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

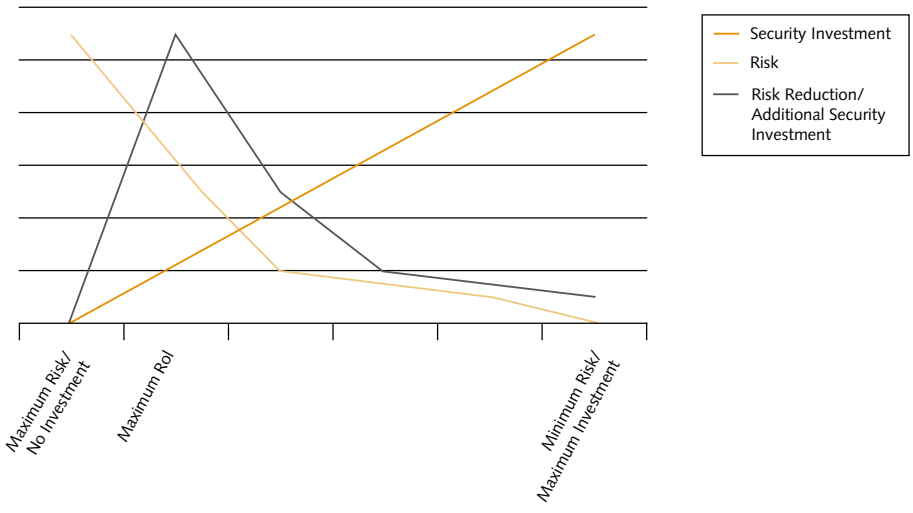

Figure 2.1: The diminishing returns of increased security investment

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

with the resources they have available to invest in security controls and operate their security management function. Chapter 6 provides guidance on getting started with ISM3. Every business has a unique context and resources. Using ISM3, each organization uses a decision-making process to take a subset from the total hierarchy of formal processes. Processes can also run several times in an organization under different process owners or in different IT managed domains.

ISM3 requires every information security process to have an identified process owner. A process owner may delegate operation or maintenance of a process to another role, while retaining responsibility and supervision for the process.

The success, performance, and capability of ISM3 processes are measured by process metrics. Process metrics help to detect abnormal conditions in a process, give a basis for comparison, and aid management decision-making. Chapter 6 includes general guidance on grouping some ISM3 processes by magnitude of investment required and the expected benefit in terms of risk reduction.

2.4.3 Process definition

ISM3 defines a comprehensive set of the information security management processes which are applicable to managing information security. The methodology does not take a prescriptive view of what processes must be used, their frequency of use, or their capability. All of these are driven by business objectives and are management decisions. In using ISM3, users must understand that these processes represent a resource trade-off against other business interests. The methodology gives the user a framework for making these trade-offs and explaining them to stakeholders.

The notation used for ISM3 processes describes certain fundamental properties. These include:

- The level of the organization responsible for each set of processes (strategic, tactical, or operational)
- The value added by the process
- Inputs to the process
- Outputs of the process – these can be documents, such as policies and reports, or they can be the result of recurring events, such as taking back-ups or analyzing log files

Process	Process Code and Name
Description	Summary of the activity performed in the process.
Value	Explanation of the benefit expected from the process.
Documentation	Policies, procedures, and templates. Process definitions needed to describe and perform the process.
Inputs	Inputs to the process (the list of processes that generate the inputs is shown in brackets). Inputs in *italics* are obtained from sources other than documents.
Outputs	Results for the process (the list of processes that use the outputs is shown in brackets). Outputs in *italics* are secondary outputs. **Note I**: Metrics reports should normally be available to the CIO, CEO, CSO, and a representative of the users.
Metric Descriptions	Definition of appropriate measures covering accuracy, precision, and other measurements of output quality (fitness-for-purpose) as appropriate. Activity, scope, load, effectiveness, unavailability, and efficiency metric descriptions are usually not specified in every process definition as they are so similar between processes it would be repetitive to do so. **Note II**: This row is a placeholder for adding rows – one row per type of metric (activity, scope, load, effectiveness, unavailability, etc.) that is relevant to the particular implementation of each process. The metrics used in the implementation of each process are strongly related to the capability built into the process.
Responsibilities	An example of a process owner is given in this row. Note that there can be more than one instance of the process, so every instance will have an individual process owner. Process owners can be a person or a team, so it is possible that a collective of people acting as a team can perform the role of process owner.. The supervisor of the process is normally the 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 is normally an internal or external auditor, or a quality assurance specialist. The role of auditor is incompatible with the supervisor role, the process owner role, and performance of any other process-related duties. Auditor independence should be safeguarded; for example, by rotation. **Note III**: Some practitioners may find the RACI model from COBIT useful for documenting the responsibilities.
Related Processes	Other ISM3 processes that generate required inputs to this process.
Related Methodologies	Well-known methodologies and best practices. The methodologies mentioned may be useful for planning, assessing, implementing, testing, monitoring, auditing, optimizing, and certifying the process.

Table 2.2: ISM3 process template

- Secondary outputs of the process – these are outputs that are qualitative or that are inputs from other processes; for example, the outputs of OSP-19: Internal Technical Audit are Attack Emulation Reports, and the secondary outputs are the vulnerabilities found, which are inputs to OSP-8: Software Development Lifecycle Control

ISM3 processes are defined using the template above (Table 2.2). Adopted ISM3 processes must have all fields in the template defined. The process template can also be used to implement non-ISM3 processes.

Note IV: The process code is just an identifier. The ISM3 process model presents gaps and out-of-numeric-order processes because of deprecated or renamed processes.
Note V: The ISM3 process definitions are included in Chapter 4. All ISM3 processes are indexed in Appendix A.

2.4.4 Process roles and responsibilities

For a responsibility to be carried out properly, the person or team must be:

- Accountable (have a personal stake in the outcome)[5]
- Competent (have the appropriate knowledge and experience)
- Motivated (influenced by a will to succeed)
- Empowered (have resources and the freedom to take decisions and give feedback)

'Division of duty' rules for transparency, partitioning, supervision, rotation, and separation of responsibilities help prevent conflicts of interest and collusions to commit and conceal unauthorized activity, including potentially criminal activity. ISM3 provides the following guidelines on responsibility assignment and process management:

- **Transparency**: Responsibilities and reporting channels should be clearly defined, documented, and communicated. In addition:
  - Strategic ISM reports should be available to stakeholders and their representatives, to the extent deemed appropriate to the laws, regulations, and governance requirements of the organization.
  - Operational ISM reports should be available to tactical and strategic ISM managers.

5 The term "accountable" is used differently in ISM3 than in the RACI model from COBIT.

  - Tactical ISM reports should be available to strategic ISM managers.
- **Partitioning**: All instances of ISM processes should have one and only one process owner. All process owners should be employees of the organization. An owner may contract out some activities related to the process, but ownership should always be held in-house. The process owner may formally delegate a process, but still bears responsibility for the competency and due diligence with which it is performed.
- **Supervision**: All ISM processes should have at least one supervisor. Stakeholder representatives may act as supervisors of strategic ISM vision, to the extent deemed appropriate to the laws, regulations, and governance requirements of the organization:
  - Strategic ISM managers may act as supervisors of tactical ISM processes.
  - Tactical ISM managers may act as supervisors of operational ISM processes.
- **Rotation**: All sensitive processes, especially audits, should be transferred periodically to another competent process owner, even if it is just to cover a 3-4 week holiday period. It should be difficult or impossible to forecast who the next process owner might be.
- **Separation**: Separation of responsibilities helps to prevent internal fraud. In combination with transparency, separation brings accountability to business processes, making clear who is responsible for the outcomes of the process. To ensure separation works in practice, it will normally be necessary to designate an appropriate back-up to every participant in the process, so that if key people are away, the system does not break down.

An appropriate distribution of responsibilities, provision of resources, and the use of ISM3 processes TSP-7 to TSP-11 help to improve personnel performance.

In describing organizational structure, the following definitions are used:
- **Process Owner**: The person or team responsible for performance of a process.
- **Role**: A set of responsibilities assigned to a person or a team (process owner is an example of a role). Roles normally involve: to perform, to supervise, to audit, or being informed about tasks.
- **Organizational Chart**: Diagram of the responsibilities for supervision between roles.
- **Border**: Defines the limits of the organization.

The following roles have special importance in ISM3:

- **Customer**: As in the ITIL definition, a customer is the role who provides resources and sets requirements for a process and a process owner.
- **Strategic Management**: Managers involved in the long-term alignment of IT with business needs.
- **Tactical Management**: Managers involved in the allocation of resources and the configuration and management of the ISMS.
- **Operational Management**: Managers involved in setting up, operating, and monitoring specific processes.

The above definitions recognize that an individual can have more than one role, in relation to different duties. For example, in a small organization, the IT manager may perform ISM duties at strategic, tactical, and operational levels. In ISM3, the terminology is intended to indicate a level of abstraction above the operational role, not the job title or position of an individual. Some roles relevant to organizations are:

- **Stakeholder**: A shareholder, owner, bond holder, non-executive board member, or other, who has a stake in performance of the organization, but no direct role in management.
- **CEO (Chief Executive Officer or Managing Director)**: The senior executive with a strategic role.
- **CIO (Chief Information Officer)**: Manager with a strategic role responsible for the performance and integrity of information systems.
- **CSO (Chief Security Officer)**: Manager with a strategic role responsible for all aspects of organizational security.
- **System Owner**: A manager with a strategic role responsible for a business process reliant on an information system.
- **User**: Someone authorized to use an information system.
- **Information Security Officer**: Manager with tactical responsibility for ISM processes.
- **Business Unit Managers**: Senior-level manager responsible for managing a segment of the organization to successfully achieve business goals and objectives.
- **Human Resources**: The part of the organization that selects, hires, and manages the professional progression of personnel.
- **Facilities**: The part of the organization that takes care of commodities like office space, storage, etc.
- **Data Custodian**: Someone with an operational management role over a repository.

- **Systems Administrator**: Someone with an operational management role over an information system.
- **Authorizer**: Someone permitted by the system owner to authorize system access requests.
- **Authority**: The systems administrator of an access control system.
- **Auditor**: Someone external to the organization checking for compliance on behalf of a process owner or a customer.

Some committees (teams) relevant to organizations are:

- **Executive Security Committee**: Oversees coordination between internal security and partners security, sets the rules on trust for suppliers and vendors:
  - CEO
  - CIO
- **Security Committee**: Oversees coordination between information security, security in the workplace, physical security:
  - CEO
  - CIO
  - CSO
  - Head of Human Resources
  - Facilities Manager
- **Information Security Committee**: Oversees information security:
  - CIO
  - CSO
  - Business Unit Managers

As a guideline, the following related roles should be kept separate (Table 2.3):

Incompatibility
Process Owner and Stakeholder Representative
Process Auditor & Process Owner
Incident Victim & Forensics Investigator
Incident Whistle-blower & Forensics Investigator
GP-2 Process Owner & any other Process Owner
Strategic Process Owner & Operational Process Owner (this incompatibility guarantees supervision)
Authorizer & System Administrator
OSP-19 Process Owner & any other Process Owner

Incompatibility
Physical Access Control Process Owner & Logical Access Control Process Owner
Request Personnel & Select Personnel (to prevent nepotism)
Repository Classifier & Repository User
Information System Owner & System Administrator
Weakness Whistle-blower & Patching Management Process Owner
System Administrator & User
OSP-20 Process Owner & any other Process Owner
Repository Backup Operator & Tape Librarian
Logs Administrator & Logs Keeper
OSP-21, OSP-25 Process Owner & any other Process Owner

Table 2.3 Incompatible roles

2.4.5 Process metrics definition

A metric is a quantitative measurement that can be interpreted and investigated in the context of a series of previous or equivalent measurements. Acting on a process to improve its metrics leads to an improvement in the value added by the process. Metrics are used to promote improvements that increase the value added by a process. While there are many metrics available to support information security governance (see SANS, NIST SP 800-55, and ISO/IEC 27004:2009), ISM3 focuses on the ones that are relevant to process management. Any process metric that reflects strongly the value added by a process can be used as a Key Performance Indicator (KPI). Process metrics can be used in Service Level Agreements (SLAs) and underpinning contracts. Process metrics are valuable when they are used to improve the consistency with which a process is carried out. If causes of variation are identified and the system improved, the process metric will improve too. The improvement cycle can be used to increase efficacy and reduce risk and cost.

Each process has a set of default metrics for each output produced. Some metrics, such as process scope, may be exactly the same for all outputs. A default metric should be used only when it assists the management of the process. A process is not required to produce all its default metrics. Metrics produced are information, which carry a production cost and perhaps an obligation to respond or report. Management must determine which metrics are cost-effective, and it must determine what to do with the information once collected, including feeding back to inform decisions on revising the organization's Security Policy.

ISM3 defines the following types of metrics (Table 2.4):

Type of Metric	Description
Activity	Number of outputs produced. *Statistics* (mean age, time between outputs, time between input and output, etc.).
Scope	Proportion of all input units covered by the process. Proportion of all inputs sampled or tested.
Unavailability	Number of interruptions to the normal operation of the process. Frequency of interruptions to the normal operation of the process. *Statistics* (mean interval between interruptions, frequency of interruptions, etc.). Uptime of normal operation of the process.
Effectiveness	Number of inputs. Mean time between inputs. Fraction of inputs that produce an output.
Efficiency	Ratio of the number of outputs submitted to the available resources for this process in actual use. Ratio of the proportion of all input units covered by this process to the available resources for this process in actual use. Ratio of the proportion of input units sampled or tested to the available resources for this process in actual use.
Load	Proportion of resources in actual use.
Quality	Accuracy, precision, or other measurements of fitness-for-purpose of the output.

Table 2.4: Various types of metric used in ISM3

As noted above, metrics are used in the context of a series of measurements. Statistical analysis – such as the mean, the variance, and the confidence limit – is used to determine trends, measure quality, and show improvement.

2.4.6 Process metrics specification

For a metric to be fully defined, the following items must be specified (Table 2.5):

Metric	Name of the metric.
Metric Type	Activity, scope, unavailability, effectiveness, load, quality, or efficiency.
Metric Description	Description of what is measured.
Measurement Procedure	How the metric is measured.
Measurement Frequency	How often is the measurement taken.
Thresholds Estimation	How the thresholds are calculated.
Thresholds Accuracy	Proportion of true positives and true negatives.
Current Thresholds	Current range of values considered normal for the metric.
Target Value	Best possible value of the metric.
Units	Units of measurement.
Categories	Name and description of every category or subdivision.

Table 2.5: Specification of a metric

The ISM3 process model only gives the metric description. ISM3 adopters determine the nature, frequency, and precision of measurement. However, while metrics can be compared if their metric specifications are very similar, metrics reports are not easily compared because they are strongly dependent on implementation issues, making benchmarking or other direct comparisons difficult.

ISM3 metrics sustain, enhance, and enable critical management practices already present in the organization.

Performance assessment process metrics are used to provide feedback on the performance of management practices, including the following.

Knowledge Management
The practice of keeping records, promoting agreement, and sharing knowledge, usually based on documentation.

Implementation
Practice performed when no operational management system or management process exists. Implementation uses information from an assessment of the organization's goals and existing informal management practices to design an appropriate management system or process.

Operation
The routine practice for executing a process that normally implies the following:

- **Testing**: Assessment of whether process outputs are as expected when test data is input.
- **Monitoring**: Checking whether the outputs of the process and the resources used are within normal range in order to detect significant anomalies.
- **Improving**: Making changes in the process to make it more suitable for the purpose, or to reduce usage of resources. Removing faults before they produce incidents, bottlenecks that hamper performance, and making trade-offs are examples of process improvements. This management practice needs information gained from evaluating, testing, or monitoring the process. The gains from the changes (if any) can be measured with subsequent testing, monitoring, or evaluation.
- **Planning**: Organizing and forecasting the amount, assignment, and milestones of tasks, resources, budget, deliverables, and performance of a process.

Evaluation
Required periodically to assess the outcomes of the ISMS:

- **Assessment**:
  - How well the process matches the organization's needs and compliance goals expressed as security objectives
  - How changes in the environment or management decisions in a process change the quality, performance, and use of resources of the process
  - Whether bottlenecks or single points of failure exist
  - Points of diminishing returns
  - Benchmarking of processes between process instances and other organizations
  - Trends in quality, performance, and efficiency

- **Audit**: Checks are made on whether the process inputs, activities, and results match their documentation.
- **Certify**: Certification evaluates whether process documentation, inputs, outputs, and activities comply with a predefined standard, law, or regulation. The certificate provides independent proof of compliance that third parties can trust.
- **Benefits Realization**: Shows how achieving security objectives contributes to achieving business objectives, measures the value of the process for the organization, or justifies the use of resources.

2.4.7 Process metrics operational use

There are five steps in the use of metrics: measurement, interpretation, investigation, representation, and diagnosis, as follows.

Measurement

The measurement of the current value of the metric is periodic and normally refers to a window; for example: "9:00pm Sunday reading of the number of viruses cleaned in the week since the last reading". Measurements from different sources and different periods need to be normalized before integration in a single metric.

Interpretation

The meaning of a measured value is evaluated comparing the value of a measurement with a threshold, comparable measurement, or target. Normal values (those within thresholds) are estimated from historic or comparable data.

The results of interpretation are:

- **Anomaly**: When the measurement is beyond acceptable thresholds.
- **Success**: When the measurement compares favorably with the target.
- **Trend**: General direction of successive measurements relative to the target.
- **Benchmark**: Relative position of the measurement or the trend with peers.

Incidents or poor performance take process metrics outside normal thresholds. Shewhart-Deming control charts are useful to indicate whether the metric value is within the normal range, as values within the arithmetic

mean plus/minus twice the standard deviation make more than 95.4% of the values of a normally distributed population. Fluctuations within the "normal" range would not normally be investigated.

Investigation
The investigation of abnormal measurements ideally ends with identification of the common cause; for example, changes in the environment or results of management decisions, or a special cause (error, attack, accident) for the current value of the metric.

Representation
Proper visualization of the metric is key for reliable interpretation. Metrics representation will vary depending on the type of comparison and distribution of a resource. Bar charts, pie charts, and line charts are most commonly used. Colors may help to highlight the meaning of a metric, such as the green-amber-red (equivalent to on-track, at risk, and alert) traffic-light scale. Units, the period represented, and the period used to calculate the thresholds must always be given for the metric to be clearly understood. Rolling averages may be used to help identify trends.

Diagnosis
Managers should use the results of the previous steps to diagnose the situation and analyze alternatives and their consequences, to arrive at appropriate business decisions.

- Fault in Plan-Do-Check-Act cycle leading to repetitive failures in a process: Fix the process.
- Weakness resulting from lack of transparency, partitioning, supervision, rotation, or separation of responsibilities (TPSRSR): Fix the assignment of responsibilities.
- Technology failure to perform as expected: Change or adapt the technology.
- Inadequate resources: Increase resources or adjust security targets.
- Security target too high: Revise the security target if the effect on the business would be acceptable.
- Incompetence, dereliction of duty: Take disciplinary action.
- Inadequate training: Institute immediate and/or long-term training of personnel.

- Environment change: Make improvement to adapt the process to the new conditions.
- Previous management decision: Check if the results of the decision were sought or unintended.
- Error: Fix the cause of the error.
- Attack: Evaluate whether the protection against the attack can be improved.
- Accident: Evaluate whether the protection against the accident can be improved.

Chapter 3

ISM3 in a business context

3.1 Business context

ISM3 is a framework for managing information security in the context of business objectives. The ISM3 practitioner analyzes the impact of information security on achieving business objectives and makes this analysis visible to management through the development of security objectives and targets. This analysis forms the basis for documenting Security Policy for the organization.

While the agreed objectives describe intent, security targets describe tolerance for deviation. For critical objectives, the tolerance of deviation in related security targets is likely to be very low. For aspirational objectives, targets with a wide tolerance can be set. While incidents are any occasion of an objective not being met, only deviation from a security target gives rise to a security management failure. ISM3 processes provide the means of managing information security.

An organization using ISM3 recognizes that there is a trade-off between information security and other business interests, and requires business and security management to work together. When ISM3 is implemented correctly, management works collaboratively towards the same goals, with less friction between the security function and other business units.

ISM3 provides an objective and measurable framework for managing information security. All objectives and security targets are expressed in tangible, specific, and measurable terms from which management is able unambiguously to conclude whether the security management system is succeeding or failing.

Security managers face a difficult challenge in justifying their security decisions to stakeholders. If there are no security incidents, stakeholders may feel there is over-investment in security. If there is a serious incident, a review might suggest that the Security Manager's assessment of a particular area

of risk was wrong. Security Managers stand to take the blame for security breaches, while success is measured as "no significant security breaches" so goes unrecognized. The root of this challenge is a lack of clarity and agreement over what security means in practice. ISM3 addresses this by using operational definitions of security. Instead of conceptual definitions of important terms, such as confidentiality, availability, and integrity, ISM3 uses operational definitions, which say how they may be achieved. This means there is a need for dialog between the Security Manager and their business managers to work out what matters (business and security objectives), how they should be measured (security targets), and the escalation threshold for declaring a major problem (an ISMS failure).

3.2 Security-in-context model

The ISM3 security-in-context model gives the Security Manager a methodology to translate the business outcomes for security into the technical specifications of the security system. The overall structure of the security-in-context model, explained in detail in the subsequent sections in this chapter, is described in the figure below:

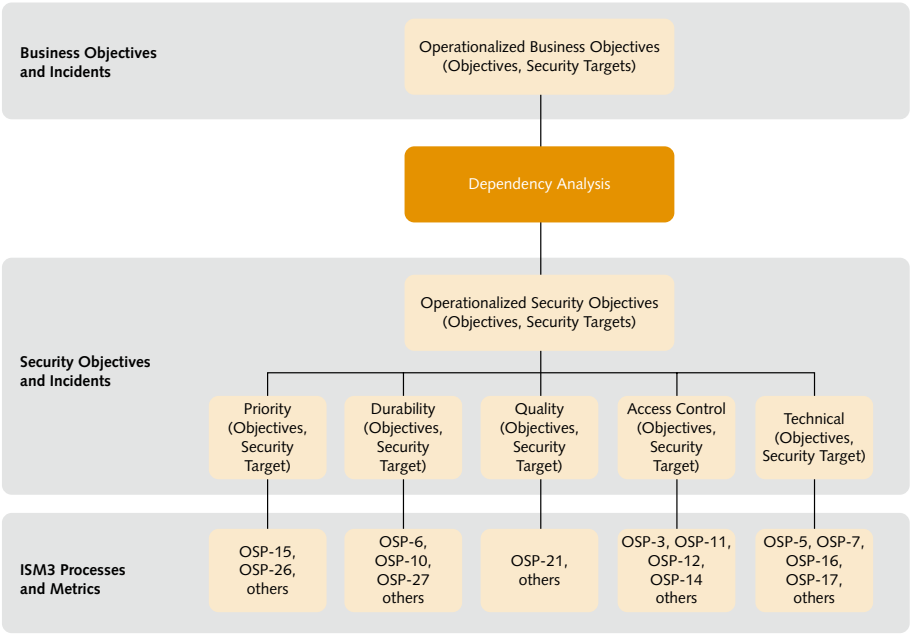

Figure 3.1: ISM3 security-in-context model

3.3 Operational approach

ISM3's operational approach defines an incident as a failure to achieve one or more of management's agreed business and security objectives. An ISMS failure occurs when a security target is breached. A state of security exists when all objectives are continually met within their security target tolerances in spite of threats.

When business objectives and security objectives are aligned, information security becomes a key contributor to the common goal of achieving the business objectives. The progress towards better security is measurable in terms of increasing predictability of achieving the security objectives. The alignment also assists in the resolution of resource trade-offs, where decisions are taken over whether to invest in security at the expense of other parts of the business. Investment is less likely to be driven by the most recent incident or threat. There is recognition that security is not invulnerability to all attacks, but rather is an economically efficient level of invulnerability given competing claims upon business resources.

3.4 Operational definitions

ISM3 aims to ease communication between security, IT, and business managers, Therefore, in creating security objectives and targets, operational terms and measures are used where possible. ISM3 avoids traditional security concepts, such as confidentiality, availability, and integrity, because there is a temptation to use them as shorthand, and that leads to misunderstanding. While security targets are necessarily specific and detailed, the use of operational terms helps to remove ambiguity and the potential for misunderstanding. As an example, instead of a general security objective like "maintaining the confidentiality of information", ISM3 states how confidentiality is achieved in operational terms, such as physical and logical access control, user enrolment, and audit trail. An example of an operational definition in this context would be: "Use of services, information repositories, and systems is restricted to authorized users.".

Terms used in ISM3 are described in Appendix B. This includes the component-based model used by ISM3 to describe in plain terms the key elements of IT architecture.

3.5 ISM3 definition – security-in-context

ISM3 defines security as "the result of *continuously* meeting or exceeding a set of objectives". Because business objectives differ between organizations, the security-in-context approach makes security in ISM3 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 the abstract information properties of *confidentiality, availability, or integrity*. Under security-in-context, an incident is a failure to meet the *organization's objectives*, which are expressed as business objectives and security objectives.

This definition implies that an event, which is classified as an incident at one organization, may not be classified as an incident at another. For example, an organization, or an IT managed domain that handles no secret information, may not classify the viewing of its files by an unauthorized party as an incident.

ISM3 focuses on achieving business and security objectives. Protection of assets is important insofar as it furthers the achievement of security objectives.

3.6 Business objectives, security objectives, and security targets

3.6.1 Business objectives

Every organization exists for specific purposes that require it to set goals and meet certain obligations. Business objectives, ranging from aspirational goals to regulatory compliance, may originate internally, or be imposed by an external party such as the government. Their achievement depends on many factors, one being information security. Every business objective in ISM3 is operationally defined. Some examples of business objectives are:

- Paying the payroll on the 1st of every month
- Paying all incoming invoices within a certain timeframe
- Paying taxes on time

- Delivering the products and services when and where committed by the organization
- Keeping all necessary records to pass any audit successfully (i.e., tax audit, software license audit, etc.)
- Preventing breach of contractual agreements
- Protecting intellectual property and legal rights
- Invoicing all products and services provided

3.6.2 Security objectives

ISM3 documents the contribution of information security towards meeting business objectives through using a *dependency analysis*. The output of the dependency analysis is a list of *security objectives* that form the basis for design, implementation, and monitoring of the ISMS. They also form the business objectives for the security component when planning enterprise architecture. Security objectives, derived from business objectives, state explicitly how information security contributes to business objectives.

Some examples of security objectives derived from the business objective "Invoicing all products and services provided" are:

- Invoices are accessible only to the Accountancy and Collection teams.
- Paid invoices are kept for three years and destroyed after no more than four years.
- The system registers the user name, date, and time every time an invoice is created.
- The system is available 9 to 5 Monday to Friday, with no more than five interruptions per week, with a duration of no more than one hour in total, and causing delay to billing of no more than 15 invoices.
- Fewer than five errors per hundred invoices.
- More than 99.8% of products served are invoiced.
- The license for the system is up-to-date.
- Personal information held in the invoicing system is registered at the Data Protection Agency and held appropriately.
- The system is not visible to systems outside the company.
- The system is hosted internally in the data center under controlled environmental conditions that provide reasonable safeguards against fire, flood, etc.

ISM3 defines five categories of security objectives:

- **Priority Security Objectives** determine what *availability* means for the business. Examples are backup and identification of single points of failure. Resources are allocated according to the priority of protected services, interfaces, and channels. In a multi-tiered information system, the priority of user-facing services is propagated to the lower-level services they depend on.
- **Durability Security Objectives** relate to the generic term *integrity* and include the planned retention and destruction of information in accordance with policy and business objectives. Durability objectives are supported by archiving and secure disposal techniques.
- **Information Quality Objectives** also relate to *integrity* and include precision (or accuracy), relevance (how up-to-date information is), completeness, and consistency of repositories. Information quality objectives usually rely upon quality control techniques, but may also include access control, accountability, authorization, and audit techniques as well. The information quality of a repository is a measure of its fitness in fulfilling security objectives.
- **Access Control Objectives** ensure that the business requirements for *confidentiality* of protected information (e.g., secrets, personal information, licensed, copyrighted, patented, and trademarked information) are clearly understood by the business. Access control requires the identification and management of authorized users, and typically includes enrolment, role management, segregation, accountability, authorization, and logging techniques for its implementation and control.
- **Technical Security Objectives** cover the underlying architecture of information systems, and are a step remote from direct impact on the business. Technical security objectives typically include operational objectives for the data center's safety, reliability, power, as well as the IT managed domain, including software patching and upgrading, maintenance processes, and vulnerability management and resilience to compromise and misuse. Technical security objectives usually depend upon data center infrastructure, technologies such as firewalls, anti-virus, intrusion detection and prevention, and processes such as patch management and secure configuration. Failure to meet technical security objectives puts all other (business and security) objectives at risk, but does not necessarily create a business objective failure itself.

3.6.3 Security targets

As well as expressing security objectives in terms of what matters to the business, ISM3 defines the tolerable deviations. All ISM3 objectives (business and security) must include their *security target*. This is the maximum deviation from the desired outcome that management tolerates before taking corrective action. ISM3 can support any specified variance. This enables the ISM3 program to support and manage both aspirational objectives (whose allowable deviations may be very high) and critical objectives (where there is usually a very narrow compliance range).

Security targets are normally defined in terms of frequency of occurrence and threshold cost, as the allowable business impact of failing to meet objectives reflects the trade-off against other priorities and objectives. Security targets show what the organization expects for its information security investment. Put another way, management's act of defining security targets also specifies its risk appetite, or the variance tolerance of its objectives.

Security objectives and their targets may vary between IT managed domains (subdivisions of a logical, technical, or organizational partition under a single management), geographic locations, or business units depending on local context, specific protection requirements, cost structures, and use of technology. The threshold values set for each security target may be different for each. This allows a tighter set of targets to be established for more sensitive IT managed domains and helps to ensure that the ISMS is tailored to the needs of each IT managed domain in an organization. Similarly, different organizations in the same sector are likely to have different security objectives. As a result, a statement of security objectives must be created and maintained for each IT managed domain of the organization.

3.6.4 Examples

The tables in this section offer examples of business objectives and security objectives for priority security, information quality, access control, and technical issues, and their related security targets. These are only examples, provided here to clarify the concepts. ISM3 practitioners must define for themselves each ISM3 managed business objective, its dependent security objectives, and security targets. Note that business objectives include internal and external (compliance) objectives.

Sample Business Objectives	Sample Security Targets
Paying the payroll on the 1st of every month.	Less than one failure per two years.
Paying taxes on time.	Less than one failure per ten years. Penalties of less than 0.1% of the accounting value of the company.
Invoice all products and services provided.	Fewer than ten incidents per year. Loss is less than 0.1% of the accounting value of the company.
Deliver the products and services when and where committed by the organization.	Fewer than ten incidents per year. Loss is less than 0.1% of the accounting value of the company.
Online booking availability.	Fewer than five incidents every year where online booking is unavailable for one hour or more between 0800 and 1700 hours or simultaneous users are reduced to 50 or less. Loss is less than 0.1% of the accounting value of the company.
Online booking reliability.	Fewer than two incidents where interruptions are more than two or add up to more than 15 minutes any working day. Loss is less than 0.1% of the accounting value of the company.
Online booking volatility.	Fewer than two incidents per month where more than five minutes of transactions are lost because of a service interruption. Loss is less than 0.1% of the accounting value of the company.
Tax information retention.	Less than one incident every year where more than 1% of data with a five years' retention requirement is lost. Loss is less than 0.1% of the accounting value of the company.
Old customers information expiry.	Fewer than two incidents every year where more than 1% of expired data is recoverable. Loss is less than 0.1% of the accounting value of the company.
Precision of customer addresses.	Fewer than two incidents every year where more than 0.5% of customer addresses are wrong or outdated any working day. Loss is less than 0.1% of the accounting value of the company.

Sample Business Objectives	Sample Security Targets
Third-party services and repositories appropriately licensed.	Fewer than ten incidents every year where an improperly licensed service or repository is used. Loss is less than 0.1% of the accounting value of the company.
Personal information collected proportional to its use.	Fewer than two incidents every year where personal data is collected without a business purpose. Loss is less than 0.1% of the accounting value of the company.
Personal information held for no longer than required.	Fewer than two incidents every year where more than 0.1% of personal records are retained beyond their expiry date. Loss is less than 0.1% of the accounting value of the company.
Tax records kept for a minimum number of years.	Fewer than two incidents every year where more than 0,1% of tax records are lost. Loss is less than 0.1% of the accounting value of the company.
Personal information is protected using the mandated security measures.	Fewer than five incidents every year where mandatory security measures are found to be missing. Loss is less than 0.1% of the accounting value of the company.
Owner of personal information agrees for it to be collected, and has the right to check it and fix it and approve how it will be used.	Fewer than ten incidents every year where a personal record is not handled appropriately. Loss is less than 0.1% of the accounting value of the company.
Repositories with personal information registered with the Data Protection agency.	Less than one incident every two years where a repository is not registered. Loss is less than 0.1% of the accounting value of the company.

Table 3.1: Sample business objectives and security targets

Priority Security Objectives	Sample Priority Security Targets
Availability: The period of time when a service, repository, interface, or channel must exist, be accessible, and usable (perform according to customer needs) upon demand according to or exceeding customer needs.	Nine hours per day every working day between 0800 and 1700 hours for ten years serving 100 simultaneous users. Loss is less than 0.1% of the accounting value of the company.
Reliability: The longest time and number of times in the availability (performance) time a service, repository, interface, or channel can be interrupted according to or exceeding customer needs.	Two times for a total time of 15 minutes per day during working hours. Loss is less than 0.1% of the accounting value of the company.
Volatility: The oldest recent messages and information that can be lost because of an interruption of service, channel, or interface according to or exceeding customer needs.	1,000 transactions lost per interruption. Five minutes of information and transactions per interruption. Loss is less than 0.1% of the accounting value of the company.

Table 3.2: Sample priority security objectives and targets

Durability Security Objectives	Sample Durability Security Targets
Retention Period: The minimum length of time a repository is kept (preserved) according to or exceeding customer and regulatory requirements.	Five years since creation. Loss is less than 0.1% of the accounting value of the company.
Expiry: The date the expired or end of lifecycle repositories and records should be permanently and reliably destroyed according to or exceeding customer and regulatory requirements. Those with personal information of customers and employees often require a specific expiry date.	10 years since end of use. Loss is less than 0.1% of the accounting value of the company.

Table 3.3: Sample durability security objectives and targets

Information Quality Security Objectives	Sample Information Quality Security Targets
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.	98% of subscriber lines installed are in the invoicing database. Loss is less than 0.1% of the accounting value of the company.
Personal information completeness must be proportional to its use.	Fewer than 20 incidents every year. Loss is less than 0.1% of the accounting value of the company.
The owner of personal information must agree for it to be collected and has the right to check it, fix it, and approve how it will be used or ceded.	Fewer than 20 incidents every year. Loss is less than 0.1% of the accounting value of the company.
The owner of personal information will be given notice when personal data is collected, including who is collecting the data.	Fewer than 20 incidents every year. Loss is less than 0.1% of the accounting value of the company.
Personal information must be used for the purpose agreed with the information owner.	Fewer than five incidents every year. Loss is less than 0.1% of the accounting value of the company.
Personal information must not be disclosed without the agreement of the information subject.	Fewer than five incidents every year. Loss is less than 0.1% of the accounting value of the company.
Personal information owners will have means to make data collectors accountable for their use of personal information.	Fewer than five incidents every year. Loss is less than 0.1% of the accounting value of the company.

Table 3.4: Sample information quality security objectives and targets

Access Control Security Objectives	Sample Access Control Security Targets
Granting the use of services and interfaces and access to repositories to authorized users.	Fewer than 25 incidents per year. Loss is less than 0.1% of the accounting value of the company.
Denying the use of services and interfaces and access to repositories to unauthorized users.	Fewer than 10 incidents per year. Loss is less than 0.1% of the accounting value of the company.
Express the will and intent about a repository of the owner of a user account or certificate.	Fewer than 20 incidents per year. Loss is less than 0.1% of the accounting value of the company.

Access Control Security Objectives	Sample Access Control Security Targets
Accurate recording of: • Interface ID and location • User account or certificate ID • Signature • Type of access attempt • Date and time of access attempt • Access attempt result • Repository, interface, service, or message accessed	Fewer than 10 incidents per year. Loss is less than 0.1% of the accounting value of the company.
Personal information is accessible to authorized users only and is held for no longer than required.	Fewer than 20 incidents per year. Loss is less than 0.1% of the accounting value of the company.
Secrets are accessible to authorized users only.	Fewer than three incidents per year. Loss is less than 0.1% of the accounting value of the company.
Third-party services and repositories are appropriately licensed and accessible only to authorized users.	Fewer than five incidents per year. Loss is less than 0.1% of the accounting value of the company.
Information systems are physically accessible only to authorized users.	Fewer than five incidents per year. Loss is less than 0.1% of the accounting value of the company.
Repositories are accessed by authorized users only.	Fewer than 10 incidents per year. Loss is less than 0.1% of the accounting value of the company.

Table 3.5: Sample access control security objectives and targets

Technical Security Objectives	Sample Technical Security Targets
Systems are as free of weaknesses as possible.	Average update level in the production IT domain within one week or less.
Systems that need to be visible to not trusted systems are the least visible possible.	Less than 10 unused ports discovered during penetration testing per year.
Systems run trusted services only.	The medium update level of antivirus is below one day.
The electricity, temperature, and humidity where systems operate exceed the systems needs.	Electricity reliability is over 99,9999%. Temperature doesn't exceed 25 degrees for more than five minutes a day. Humidity exceeds upper limit of 80% for less than 10 minutes a day.

Table 3.6: Sample technical security objectives and targets

TIP: The following list of questions can help to investigate security objectives and targets of a system:

System Access

- Who are the users of the system?
- Do they need to be specifically authorized?
- From whom do we want to protect the system's information?
- Will any part of the system be located in publicly accessible locations?

System Compliance

- Will the system handle personal information of clients, potential clients, stockholders, or employees?
- If parts of the system are installed in different locations, which parts are subject to different regulations in terms of handling of personal information and data breach disclosure?
- Will the system use licensed information from third parties?
- If parts of the system are installed in different locations, which of those parts are subject to different licensed information regulations?
- Will the system handle intellectual property?
- If parts of the system are installed in different locations, which of those parts are subject to different intellectual property regulations?

System Operation Quality

- When should the system be performing normally (e.g., 8 hours per day for the 5 working days of the week, or 24x7, etc.)?
- How many interruptions are acceptable?
- What would be the longest acceptable interruption?
- What is the maximum number of transactions that can be lost because of an interruption?
- For how long will the system's data be archived?
- If the data needs to be deleted, when should this happen?
- What is the maximum acceptable percentage of records with wrong information?
- What is the maximum percentage of records that can be missing?

3.7 ISM3 interpretation of incidents, success, and failure

ISM3 uses business and security objectives and security targets as the criteria to determine both the occurrence of incidents and the overall success of an ISM. An *incident* is recognized every time a business or security objective is not met. Determining an incident's impact upon business objectives should include both direct and indirect impacts:

- Direct impact:
  - Lost sales or service penalties
  - Cost to return the system to the pre-incident state, including re-creation of the information
  - Cost of maintaining business-as-usual during the incident
  - Property damage and loss
  - Others, such as financial penalties, higher insurance premiums, liability in the event of litigation
- Indirect impact:
  - Damage to image, brand, or reputation
  - Capital impairment, perhaps in the form of lost goodwill
  - Loss of trust
  - Treasury/cashflow implications
  - Breach of contract, statutory, or regulatory legal obligations
  - Breach of ethical codes of conduct
  - Breach of social and moral obligations
  - Breach of professional, regulatory, or statutory responsibilities

The occurrence of an incident, however, does not by itself mean that the ISMS has failed. ISM3 defines *success* as the achievement of the security target relating to that objective, not whether an incident has or has not occurred. Meeting all security targets throughout the year, for example, would mean that the ISMS has been successful for that entire year, regardless of any incidents that occurred during that period.

ISM3 defines *failure* as the opposite of success; that is, one or more business targets or security targets were not met. There are two failure modes relevant to managing information security:

1. Failure to meet a security target of a security objective.
   All failures of this type are failures of the ISMS, regardless of whether business objectives were met in spite of the failure. Failure to meet this category of security target puts the success of achieving a business objective at risk of failure as described in the dependency analysis.

2. Failure to meet a security target of a business objective.
   Not all failures of this type are failures of information security management. Failures to meet the security target or business objectives require further analysis to determine whether information security was the root cause of missing the target. When information security played no part in failing to achieve the business objective, there was no failure of the ISMS. However, if information security was the cause, then business and security management must review and revise the dependency analysis to reflect new knowledge of how success in achieving business objectives depends upon information security management. They must also revise security objectives and targets based upon this knowledge, and adapt the ISMS itself to achieve the new security targets predictably.