SECURITY SERIES

Open Information Security Management Maturity Model (O-ISM3)

Van Haren PUBLISHING

THE Open GROUP

Open Information Security Management Maturity Model (O-ISM3)

Other publications by Van Haren Publishing

Van Haren Publishing (VHP) specializes in titles on Best Practices, methods and standards within four domains:

- IT management
- Architecture (Enterprise and IT)
- Business management and
- Project management

Van Haren Publishing offers a wide collection of whitepapers, templates, free e-books, trainer material etc. in the **VHP Freezone**: freezone.vanharen.net

VHP is also publisher on behalf of leading organizations and companies:
ASLBiSL Foundation, CA, Centre Henri Tudor, Gaming Works, Getronics, IACCM, IAOP, IPMA-NL, ITSqc, NAF, Ngi, PMI-NL, PON, Quint, The Open Group, The Sox Institute

Topics are (per domain):

IT (Service) Management / IT Governance
ABC of ICT
ASL
BiSL
CATS
CMMI
CoBIT
ISO 17799
ISO 27001
ISO 27002
ISO/IEC 20000
ISPL
IT Service CMM
ITIL® V3
ITSM
MOF
MSF
SABSA

Architecture (Enterprise and IT)
Archimate®
GEA®
SOA
TOGAF®

Business Management
CMMI
Contract Management
EFQM
eSCM
ISA-95
ISO 9000
ISO 9001:2000
OPBOK
Outsourcing
SAP
SixSigma
SOX
SqEME®

Project/Programme/ Risk Management
A4-Projectmanagement
ICB / NCB
MINCE®
M_o_R®
MSP™
P3O
PMBOK® Guide
PRINCE2®

For the latest information on VHP publications, visit our website: www.vanharen.net, or freezone.vanharen.net for free whitepapers, templates and e-books.

Open Information Security Management Maturity Model (O-ISM3)

Colophon

Title:	Open Information Security Management Maturity Model (O-ISM3)
A Publication of:	The Open Group
Author:	The Open Group
Editors:	Ian Dobson, Cathy Fox, and Jim Hietala
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN:	978 90 8753 6657
Edition:	First edition, first impression, May 2011
Design and Layout:	CO2 Premedia bv, Amersfoort – NL
Copyright:	© The Open Group 2011

For any further enquiries about Van Haren Publishing, please send an e-mail to: info@vanharen.net

Comments relating to the material contained in this document may be submitted to:

The Open Group
Apex Plaza, Forbury Road
Reading
Berkshire RG1 1AX
United Kingdom
or by electronic mail to: ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service, including UNIX® certification.

Further information on The Open Group is available at www.opengroup.org.

The Open Group has over 15 years' experience in developing and operating certification programs and has extensive experience developing and facilitating industry adoption of test suites used to validate conformance to an open standard or specification.

More information is available at www.opengroup.org/certification.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards and Guides, but which also includes white papers, technical studies, branding and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

As with all *live* documents, Technical Standards and Specifications require revision to align with new developments and associated international standards. To distinguish between revised specifications which are fully backwards-compatible and those which are not:

- A new *Version* indicates there is no change to the definitive information contained in the previous publication of that title, but additions/extensions are included. As such, it *replaces* the previous publication.

- A new *Issue* indicates there is substantive change to the definitive information contained in the previous publication of that title, and there may also be additions/extensions. As such, both previous and new documents are maintained as current publications.

Readers should note that updates – in the form of Corrigenda – may apply to any publication. This information is published at www.opengroup.org/corrigenda.

This document

The Open Information Security Management Maturity Model (O-ISM3) is The Open Group framework for managing information security, and wider still to managing information in the wider context. It aims to ensure that security processes in any organization are implemented so as to operate at a level consistent with that organization's business requirements. ISM3 is technology-neutral. It defines a comprehensive but manageable number of information security processes sufficient for the needs of most organizations, with the relevant security control(s) being identified within each process as an essential subset of that process. In this respect, it is fully compatible with the well-established ISO/IEC 27000:2009, COBIT, and ITIL standards in this field. Additionally, as well as complementing the TOGAF model for enterprise architecture, ISM3 defines operational metrics and their allowable variances.

Efficient business systems are driven by demand and use measurements to improve quality. ISM3 provides a framework for building, tailoring, and operating an Information Security Management System (ISMS). The use of metrics ensures that the management system uses objective quantitative criteria to inform business decisions on allocating IT security resources efficiently and responding to changes. The beneficial outcomes for information security are lower risk and better Return on Investment (RoI).

To be effective, an organization's information security processes must be documented, measured, and managed. ISM3 defines maturity in terms of the operation of key security processes. Capability is defined in terms of the metrics and management practices used. ISM3 requires security objectives and targets to be derived from business objectives, and promotes the formal measurement of effectiveness of each security management process.

Organizations in different business sectors and countries have different business requirements and risk tolerances. The O-ISM3 framework helps information Security Managers to evaluate their own operating environment and to plan their security management processes so they are consistent with and cost-effective for their organization's business objectives.

Trademarks

Boundaryless Information Flow™ is a trademark and ArchiMate®, Jericho Forum®, Motif®, Making Standards Work®, OSF/1®, The Open Group®, TOGAF®, UNIX®, and the "X" device are registered trademarks of The Open Group in the United States and other countries.

COBIT™ is a trademark of the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI).

ITIL® is a registered trademark of the Office of Government Commerce in the United Kingdom and other countries.

Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.

The Open Group acknowledges that there may be other brand, company, and product names used in this document that may be covered by trademark protection and advises the reader to verify them independently.

Acknowledgements

The Open Group would like to thank the people who contributed with work, organization, or valuable comments to the development of this O-ISM3 standard.

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

Contributors to v2.7x (published by The Open Group):
- Chris Carlson, Boeing
- Anton Chuvakin, Security Warrior Consulting
- Ian Dobson, The Open Group
- Phil Griffin, Griffin Consulting
- Jim Hietala, The Open Group
- Alex Hutton, Verizon
- François Jan, Arismore
- Mike Jerbic, Trusted Systems Consulting Group
- Mary Ann Mezzapelle, HP
- Edward Stansfeld, Audit Scotland

Special thanks to significant contributors to versions up to v2.30 (published by the ISM3 Consortium):
- Alex Hutton, Riskanalys.is
- Robert Kloots, CSF bv
- Anup Narayanan, First Legion Consulting
- Anthony B. Nelson, Estec Security
- Kelly Ray, Open Compliance and Ethics Group
- Arthur Richard, Kuwait Oil Company
- George Spafford, Pepperweed Consulting
- Edward Stansfeld, Audit Scotland (editor and principal reviewer and contributor)
- K Rama Subramaniam, Valiant Technologies Pvt Ltd
- Shane Wansink, Deakin University
- Jeff Warren, DHS – Government of Victoria/Australia

Referenced documents

Paradigms

- Defence in Depth
- Keep it Simple, Stupid
- Mayfield's Paradox
- Minimum Privilege
- Need to Know
- Objective-Value-Activity
- People, Process, and Technology
- Prevention, Detection, and Response
- Security by Design
- Shewhart Cycle or Deming Wheel (Plan, Do, Check, Act)

Documents

The following are referenced in this O-ISM3 standard:

- AS 5037:2005: Knowledge Management – A Guide; refer to: www.itgovernance.co.uk.
- AS/NZS 4360:2004: Risk Management (superseded by AS/NZS ISO 31000:2009); refer to: www.riskmanagement.com.au.
- Building Security In Maturity Model (BSIMM); refer to: bsimm2.com.
- BS 25999: Business Continuity; refer to: www.bsigroup.com.
- Carnegie Mellon University Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI); refer to: www.sei.cmu.edu/cmmi.
- Carnegie Mellon University Software Engineering Institute (SEI) People CMM (PCMM); refer to: www.sei.cmu.edu/cmmi/tools/peoplecmm.
- Center for Internet Security (CIS) ; refer to: www.cisecurity.org.
- CLUSIF MEHARI; refer to: www.clusif.asso.fr.
- COBIT Framework for IT Governance and Control, ISACA; refer to: www.isaca.org.
- CRAMM; refer to: www.cramm.com.
- EBIOS; refer to: www.ssi.gouv.fr/archive/en/confidence/ebiospresentation.html.
- Enterprise Security Architecture Consortium Specification (in conjunction with the NAC) (H071), published by The Open Group, December 2004; refer to: www.opengroup.org/bookstore/catalog/h071.htm.

- Federal Enterprise Architecture (USA); refer to: www.whitehouse.gov/omb/e-gov.
- HIMIS (Human Impact Management for Information Security); refer to: isqworld.com/index.php/zones/himis.
- Information Operations (JP 3-13 2006); refer to: http://information-retrieval.info/docs/DoD-IO.html.
- *Information Security Governance: Towards a Framework for Action*, Business Software Alliance, 2003.
- Institute for Security and Open Methodologies (ISECOM) Open Source Security Testing Methodology Manual (OSSTMM); refer to: www.isecom.org/osstmm.
- ISACA IT Audit, Assurance, Security, and Control Standards; refer to: www.isaca.org.
- ISACA IS Control Professionals Standards
- ISC2 CISSP; refer to: www.isc2.org.
- ISO 9000:2005: Quality Management Systems – Fundamentals and Vocabulary; refer to: www.iso.org.
- ISO 9001:2000: Quality Management Systems – Requirements; refer to: www.iso.org.
- ISO 15228: 2005: Textile Machinery and Accessories – Profile Reeds for Air Jet Weaving Machines – Dimensions; refer to: www.iso.org.
- ISO 15489:2001: Information and Documentation – Records Management; refer to: www.iso.org.
- ISO/IEC 12207:2008: Systems and Software Engineering – Software Lifecycle Processes; refer to: www.iso.org.
- ISO/IEC 15408:2009: Information Technology – Security Techniques – Evaluation Criteria for IT Security; refer to: www.iso.org.
- ISO/IEC 21827:2002: Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM); based on Carnegie Mellon's Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI); see www.sei.cmu.edu/cmmi.
- ISO/IEC 24762:2008: Information Technology – Security Techniques – Guidelines for Information and Communications Technology Disaster Recovery Services; refer to: www.iso.org.
- ISO/IEC 27000:2009: Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary; refer to: www.iso.org.

- ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management Systems – Requirements; refer to: www.iso.org.
- ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management; refer to: www.iso.org.
- ISO/IEC 27004:2009: Information Technology – Security techniques – Information Security Management – Measurement; refer to: www.iso.org.
- ISO/IEC 27005:2008: Information Technology – Security Techniques – Information Security Risk Management; refer to: www.iso.org.
- ISO/IEC TR 18044:2004: Information Technology – Security Techniques – Information Security Incident Management; refer to: www.iso.org.
- IT Infrastructure Library (ITIL) IT Service Management (ITSM); refer to: www.itil-itsm-world.com.
- MAP MAGERIT; refer to: www.csi.map.es/csi/pg5m20.htm.
- Military Deception (JP 3-13.4); refer to: www.dtic.mil/doctrine/new_pubs/jp3_13_4.pdf.
- National Security Agency (NSA); refer to: www.nsa.gov.
- NIST Role-Based Access Control (RBAC); refer to: csrc.nist.gov/rbac.
- NIST SP 800-30: Risk Management Guide for Information Technology Systems, July 2002; refer to: http://csrc.nist.gov/publications/nistpubs.
- NIST SP 800-55: Performance Measurement Guide for Information Security, July 2008; refer to: http://csrc.nist.gov/publications/nistpubs.
- PCI-DSS (PCI Data Security Standard); refer to: www.pcisecuritystandards.org/security_standards/pci_dss.shtml.
- Project Quant; refer to: securosis.com/projectquant.
- OASIS Reference Model for SOA; refer to: www.oasis-open.org.
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), CERT; refer to: www.cert.org/octave.
- Open Web Application Security Project (OWASP); refer to: www.owasp.org.
- Operations Security (JP 3-13.3); refer to: www.dtic.mil/doctrine/new_pubs/jp3_13_3.pdf.
- Risk Taxonomy Technical Standard (C081), published by The Open Group, January 2009; refer to: www.opengroup.org/bookstore/catalog/c081.htm.
- SABSA (Sherwood Applied Business Security Architecture); refer to: www.sabsa-institute.org.

- SANS; refer to: www.sans.org.
- SAS70 (Statement on Auditing Standards No. 70); refer to: sas70.com.
- Serenity Project (EU); refer to: www.serenity-project.org.
- Six Sigma, Motorola; refer to: www.motorola.com/motorolauniversity.jsp.
- Slave Virtual Router Redundancy Protocol (SVRRP); refer to: www.ietf.org/rfc/rfc3768.txt.
- SPSMM (Secure Programming Standards Methodology Manual); refer to: www.isecom.org/projects/spsmm.shtml.
- Standardized Information Gathering, BITS; refer to: www.sharedassessments.org.
- Systems Security Engineering Capability Maturity Model (SSE-CMM); refer to: www.sse-cmm.org.
- TOGAF® 9 (G091), published by The Open Group, February 2009; refer to: www.opengroup.org/bookstore/catalog/g091.htm.
- *The Survivability of Network Systems: An Empirical Analysis*, Cargenie Mellon University, 2000; refer to: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.7080&rep=rep1&type=pdf.

Some of the following have provided valuable ideas for the development of this O-ISM3 standard, so are acknowledged here as influential sources, even though they may not all be directly referenced.

- AEDI CAYSER; refer to: www.aedi.es/cayser/CAYSER.asp.
- American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP); refer to: www.cica.ca.
- Balanced Scorecards; refer to: http://en.wikipedia.org/w/index.php?title=Balanced_scorecard&oldid=360259742.
- Business Process Improvement; refer to: http://en.wikipedia.org/w/index.php?title=Business_process_improvement&oldid=358941230.
- Certified Information Systems Auditor (CISA), ISACA; refer to: www.isaca.org.
- Certified Information Security Manager (CISM), ISACA; refer to: www.isaca.org.
- CISWG Report of the Best Practices and Metrics Teams; refer to: www.educause.edu/ir/library/pdf/CSD3661.pdf.
- *Designing Secure Information Systems and Software: Critical Evaluation of the Existing Approaches and a New Paradigm*, Mikko Siponen, 2002; refer to: http://herkules.oulu.fi/isbn9514267907/isbn9514267907.pdf.

- EA 7/03: EA Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems; refer to: www.european-accreditation.org.
- Events Logging Markup Language (ELML); refer to: www.ISM3.com.
- Federal Information Security Management Act (USA), 2002.
- IETF RFC 2119: Key Words for Use in RFCs to Indicate Requirement Levels; refer to: www.ietf.org/rfc/rfc2119.txt.
- Information Assurance Markup Language (IAML); refer to: www.ISM3.com.
- Information System Security Association (ISSA) Generally Accepted Information Security Principles (GAISP); refer to: www.issa.org.
- ISO 19011:2002: Guidelines for Quality and/or Environmental Management Systems Auditing; refer to: www.iso.org.
- *Mathematical Proofs of Mayfield's Paradox: A Fundamental Principle of Information Security*, University of New Haven; refer to: www.isaca.org/Template.cfm?Section=Home&CONTENTID=17181&TEMPLATE=/ContentManagement/ContentDisplay.cfm.
- NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations, August 1009; refer to: http://csrc.nist.gov/publications/nistpubs.
- OCEG Measurement & Metrics Guide; refer to: www.oceg.org/view/mmg.
- Shewhart-Deming Control Charts; refer to: http://en.wikipedia.org/w/index.php?title=Control_chart&oldid=360041352.
- *Towards Maturity of Information Maturity Criteria: Six Lessons Learned from Software Quality Criteria*, Mikko Siponen, 2002.

Chapter 1

Introduction

1.1 Positioning security management

In the big-picture view of computing systems, we need information security to protect our systems from the risk of threats which have the potential to cause damage. In the business context, information security practitioners generally approach this need by breaking it down into the following areas:

- **Risk Management**: To identify and estimate levels of exposure to the likelihood of loss, so that business managers can make informed business decisions on how to manage those risks of loss by accepting the risk, or by mitigating it, either through investing in appropriate internal protective measures judged sufficient to lower the potential loss to an acceptable level, or by investing in external indemnity. The business managers' decisions here are captured as their Security Policy, which describes how they will manage their IT security.
- **Security Controls**: A business creates and maintains a corporate policy on its goals and objectives that drive its operations, and as part of its IT-dependent operations it uses its risk assessment results to formulate an IT Security Policy that supports and enforces its corporate policy to protect its assets (primarily its most valuable asset – data) and assure its operations are as secure as they need to be for the level of protection required.
- **Security Management**: To support the selection, maintenance, and overall Security Policy for the security controls deployed in a business enterprise. In our increasingly connected world there is also a strong business driver to partner with other organizations, suppliers, customers, and outworkers, and this necessitates establishing mutually agreed security arrangements for sharing data and applications. Other aspects of security management include audit and logging, and regulatory compliance.

An Information Security Management System (ISMS) ensures effective management of security policies and the security measures and controls that support and enforce those policies, to cost-effectively prevent or mitigate the effects of attacks, errors, and accidents that threaten the intended operation

of information systems and the organizational processes they support. This Open Information Security Management Maturity Model (O-ISM3) standard focuses on the common processes of information security, which to some extent all organizations share. ISM3 is technology-neutral, so practitioners may use whatever protection techniques are appropriate to achieve the process objectives and outputs. Just as enterprise architecture processes define the desired operation of information systems, security management processes define operational metrics and their allowable variances.

1.2 Key characteristics of ISM3

A distinctive feature of ISM3 is that it is based on a fully process-based approach to information security management and maturity, on the basis that every control needs a process for managing it. It breaks information security management down into a comprehensive but manageable number of processes, with specifically relevant security control(s) being identified within each process as an essential subset of that process.

ISM3 defines information security management maturity in terms of the operation of an appropriate complementary set of ISM3 information security processes. It defines capability in terms of the metrics and management practices used, and it requires the linking of security objectives and targets to business objectives. Market-driven maturity levels help organizations choose the scale of ISMS most appropriate to their needs. The maturity spectrum facilitates the trade-off of cost, risk, and usability and enables incremental improvement, benchmarking, and long-term targets.

While many information security management approaches see risk assessment as a necessary first stage, and ISM3 can use it as well as any other standard in this field, it does not demand a risk assessment-based approach. In some cases, a business may decide it is not necessary to do a risk assessment to decide it needs a security control. For example, controls can be chosen based on:

- Common-sense
- Best practices (passwords)
- Learning from incidents (better firewalls or AV, maybe)
- A specifically-focused vulnerability or threat analysis

- Client requirements (I don't want users from project A accessing data belonging to my project)

The ISM3 approach offers organizations the flexibility to choose any subset of its information security processes based on various criteria.

Compatibility with ISO 9000 Quality Management
ISM3 uses a process-based and observable metrics-based methodology to manage operational security processes. With similarities in structure and approach to quality management methods like ISO 9000, ISM3 requires the formal articulation of security management processes. This standard includes a baseline ISM, and guidelines for adding processes beyond the minimal system based upon experience of incremental impact upon information security, risk, and cost. It also includes a description of the metrics required to operate and improve the ISMS, and a process capability model and maturity levels that build from all this. ISM3 differs from other security management tools because of its emphasis on the practical and the measurable, which ensures that ISMSs can adapt without re-engineering in the face of changes to technology and risk.

Compatibility with ISO/IEC 27000
ISM3 is compatible in many ways with the ISO/IEC 27000:2009 standard, but it uses a different approach. ISO/IEC 27001:2005 focuses on security management as a single process for what controls are required and in place to build an ISMS, and ISO/IEC 27002:2005 outlines a large number of potential controls and control mechanisms from which to choose to achieve selected control objectives using the guidance provided by ISO/IEC 27001. In contrast, the ISM3 approach is to define and measure what people do in the activities that support security; in this respect we may consider ISO/IEC 27001 to serve an auditor's requirements, while ISM3 meets a manager's needs.

ISM3 uses a different approach to ISO/IEC 27001. It covers this ground and in addition provides a comprehensive framework for selecting, implementing, and managing a set of security processes to meet measurable business goals. It breaks security management down into a number of related activities, in which each security activity is defined as a separate process, with its own related security control(s), documentation, inputs, outputs, metrics,

and linkages to other explicitly defined activities. In so doing it gives the personnel responsible for the operation of each process the required clarity of understanding over its purpose, resources, and reporting to enable them to operate it to best effect.

Compatibility with COBIT

ISM3 implementations use a management responsibilities framework consistent with the ISACA COBIT framework model, which describes best practice in the parent field of IT service management. COBIT provides an over-arching standard applicable to information provision, and for the subset related to security provision, ISM3 offers a framework for security management and the tools to break this down by process, environment, and responsibility.

Compatibility with ITIL

ITIL provides an established toolkit of process-related good practices in the specific fields of IT service delivery and IT service management. ITIL users can use the ISM3 process orientation to strengthen their ITIL security processes. ISM3 also has a potential use in managing outsourced security processes; for example, Service Level Agreements (SLAs) that use an ISM3 approach to operational metrics objectives and targets are specific and measurable (see Chapter 5).

1.3 Potential for certification

There is potential for development of an ISM3 certification program to serve the needs of organizations and the industry where a business case arises for demonstrating conformance to a specific ISM3 security management level of achievement. Certification schemes could be created for:

- Specific ISM3 implementations – their maturity levels (see Section 2.3). Maturity levels are intended to be interoperable across organizations, and to be relevant to Service Level Agreements (SLAs) – see Chapter 5. They can also be used to certify compliance to specified industry norms, as well as to regulatory requirements. An organization certified to a specific level can communicate that certification to a trading partner to give a clear understanding of how their information security is managed.

- ISM3 practitioners, to certify security management professional competence along similar lines to the ISC2-CISSP industry-recognized qualification. This could include Manager, Auditor, and Trainer certifications.

Development activity to create an ISM3 certification program is outside the scope of this OISM3 standard. If and when sufficient business case justifies starting a new project to respond to such a requirement, it will be announced to Open Group Security Forum members as a call for participation, with details posted on the ISM3 public web site at www.opengroup.org/projects/security/ism3/.

1.4 Summary

ISM3 is designed with all kinds of organization in mind. In particular, businesses, non-governmental organizations, and enterprises that are growing or outsourcing may find ISM3 attractive. In summary, ISM3:

- Provides a tool for creating ISMSs that are fully aligned with the business mission and compliance needs
- Applies to any organization regardless of size, context, and resources
- Enables organizations to prioritize and optimize their investment in information security
- Enables continuous improvement of ISMSs using metrics
- Enables metric-driven, verifiable outsourcing of security processes

Chapter 2

Concepts – processes, capability, and maturity

2.1 Defining the key terms

This chapter explains the principal ISM3 concepts of process, capability, and maturity, and how they relate to each other. It also introduces the role of metrics, their different types, and their support for common management practice areas.

- **Process** – The *process* is the smallest, atomic unit of the standard. Everything ISM3 does centers around the concept of the process. Processes have *capabilities* and are managed using *management practices*.
- **Capability** – The *metrics* of a process enable its management practices and reveal its capability. From the point of view of an auditor, a process's *metrics* determine its capability.
- **Maturity** – Selected ISM3 processes collected together and operated at a sufficient capability determine an organization's *information security management maturity* or simply *maturity*. The maturity and the capability levels can be used as a basis for development of a certification scheme, which would be of special value to certification authorities (auditors).

2.1.1 Tying these key terms together

The table below specifies what metrics are needed for a process to achieve each capability level and its respective mapping to management practices.

Metrics enable capability to move from a basic state to an optimized state.

Process capability is determined by the metrics the process produces. Metrics are classified by type. There are five process capability levels: basic, defined, managed, controlled, and optimized. Metrics are classified into seven possible types.

Capability Level		Initial	Managed	Defined			Controlled	Optimized
Management Practices Enabled		Audit, Certify	Test	Monitor	Planning	Benefits Realization	Assessment	Optimization
Documentation		*	*	*	*	*	*	*
Metric Type	Activity		*	*	*	*	*	*
	Scope		*	*	*	*	*	*
	Unavailability[1]		*	*	*	*	*	*
	Effectiveness		*	*	*	*	*	*
	Load			*	*	*	*	*
	Quality						*	*
	Efficiency							*

Table 2.1 Classification of metric types

2.2 Capability levels

Expanding on the definition above, *capability* is a property of how a process is managed. From a managerial perspective, the higher the capability, the more management practices that are applicable, and the more robust, transparent, and self-correcting the process. From an auditor's perspective, the capability achieved by a process depends on the documentation and the metrics used to manage it.

Some factors that help to achieve higher capability levels are a proper distribution of responsibilities, the resources available for the process, and the motivation, skills, accountability, and empowerment of the personnel. (See also Section 2.4.4.)

2.3 Maturity levels

ISM3 maturity levels are specific combinations of ISM3 processes practiced at specified capability levels. Processes are allocated to certifiable maturity levels according to a spectrum, from a basic ISMS to an advanced one. There is a relationship between the number of processes, their capability, and the maturity of the ISMS. The more processes, and the higher the capability, the higher the maturity. The key relationships behind ISM3's maturity levels are:

1 Throughout ISM3, the term "unavailability" is preferred to "availability" because ISM3 in concerned with measuring and reporting unavailability.

- Mapping (or grouping) of processes to each ISM3 maturity level
- Defining a capability for each mapped process at each ISM3 maturity level

The maturity levels are designed to suit the needs of organizations with different:

- Size
- Resources
- Threats
- Impact, both economic and non-financial (e.g., reputation)
- Risk appetite
- Economic sector

Organization types that will be covered include small and medium-sized companies, governmental units, larger enterprises, business process outsourcers (BPOs), e-commerce specialists, organizations and utilities that provide critical infrastructures, cloud and software-as-a-service providers, and outsourced security providers.

2.3.1 Maturity levels and RoI

Maturity-level design takes cost into account by favoring deployment of ISM3 processes that give a high Return on Investment (RoI) at earlier maturity levels. In general, processes implemented at a high capability will render a higher RoI. Note that the marginal RoI is not linear as investment increases, and that an excessive investment in security – beyond the assessed risk cost

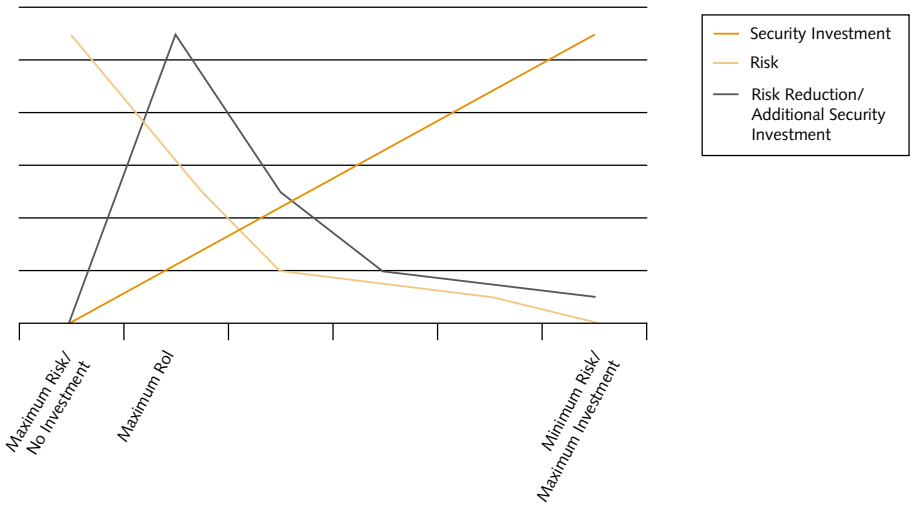

Figure 2.1: The diminishing returns of increased security investment

of loss – can give a negative return. Mayfield's Paradox and a study from Carnegie Mellon[2] shows that as security posture improves, the marginal cost of further improvement also increases.

2.4 Processes

2.4.1 Levels

ISM3 identifies four levels of security management on the basis that each process level reports to the higher one, so it is only the Strategic level that reports to the CIO. If the CIO takes a Tactical level responsibility, this occurs seamlessly.

- Strategic (Direct and Provide), which deals with broad goals, coordination, and provision of resources
- Tactical (Implement and Optimize), which deals with the design and implementation of the ISMS, specific goals, and management of resources
- Operational (Execute and Report), which deals with achieving defined goals by means of technical processes

Plus a fourth Generic level for general management.[3]

ISM3 defines a number of processes – defined in Chapter 4 and listed in Appendix A – which service these levels, and are therefore grouped under these same four level types:[4]

- Generic Processes (GP)
- Strategic-Specific Processes (SSP)
- Tactical-Specific Processes (TSP)
- Operational-Specific Processes (OSP)

2.4.1.1 Generic Processes

Generic Processes provide the essential infrastructure for the implementation, assessment, and improvement of ISMS processes. They comprise:

- Knowledge Management to gather and share security management information across the IMS

2 Carnegie Mellon University: "The Survivability of Network Systems: An Empirical Analysis".

3 The ISM3 approach to adopting these four levels is strongly influenced by the referenced paper "Information Security Governance: Towards a Framework for Action", Business Software Alliance, 2003.

4 "Generic Processes" and "Specific Processes" in ISM3 are akin to the "Generic Practices" and "Specific Practices" in Carnegie Mellon's Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI). Further information is available at www.sei.cmu.edu/cmmi.

- ISMS and Business Audit to validate compliance with internal policies and regulatory requirements
- ISM Design/Evolution to evaluate whether current processes are achieving the security management targets that have been set

For Generic Process definitions, see Section 4.2.

2.4.1.2 Strategic-Specific Processes

Strategic management is responsible for selecting and designing services to provide value within the cost and risk parameters of the organization. Strategic management is accountable to stakeholders for the use of resources through governance arrangements. The customers of strategic management are therefore external and possibly internal stakeholders.

Strategic management fulfils the following specific goals and responsibilities with respect to security:

- Provides leadership and coordination of:
  - Information security
  - Physical security
  - Workplace security (outside the scope of ISM3, because it is a cross-disciplinary (i.e., schools of thought) area concerned with protecting the safety, health, and welfare of people engaged in work or employment)
  - Interaction with organizational units
- Reviews and improves the ISMS, including the appointment of managers and internal and external auditors
- Defines relationships with other organizations, such as partners, vendors, and contractors
- Allocates resources for information security
- Defines security objectives consistent with business objectives, protecting stakeholders' interests
- Defines the organizational scheme of delegation

For strategic management process definitions, see Section 4.3.

2.4.1.3 Tactical-Specific Processes

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 ISMS and for the use of resources.

Tactical management has the following specific goals and responsibilities:

- Provide feedback to strategic management
- Manage budget, people, and other resources allocated to information security
- Define the environment for operational management:
  - Security Targets and Asset Classification
  - Security Architecture and Lifecycle Management
  - Service Level Management (define measurement systems and metrics)
  - Insurance Management
  - Personnel Security
  - Information Operations

For tactical management process definitions, see Section 4.2.2.

2.4.1.4 Operational-Specific Processes

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

Operational management has the following specific goals and responsibilities:

- Provide feedback to tactical management, including incident and metrics reports
- Procure and apply allocated resources efficiently and effectively
- Identify and protect assets within the lifecycle
- Protect and support information systems throughout their lifecycle
- Applying access management and environmental controls for users and services
- Availability management (may be shared with IT Operations Availability Management and IT Service Continuity Management)
- Testing and auditing
- Monitoring and management of the security measures lifecycle
- Carry out processes for incident prevention, detection, and mitigation (both real-time and following an incident)

For operational management process definitions, see Section 4.2.3.

2.4.2 Selecting your set of processes

The set of processes an organization should choose to use for their ISM3 implementation depends on its Security Policy (see Section 1.1), reconciled