INFORMATION SECURITY CRITERIA MAPPED

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

1 Information Security Criteria

Items in the first column are repeated as needed to show different matches with criteria from the rest of the columns.

ISM3 Security Objectives	ISO Integrity, Availability, Confidentiality	Cobit Information Criteria	Parkerian Hexad
Accurate time and date should be reflected in all records	No equivalent	No equivalent	No equivalent
Availability of repositories, services and channels should exceed Customer needs. It can be measured as the period of time when a service, repository, interface or channel must exist, be accessible and usable (perform according to customer needs) upon demand. It is measured as well by the oldest recent messages and information that can be lost because of an interruption of service, channel or interface	Availability is the property of being accessible and usable upon demand by an authorized entity	Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities	Availability means having timely access to information
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	No equivalent	Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner	Utility means usefulness
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	No equivalent	Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations	Utility means usefulness

ISM3 Security Objectives	ISO Integrity, Availability, Confidentiality	Cobit Information Criteria	Parkerian Hexad
Compliance Needs and Limitations. Examples: • Third party services and repositories need to be appropriately licensed. • Personal information completeness must be proportional to its use. • 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 or ceded. • 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. • Personal information is held for no longer than required Tax records must be kept for a minimum number of years. • Repositories with Personal information have to be registered with a Data Protection agency	No equivalent	Compliance deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, e.g., externally imposed business criteria as well as internal policies	No equivalent

ISM3 Security Objectives	ISO Integrity, Availability, Confidentiality	Cobit Information Criteria	Parkerian Hexad
Expired or end of life-cycle repositories should be permanently destroyed. It can be measured as the date the expired or end of life-cycle repositories and records should be permanently and reliably destroyed.	No equivalent	No equivalent	No equivalent
Information systems and repositories should be physically accessible only to authorized users	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Confidentiality concerns the protection of sensitive information from unauthorized disclosure.	Possession or Control
Intellectual property (licensed, copyrighted, patented and trademarks) should be accessible to authorized users only	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Confidentiality concerns the protection of sensitive information from unauthorized disclosure.	Confidentiality refers to limits on who can get what kind of information. For example, executives concerned about protecting their enterprise's strategic plans from competitors individuals are concerned about unauthorized access to their financial records.
This is a businesses objective, not a security objective	This is not a information security criterion	Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.	This is not a information security criterion
Personal information should be accessible for a valid purpose to authorized users only and is held for no longer than required	Confidentiality (partial match)	Effectiveness (partial match)	Confidentiality (partial match)

ISM3 Security Objectives	ISO Integrity, Availability, Confidentiality	Cobit Information Criteria	Parkerian Hexad
Personal information should preserve the anonymity of the information subjects if necessary, for example not linking user accounts or certificates to an identifiable user	No equivalent	No equivalent	No equivalent
Precision, relevance (up-to-date), completeness and consistency of repositories should exceed Customer needs. It can be measured as the maximum rate of erroneous and outdated information in the information available.	No equivalent	Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.	Utility means usefulness
Precision, relevance (up-to-date), completeness and consistency of repositories should exceed Customer needs. It can be measured as the maximum rate of erroneous and outdated information in the information available.	No equivalent	Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations	Utility means usefulness
Reliability and performance of services and channels should exceed Customer needs. it can be measured as 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.	Reliability (partial match)	Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities	Availability means having timely access to information.
Reliability and performance of services and channels should exceed Customer needs. it can be measured as 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	Reliability: the property of consistent intended behavior and results	Reliability relates to the provision of appropriate information for management to operate the entity and to exercise its fiduciary and governance responsibilities	Availability means having timely access to information

ISM3 Security Objectives	ISO Integrity, Availability, Confidentiality	Cobit Information Criteria	Parkerian Hexad
Repositories should be accessed by authorized users only	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Confidentiality concerns the protection of sensitive information from unauthorized disclosure	Confidentiality refers to limits on who can get what kind of information. For example, executives concerned about protecting their enterprise's strategic plans from competitors individuals are concerned about unauthorized access to their financial records.
Retention period can be measured as the minimum length of time a repository is kept (preserved) according to or exceeding customer and regulatory requirements	Integrity the property of safeguarding the accuracy and completeness of assets	Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations	Integrity refers to being correct or consistent with the intended state of information
Secrets (personal, industrial, trade) should be accessible to authorized users only	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Confidentiality concerns the protection of sensitive information from unauthorized disclosure	Confidentiality refers to limits on who can get what kind of information. For example, executives concerned about protecting their enterprise's strategic plans from competitors individuals are concerned about unauthorized access to their financial records.
Systems should be as free of weaknesses as possible	Integrity the property of safeguarding the accuracy and completeness of assets	Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations	Integrity refers to being correct or consistent with the intended state of information.

ISM3 Security Objectives	ISO Integrity, Availability, Confidentiality	Cobit Information Criteria	Parkerian Hexad
Systems should run trusted services only	Integrity the property of safeguarding the accuracy and completeness of assets	Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations	Integrity refers to being correct or consistent with the intended state of information.
Systems that need to be visible to not trusted systems are the least visible possible. Systems are visible to trusted systems only	No equivalent	No equivalent	No equivalent
The Authentication Process links the use of user accounts with their owner and manages the lifecycle of sessions	Authenticity: The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information	No equivalent	No equivalent
The Authentication Process links the use of user accounts with their owner and manages the lifecycle of sessions	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Confidentiality concerns the protection of sensitive information from unauthorized disclosure.	Confidentiality refers to limits on who can get what kind of information. For example, executives concerned about protecting their enterprise's strategic plans from competitors individuals are concerned about unauthorized access to their financial records.

ISM3 Security Objectives	ISO Integrity, Availability, Confidentiality	Cobit Information Criteria	Parkerian Hexad
The Authorization Process grants the use of services and interfaces and access to repositories to authorized users and denies it to unauthorized users.	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Confidentiality concerns the protection of sensitive information from unauthorized disclosure.	Confidentiality refers to limits on who can get what kind of information. For example, executives concerned about protecting their enterprise's strategic plans from competitors individuals are concerned about unauthorized access to their financial records
The electricity, temperature and humidity where systems operate should exceed the systems needs	No equivalent	No equivalent	No equivalent
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.	Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity	Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations	No equivalent
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.	Non-repudiation: the ability to prove an action or event has taken place, so that this event or action cannot be repudiated later.	No equivalent	Authenticity refers to correct labeling or attribution of information.
Third party services and repositories should be appropriately licensed and accessible only to authorized users	Confidentiality (partial match)	Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations	Possession or Control

ISM3 Security Objectives	ISO Integrity, Availability, Confidentiality	Cobit Information Criteria	Parkerian Hexad
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.	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Confidentiality concerns the protection of sensitive information from unauthorized disclosure.	Confidentiality refers to limits on who can get what kind of information. For example, executives concerned about protecting their enterprise's strategic plans from competitors individuals are concerned about unauthorized access to their financial records.
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.	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Confidentiality concerns the protection of sensitive information from unauthorized disclosure.	Confidentiality refers to limits on who can get what kind of information. For example, executives concerned about protecting their enterprise's strategic plans from competitors individuals are concerned about unauthorized access to their financial records.

ISM3 Security Objectives	ISO Integrity, Availability, Confidentiality	Cobit Information Criteria	Parkerian Hexad
Use of services and physical and logical access to repositories and systems should be restricted to authorized users	Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.	Authenticity refers to correct labeling or attribution of information.
Users should be accountable for the repositories and messages they create or modify	Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity	No equivalent	Authenticity refers to correct labeling or attribution of information
Users should be accountable for their acceptance of contracts and agreements	Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity	No equivalent	Authenticity refers to correct labeling or attribution of information
Users should be accountable for their use of services	Accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity	No equivalent	Authenticity refers to correct labeling or attribution of information

