SECURITY SERIES

Risk Management

The Open Group Guide

Van Haren Publishing

THE Open GROUP

Risk Management
The Open Group Guide

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.

Risk Management

The Open Group Guide

Colofon

Title:	Risk Management - The Open Group Guide
A Publication of:	The Open Group
Authors:	The Open Group
Editors:	Ian Dobson and Jim Hietala
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN:	978 90 8753 663 3
Edition:	First edition, first impression, April 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

Preface

This book has been developed by **The Open Group,** 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.

Trademarks

Acknowledgements

Part 1: The Open Group Technical Standard: Risk Taxonomy
The Open Group gratefully acknowledges the contribution of:
- Alex Hutton, CEO, Risk Management Insight
- Jack Jones, CTO, Risk Management Insight

for contributing their FAIR (Factor Analysis of Information Risk) development work into the Security Forum of The Open Group, and their continued support in guiding the Security Forum members through The Open Group development and approval process to publish this Risk Taxonomy standard. The Open Group also acknowledges the members of its Security Forum who contributed to its development.

Part 2: The Open Group - Technical Guide
Requirements for Risk Assessment Methodologies
The Open Group gratefully acknowledges the contribution of:
- Alex Hutton, CEO, Risk Management Insight (www.riskmanagementinsight.com)

- Jack Jones, CTO, Risk Management Insight and the members of The Open Group Security Forum who contributed to its development.

Part 3: The Open Group Technical Guide FAIR–ISO/IEC 27005 Cookbook

The Open Group gratefully acknowledges the contribution of lead authors:
- Christopher Carlson, The Boeing Company
- Alex Hutton, Risk Management Insight, with the valued support of contributing author
- Anastasia Gilliam, Independent Consultant and the members of The Open Group Security Forum who contributed to its development.

References

The following documents are referenced in Part 1: The Open Group Technical Standard: **Risk Taxonomy**:

- An Introduction to Factor Analysis of Information Risk (FAIR), Risk Management Insight LLC, November 2006; refer to www.riskmanagementinsight.com.
- Methods for the Identification of Emerging and Future Risks, European Network and Information Security Agency (ENISA), November 2007; refer to www.enisa.europa.eu/doc/pdf/deliverables/EFR_Methods_Identification_200804.pdf.
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), US-CERT; refer to www.cert.org/octave.
- A Taxonomy of Computer Program Security Flaws, with Examples, Naval Research Laboratory, September 1994; refer to http://chacs.nrl.navy.mil/publications.

The following documents are referenced in Part 2: The Open Group Technical Guide: **Requirements for Risk Assessment Methodologies**:

- COBIT (Control Objectives for Information and related Technology), Information Systems Audit and Control Association (ISACA); refer to www.isaca.org
- COSO (Committee of Sponsoring Organizations) Enterprise Risk Management Framework; refer to www.coso.org
- ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management

- ITIL (Information Technology Infrastructure Library); refer to www.itil-officialsite.com/home
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation); refer to www.cert.org/octave
- Risk Taxonomy Technical Standard, January 2009 (ISBN: 1-931624-77-1, C081), published by The Open Group
- FAIR - ISO/IEC 27005 Cookbook Technical Guide, November 2010 (ISBN: 1-931624-87-9, C103), published by The Open Group

The following documents are referenced in Part 3: The Open Group **Technical Guide FAIR–ISO/IEC 27005 Cookbook:**

- ISO/IEC 27005:2008: Information Technology – Security Techniques – Information Security Risk Management.
- ISO/IEC 27001:2005: Information Technoloy – Security Techniques – Information Security Management System – Requirements (ISMS)
- ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management (Controls)
- Technical Standard: Risk Taxonomy (C081, ISBN: 1-931624-77-1), January 2009, published by The Open Group
- Technical Guide: Requirements for Risk Assessment Methodologies (G081, ISBN: 1-931624-78-X), January 2009, published by The Open Group

Contents