valuable property of the organization.
Attack	A class of incident with an intentional human cause. (Not equivalent to [ISO] Attack “An attempt to exploit a vulnerability”)
Audience	Group of authorised users of an interface, service or repository.
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 Skills to conduct an Audit on behalf of a Process Owner or a Customer.
Authentication	Process that links the use of user accounts with their owner and manages the lifecycle of sessions.
Authority	The technical person who implements approved access requests.
Authorization	Process that grants the use of services and interfaces and access to repositories to authorized&authenticated users and denies it to unauthorised users.
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.
Availability	1. The period of time when a process must performed as expected upon demand with minimal or no interruptions. 2. The period of time when a service, interface of channel must be accessible and usable upon demand with minimal or no interruptions.

Term	Glossary Definitions
Baseline	The recorded state of an information system at a specific point in time.
Border	A boundary between two environments.
Catastrophe	Any incident that could result in an organization's demise.
Certificate	1. A credential based on Public Key Cryptography techniques. 2. A credential of being compliant with some standard or regulation.
Certification Body / Registration body	A third party that assesses and certifies/ registers the ISMS of an organization with respect to published ISMS standards, and any supplementary documentation required under the system.
Certification Document / Registration Document	Document indicating that an organization'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	An information system that uses a service provided by another information system.
Common cause	An non-assignable cause for a metric going beyond current thresholds, which may be a stochastic or chance effect.
Configuration Item	A service, repository, channel, interface or set of them.
Configuration Management DataBase	A database that contains the details of configuration items and their relationships.
Control	Any kind of measure that can prevent, detect and correct undesired events. (Equivalent to [Cobit] Control)
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 cannot be replaced by alternative capabilities, and is highly likely to jeopardize business goals.
Customer	He who provides the resources and sets the requirements for the process. (Equivalent to [Cobit] and [CMMI] Customer)
Device	Instrument, software, measurement standard, reference material, auxiliary apparatus or combination thereof used to measure a process metric.
Digital Signature	A type or record that includes the will and intent of a user about a repository. It might be hidden using watermarking techniques.
Disaster	See Catastrophe
Effectiveness	An instance of an input of a process producing the expected output.
Efficiency	The proportion between the resources used to deliver an output given a certain input and the number and quality of outputs.

Term	Glossary Definitions
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 information or missing resources needed for the task. (There is no [ISO] equivalent). (Similar to [ITIL] Error)
Event	Any fact that can lead to the detection of an incident. (Equivalent to [ISO] Alert) (Similar to ITIL Event).
Expectation	Any hope for the future state of assets, organizational processes or information systems.
Exposure	Any weakness that is visible to potential attackers.
Fault	Synonym for Error.
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.
Impact	The direct and indirect cost of an incident including the cost of restoring the assets to the pre-incident state. (Similar to [ITIL] Impact)
Incident	A failure to meet a security objective resulting from accidents, errors or attacks. (There is no [ISO] equivalent). (Not Equivalent to [ITIL] Incident) (Not equivalent to [Cobit] Incident)
Indicative Equipment	A Device that delivers qualitative information.
Information System	A human and technical infrastructure for the storage, processing, transmission, input and output of information.
Information System Owner	The Customer [ITIL] of an information system, who has all the rights to the system, including discontinuation.
Input specifications	Procedures and policies that specify the requirements for the input of a process
Inputs	The resource needed to generate the output of a process for which there are no possible alternatives.
Intellectual property	Information which an organization has rights over under copyright, trade mark or patent law.
Interface	A means of information input or output between a user and an information system.
Intrusion	The theft of information about a target by an attacker.
Key Goal Indicator	A metric of success of a process or management system. (Similar to [Cobit] Key Goal Indicator)
Key Performance Indicator	A metric of performance success of a process or management system. (Similar to [Cobit] Key Performance Indicator)
Knowledge Management	The Process responsible for gathering, analysing, storing and sharing knowledge information within an organization. The primary purpose of Knowledge Management is to improve Efficiency by reducing the need to rediscover knowledge.
Licence	An agreement that details the rights granted by an intellectual property owner to use certain information.

Term	Glossary Definitions
Lifecycle	The set of states that make up a series of operational conditions of an information system.
Logging	See Recording.
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.
Management	To manage something is to define and achieve goals while optimising the use of Resources.
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.
Mean Time Between Failures	The average time between a two failures of an information system.
Mean Time To Repair	The average time taken to restore an information systems after a failure.
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.
Metric	A quantitative measurement that can be interpreted in the context of a series of previous or equivalent measurements.
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).
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.
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 organization.
Operational Level Agreement (OLA)	SLA between a process provider and a Customer from the same organization who is a process provider to other Customers. (Equivalent to [ITIL] OLA)
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.
Organization	A group of people that agree or accept responsibilities to act together with a common purpose. Associations, companies and public institutions, for example, are organizations.
Output	Results of a process.

Term	Glossary Definitions
Output specifications	Procedures and policies that specify the requirements for the output of a process.
Partition	Any subdivision of a whole that does not intersect totally or partially any other subdivision
Performance	Comparison between the outputs obtained and the set goals for outputs of a process.
Policy	Documented rules to observe during implementation and maintenance that serve as governing principles when procedures are not detailed enough for a minority of cases.
Personal information	Information that can identify a person.
Private information	See Personal information.
Problem	A cause of several non-simultaneous errors or accidents.
Process	A organized set of tasks that uses resources and inputs to produce outputs.
Process operator	Person or team that performs a process.
Process Owner	The person or team responsible for a process, including performance, prioritizing, planning for growth, and accounting for costs. (Not Equivalent to [CMM] Process Owner)
Process specification	Procedures and policies that specify the requirements for a process.
Provider	The process owner of a process that delivers its outputs.
Quality	The meeting or surpassing of expectations.
Record	An particular instance result of logging, including details like Interface ID and Location, User account or certificate ID, Signature, Type, Date and Time of Access attempt, Access attempt result, Repository, Interface, Service or Message accessed, etc.
Recording	The process that registers the results of the user registration, authentication, authorization, use of systems and signing processes, so these can be investigated and will and intent or responsibilities determined.
Recovery Point	Point in time when business processes or information systems can fall back in case of an incident.
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.
Repository	Any permanent or transient storage of information.
Resilience	The ratio between the MTBF of a functionally equivalent redundancy free system and the MTBF of the system.

Term	Glossary Definitions
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. • Energy; • Hardware, Software, Communication; • Information (Logistic, organizational, Procedimental, Technical, Policies, Contracts). • Logistics and Infrastructure; • Money; • People; • Some fundamental resources are: • Space; • Time;
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.
Responsiveness	See Performance
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)
Scalability	The ability of an IT Service, Process, Configuration Item etc. to perform its agreed function when the workload or scope changes.
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. (Similar to [ITIL] Service)
Service Level Agreement (SLA)	Quality agreement between a process provider and a Customer specified using a set of metrics. (Similar to SLA [ITIL])
Service Level Objective (SLO)	See Threshold
Session	A temporary relationship of trust between services or interfaces. The establishment of this relationship can start authentication one way or both ways and can timeout or be terminated by either service or interface.
Skills	Demonstrated personal attributes and demonstrated ability to apply knowledge and competence
Signing	Process that records the will and intent about a repository of the owner of the user account or certificate concerning a repository, such as agreeing, witnessing or claiming authorship of repositories and messages like original works, votes, contracts and agreements.
Special cause	An assignable cause for a metric going beyond current thresholds.
Specific Goal	An objective of a set of specific practices.

Term	Glossary Definitions
Specific Practice	A process.
Stakeholder	A person, team or organization with interest in the success of a process, a management system or an organization.
Strategic Processes (SP)	Processes that determine the objectives of lower level processes.
Supplier	See Provider
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 (applications, systems, nodes, services, interfaces, repositories or channels) which may be the victim or potential victim of an attack.
Terminal	An interface that is used directly by a User.
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. (Equivalent to [ITIL] Threshold)
TPSRSR	Acronym for Transparency, Partitioning, Supervision, Rotation and Separation of Responsibilities.
Transaction	A discrete function performed by an IT Service. For example transferring money from one bank account to another. A single Transaction may involve numerous additions, deletions and modifications of data. Either all of these complete successfully or none of them is carried out.
Underpinning contract (UC)	A Service Level Agreement between a external process or product provider with a Customer
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.
User Registration	Process that links user accounts and certificates to identifiable users, and manages the lifecycle of user accounts, certificates and access rights.
Visibility	The degree to which information assets at a border present 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) (Similar to [Cobit] Risk)
Warning	See Alert
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)