INFORMATION SECURITY GLOSSARY

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

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)

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	A set of actions designed to achieve a particular result. Activities are usually defined as part of Processes or Plans, and are documented in Procedures.
Agreement	A Document that describes a formal understanding between two or more parties. An Agreement is not legally binding, unless it forms part of a Contract.
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 organisation 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.

Term	Glossary Definitions
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.
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 organisation with respect to published ISMS standards, and any supplementary documentation required under the system.
Certification Document / Registration Document	Document indicating that an organisation's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system.
Certification System / Registration System	System having its own rules of procedure and management for carrying out the assessment leading to the issuance of a certification/ registration document and its subsequent maintenance.
Channel	A channel is the medium used by services to exchange messages transparently, without explicit help from other lower level services. This collaboration is normally needed for creating and closing logical channels.
Client	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	The Customer of a process 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	A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or activity is one that achieves its agreed Objectives.

Term	Glossary Definitions
Efficiency	A measure of whether the right amount of resources have been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources.
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.
Failure	Loss of ability to Operate to Specification, or to deliver the required output. The term Failure may be used when referring to IT Services, Processes, Activities, Configuration Items etc. A Failure often causes an Incident.
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 Information Technology 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 organisation 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)

Term	Glossary Definitions
Knowledge Management	The Process responsible for gathering, analysing, storing and sharing knowledge information within an Organisation. 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.
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.
Monitoring	Implies observing, supervising, keeping under review (using monitoring devices); it can involve measuring or testing at intervals, especially for the purpose of regulation or control.
Network	A set of physical or logical channels connecting repositories and interfaces.
Node	An information system whose primary function is relay messages between channels (Not equivalent to [ISO] Node).
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 organisation.
Operational Level Agreement (OLA)	SLA between a process provider and a Customer from the same organisation who is a process provider to other Customers. (Equivalent to [ITIL] OLA)

Term	Glossary Definitions
Operational Process (OP)	A process that delivers the requirements set by tactical management.
Opportunity	The combination of an asset, a threat and an occasion that may give rise to an incident.
Organisation	A group of people that agree or accept responsibilities to act together with a common purpose. Associations, Companies and public institutions, for example, are organisations.
Output	Results of a process.
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.

Term	Glossary Definitions
Resilience	The ratio between the MTBF of a functionally equivalent redundancy free system and the MTBF of the system.
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	The set of successful and failed accesses to repositories and uses of services between the time a user account is authenticated and the time the authentication expires or the authentication is terminated.
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

Term	Glossary Definitions
Specific Goal	An objective of a set of specific practices.
Specific Practice	A process.
Stakeholder	A person, team or organisation with interest in the success of a process, a management system or an organisation.
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 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 an interfaces or provide services to information systems outside the organization.
Vulnerability	The likelihood of an incident, measured as real instances against possible attacks, accidents and errors per year. These attacks, accidents and errors can be triggered by one or several threats. (Not equivalent to [ISO] Vulnerability) (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)