ISM^3

INFORMATION_SECURITY_MANAGEMENT_MATURITY_MODEL

MATURITY AND CAPABILITY LEVELS 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

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

1 Maturity Levels Mapping

ISM3 Maturity Levels	Cobit Maturity Levels	CMMI Maturity Levels
No equivalent	**Non-existent** Complete lack of any recognizable processes. The enterprise has not even recognized that there is an issue to be addressed.	No equivalent
No equivalent	**Initial** There is evidence that the enterprise has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead there are approaches that tend to be applied on an individual or case-by-case basis. The overall approach to ad hoc management is disorganized.	**Initial (ad hoc)** ● Ad hoc, chaotic ● Heroics ● Performance difficult to predict ● Management practices may not be effective At maturity level 1, processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment to support the processes. Success in these organizations depends on the competence and heroics of the people in the organization and not on the use of proven processes. In spite of this chaos, maturity level 1 organizations often produce products and services that work; however, they frequently exceed their budgets and do not meet their schedules Maturity level 1 organizations are characterized by a tendency to over commit, abandonment of processes in a time of crisis, and an inability to repeat their successes.
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.	No equivalent	No equivalent

ISM3 Maturity Levels	Cobit Maturity Levels	CMMI Maturity Levels
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.	**Repeatable** Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.	**Managed** ● Project Management more disciplined than at level 1 ● Policies established and followed ● These are documented and followed:b Project Plans, Process descriptions ● Resources are adequate, reviews occur ● Repeatable processes, and successes ● Processes characterized for projects ● Management often reactive At maturity level 2, the projects of the organization have ensured that processes are planned and executed in accordance with policy; the projects employ skilled people who have adequate resources to produce controlled outputs; involve relevant stakeholders; are monitored, controlled, and reviewed; and are evaluated for adherence to their process descriptions. The process discipline reflected by maturity level 2 helps to ensure that existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans.
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.	**Defined** Procedures have been standardized and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.	**Defined** ● Processes are characterized for the organization Management is proactive, tackling problems before they occur At maturity level 3, processes are well characterized and understood, and are described in standards, procedures, tools, and methods. The organization's set of standard processes, which is the basis for maturity level 3, is established and improved over time. These standard processes are used to establish consistency across the organization. Projects establish their defined processes by tailoring the organization's set of standard processes according to tailoring guidelines.

ISM3 Maturity Levels	Cobit Maturity Levels	CMMI Maturity Levels
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.	**Managed** It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.	**Quantitatively Managed** ● Statistical and other quantitative methods are used, at the organizational and project. levels, to understand the past process performance . ● Predict the future process performance. ● Predict the future product quality and service quality. At maturity level 4, the organization and projects establish quantitative objectives for quality and process performance and use them as criteria in managing processes. Quantitative objectives are based on the needs of the customer, end users, organization, and process implementers. Quality and process performance is understood in statistical terms and is managed throughout the life of the processes. For selected subprocesses, detailed measures of process performance are collected and statistically analyzed. Quality and process-performance measures are incorporated into the organization's measurement repository to support fact-based decision making. Special causes of process variation are identified and, where appropriate, the sources of special causes are corrected to prevent future occurrences.
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.	**Optimized** Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the work flow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.	**Optimizing** ● Incremental and innovative improvements that measurably increase process capabilities are identified, evaluated, and deployed. At maturity level 5, an organization continually improves its processes based on a quantitative understanding of the common causes of variation inherent in processes. (See the definition of "common cause of process variation" in the glossary.) Maturity level 5 focuses on continually improving process performance through incremental and innovative process and technological improvements. Quantitative process improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement. The effects of deployed process improvements are measured and evaluated against the quantitative process improvement objectives. Both the defined processes and the organization's set of standard processes are targets of measurable improvement activities.

2 Capability Levels Mapping

ISM3 Capability Levels	Cobit Capability Levels	CMMI Capability Levels
Not Applicable	Management processes are not applied	**Incomplete**
Undefined The process might be used, but it is not defined or Documented.	Processes are ad hoc and disorganized	**Performed** A performed process is a process that satisfies the specific goals of the process area. It supports and enables the work needed to produce work products.
Not Applicable	Processes follow a regular pattern	Not Applicable
Defined The process is Documented and used.	Processes are documented and communicated	**Managed** A managed process is a performed process that has the basic infrastructure in place to support the process. It is planned and executed in accordance with policy; employs skilled people who have adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled, and reviewed; and is evaluated for adherence to its process description
Managed The process is Defined and the results of the process are used to fix and improve the process. (ISO9001 equivalent) The following metrics are used: ● Scope ● Activity ● Availability ● Efficacy	Not Applicable	**Defined** A defined process is a managed process that is tailored from the organization's set of standard processes according to the organization's tailoring guidelines, and contributes work products, measures, and other process improvement information to the organizational process assets. A critical distinction between capability levels 2 (Managed) and 3 i(Defined) s the scope of standards, process descriptions, and procedures. At capability level 2, the standards, process descriptions, and procedures may be quite different in each specific instance of the process (e.g., on a particular project). At capability level 3, the standards, process descriptions, and procedures for a project are tailored from the organization's set of standard processes to suit a particular project or organizational unit and therefore are more consistent, except for the differences allowed by the tailoring guidelines. Another critical distinction is that at capability level 3, processes are typically described more rigorously than at capability level 2. A defined process clearly states the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs, and exit criteria. At capability level 3, processes are managed more pro actively using an understanding of the interrelationships of the process activities and detailed measures of the process, its work products, and its services.

ISM3 Capability Levels	Cobit Capability Levels	CMMI Capability Levels
Controlled The process is Managed and milestones and need of resources is accurately predicted. The following metrics are used: ● Load ● Update	Processes are monitored and measured	**Quantitatively Managed** A quantitatively managed process is a defined process that is controlled using statistical and other quantitative techniques. Quantitative objectives for quality and process performance are established and used as criteria in managing the process. Quality and process performance is understood in statistical terms and is managed throughout the life of the process.
Optimized The process is Controlled and improvement leads to a saving in resources The following metrics are used: ● Efficiency, ROSI	Good Practices are followed and automated	**Optimizing** An optimizing process is a quantitatively managed process that is improved based on an understanding of the common causes of variation inherent in the process. The focus of an optimizing process is on continually improving the range of process performance through both incremental and innovative improvements.