ISM3

INFORMATION_SECURITY_MANAGEMENT_MATURITY_MODEL

HandBook

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

The cover is cropped from the Wikimedia Commons “Streichholz” by Sebastian Ritter, licensed under the Creative Commons Attribution-ShareAlike 2.5 License, used with permission of the author.

Founding 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

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
- 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.
- 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)

Table of Contents

1 Concepts – Processes and Metrics

Each information security management process is described in terms of the following:

<table>
<tr><td><b>Definition</b></td><td colspan="2"><b>Description</b></td><td colspan="2"><b>Rationale</b></td></tr>
<tr><td><b>Requirements</b></td><td colspan="2"><b>Documentation</b></td><td><b>Inputs</b></td><td><b>Outputs</b></td></tr>
<tr><td><b>Metrics</b></td><td><b>Activity</b></td><td><b>Scope</b></td><td><b>Update</b></td><td><b>Availability</b></td></tr>
<tr><td><b>Management</b></td><td colspan="4"><b>Responsibilities</b></td></tr>
<tr><td><b>Connections</b></td><td colspan="2"><b>Related Processes</b></td><td colspan="2"><b>Related Methodologies</b></td></tr>
</table>

In this HandBook only the definition is given. For the remaining details and to clear any doubt about terminology used, please check ISM3 proper. The full structure of the process definition template is:

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: 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 organisation or the environment is covered by the process.
Update	Metric description of the frequency of update of the process activity and the systems that support this activity.
Availability	Metric description of the period of time that a process has performed as expected upon demand, and the frequency and duration of interruptions.
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.
Related Processes	Other ISM3 processes that are required to generate key inputs.
Related Methodologies	Well-known methodologies and best practices. These methodologies may be useful to identify relevant activities, risks and controls.

2 Concepts - Security in Context Model

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*. There should be a balance between Business, compliance and technical needs and limitations, like cost, functionality, privacy, liability and risk.

As the next table outlines, achieving business goals depends on business objectives, which in turn depend partially on security objectives. There are three type of security objectives, the ones derived directly from business needs, the ones that are consequence of the regulatory environment and the ones derived from the use of information systems.

	Examples	**Depend total or partially on...**
Business Goals	▪ Achieving a vision and mission; ▪ Continuing to exist; ▪ Maintaining and growing revenue; ▪ Attract, maintain and foster talent; ▪ Maintaining and growing brand and reputation; ▪ Complying with internal ethics and social responsibility goals; ▪ Complying with regulations and contracts;	**Business Objectives**
Business Objectives	▪ Paying the payroll on the 1st of every month; ▪ Paying all incoming invoices within a certain time frame; ▪ Paying taxes in time; ▪ Invoice all products and services provided; ▪ Deliver the products and services when and where committed by the organization; ▪ Keep any records needed to pass successfully any audit, like a tax audit or a software licences audit. ▪ Prevent breach of contractual agreements; ▪ Protect intellectual property and legal rights;	**Market Conditions, Competition, Seasonal changes, Costs, Pricing, Workforce skill and commitment, Innovation...** **Quality Objectives** **Security Objectives**
Security Objectives	▪ Personal information can't be kept for longer than needed. ▪ Systems are as free of weaknesses as possible. ▪ Users are accountable for their acceptance of contracts and agreements.	**Compliance Needs and Limitations** **Technical Needs and Limitations** **Business Needs and Limitations**

	Examples	Depend total or partially on...
Compliance Needs and Limitations	▪ Third party services and repositories need to be appropriately licensed. ▪ Personal information completeness must be proportional to its use. ▪ Personal information can't be kept for longer than needed. ▪ Tax records must be kept for a minimum number of years. ▪ Personal information must be protected using certain security measures depending on the type of personal information. ▪ 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 of ceded. ▪ Repositories with Personal information have to be registered with a Data Protection agency. ▪ Encryption must be used under legal limitations. ▪ Secrets must be kept according to the terms of agreed Non Disclosure Agreements. ▪ The owner of Personal information will be given notice when his data is being collected, including who is collecting the data. ▪ Personal information must used for the purpose agreed with the information owner.. ▪ Personal information must not be disclosed without the agreement of the information owner.. ▪ Personal information owners will have means to make data collectors accountable for their use of his personal information.	OSP-21 Information Quality and Compliance Probing (among others)
Technical Needs and Limitations	▪ Systems are as free of weaknesses as possible. ▪ Systems are visible to trusted systems only. ▪ Systems that need to be visible to not trusted systems are the less visible possible. ▪ Systems run trusted services only. ▪ The electricity, temperature and humidity where systems operate exceeds the systems needs.	OSP-5 Environment Patching OSP-7 Environment Hardening OSP-16 Segmentation and Filtering Management OSP-17 Malware Protection Management (among others)
Business Needs and Limitations	▪ Use of services and physical and logical access to repositories and systems is restricted to authorized users; ▪ Users are accountable for the repositories and messages they create or modify; ▪ Users are accountable for their acceptance of contracts and agreements. ▪ Users are accountable for their use of services. ▪ Availability of repositories, services and channels exceeds Customer needs; ▪ Repositories are retained at least as long as Customer requirements; ▪ Precision, relevance (up-to-date), completeness and consistency of repositories exceeds Customer needs;	**Access Control Objectives** **Priority Objectives** **Durability Objectives** **Information Quality Objectives**

	Examples	**Depend total or partially on...**
Access Control Objectives	▪ Personal information preserves the anonymity of the information subjects if necessary, for example not linking user accounts or certificates to an identifiable user; ▪ Links the use of user accounts with their owners; ▪ Granting the use of services and interfaces and access to repositories to authorized users. ▪ Denying the use of services and interfaces and access to repositories to unauthorized users. ▪ Express the will and intent about a repository of the owner of a user account or certificate. ▪ Accurate recording of: ▪ Interface ID and Location; ▪ User account or certificate ID; **a)** ▪ Signature; ▪ Type of Access Attempt ▪ Date and Time of Access attempt; ▪ Access attempt result; ▪ Repository, Interface, Service or Message accessed. ▪ Personal information is accessible to authorized users only and is held for no longer than required ▪ Secrets are accessible to authorized users only ▪ Third party services and repositories are appropriately licensed and accessible only to authorized users ▪ Information systems are physically accessible only to authorized users ▪ Repositories are accessed by authorised users only ▪ Will and intent on repositories is expressed using valid digital signatures	OSP-3 Inventory Management OSP-11 Access control OSP-12 User Registration OSP-14 Physical Environment Protection Management (among others)
Priority Objectives	▪ Availability of repositories, services and channels exceeds Customer needs; ▪ Reliability and performance of services and channels exceeds Customer needs; ▪ Volatility of services and channels within Customer needs;	OSP-26 Enhanced Reliability and Availability Management OSP-15 Operations Continuity Management (among others)
Durability Objectives	▪ Repositories are retained at least as long as Customer requirements; ▪ Expired or end of life-cycle repositories are permanently destroyed;	OSP-6 Environment Clearing OSP-10 Backup Management OSP-27 Archiving Management (among others)
Information Quality Objectives	▪ Precision, relevance (up-to-date), completeness and consistency of repositories exceeds Customer needs;	OSP-21 Information Quality and Compliance Probing (among others)

3 Requirements - Certification

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.

These tables specify the processes required to achieve every maturity level.

General

	Level 1	Level 2	Level 3	Level 4	Level 5
GP-1 Document Management	X	X	X	X	X +Metrics
GP-2 ISM System and Business Audit	X	X	X	X	X +Metrics
GP-3 ISM Design and Evolution	X	X	X	X	X +Metrics

Strategic Management

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

Tactical Management

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

Operational Management

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

4 Information Security Management Process Model

4.1 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.

4.2 Generic Practices

Generic Practice	**GP-1 Document management**
Description	This process underpins the ISM System by defining document quality standards, organisation 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.

Generic Practice	**GP-2 ISM System and Business Audit**
Description	This process validates: • The compliance of business processes with applicable regulations. • If the existing scheme of delegation follows TPSRSR rules. • If the implementation of ISM system as defined. 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.

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 Design, amongst them: • ISM3 Maturity Level choice; • ROSI Evaluation; • Threat Evaluation; • Vulnerability Evaluation; • Business Impact Evaluation. • Risk Evaluation (Threat, Vulnerability and Impact Evaluation); Modelling the organisation 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.
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 organisation towards higher levels of capability.

4.3 Specific Practice: Strategic Management

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

4.3.1 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 organisations, 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.

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.

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.

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.

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.

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.

4.4 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.

4.4.1 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.

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.

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.

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.

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.

Process	TSP-4 Service Level Management
Description	Defines process metrics for other processes in the ISM. Reviews the thresholds for every process metric. Diagnoses and requests action on abnormal metric measurements. 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.

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.

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.

Process	TSP-8 Security Personnel Selection
Description	This process aims to guarantee the commitment, competency, knowledge and experience of new employees through evidence-based assessment.
Rationale	Personnel trusted to carry out security processes must be competent, accountable and empowered. Evidence in the form of responses to Skills-based interview questions, professional certifications and educational qualifications are needed to support selection decisions.

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.

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.

Process	TSP-11 Security Awareness
Description	This process informs and educates users, raising the profile of information security

Process	TSP-11 Security Awareness
	throughout the organization.
Rationale	A high standard of security awareness throughout the organisation is required to prevent and mitigate security incidents.

4.5 Specific Practice: Operational Management

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

4.5.1 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).

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.

Process	OSP-2 Select tools for implementing security measures
Description	Selection of the specific products that best fit the Information Security Objectives and metrics within the budget assigned.
Rationale	Efficient use of resources results from effective selection of appropriate security tools.

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 classification, priority, durability and quality.

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.

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.

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.

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.

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.

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.

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.
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.

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.
Rationale	Incidents relating to the infection of internal assets with Malware can be prevented and mitigated by an appropriate Malware protection process.

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. • 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.

Process	OSP-11 Access control
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.

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. 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.
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.

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.
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.

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**: 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.

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.

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.
Related Processes	OSP-2 Select tools for implementing security measures 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.

Process	**OSP-19 Internal Technical Audit**
Description	This process validates: • The effectiveness of vulnerability reduction measures. • The effectiveness of access control 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 organisation can be prevented by attacks emulation and subsequent software mending, environment hardening, investment and improved monitoring.

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.

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.

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.

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.

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.

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;

5 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. Different environments will have their own security objectives and their own instances of ISM processes. The following are examples of common logical environments, with examples of the states that make up their lifecycles:

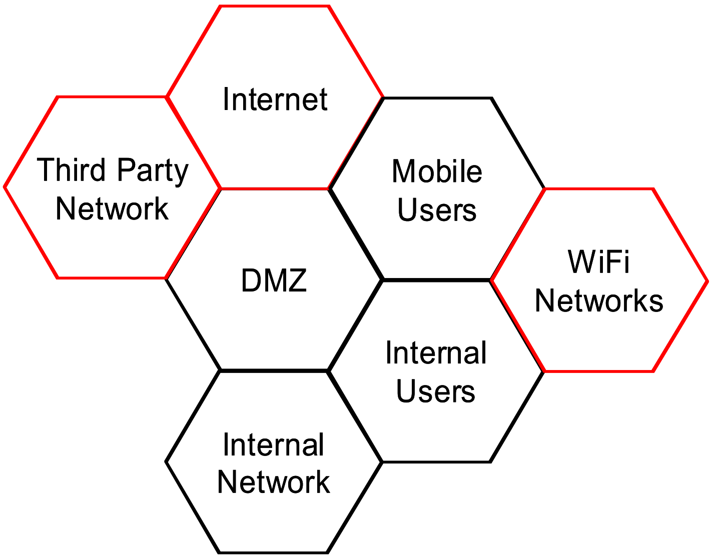
- Internal / User environment.
  - Reception;
  - Delivery;
  - Operation;
  - Change of ownership;
  - External maintenance;
  - Retirement;
  - Sale;
  - Theft.

- 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.



6 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 organisations may be at risk from interception of a low level channel (OSI level 1), such as infra-red on a wireless keyboard, and have specific policies for infra-red channel.

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

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

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

Service	**Message**
Bank Account	Transfer from another account
SOAP API Interface	SOAP Call
Port	TCP Packet
Ethernet Port	Ethernet Packet