

# Risk Management

## The Open Group Guide



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](http://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](http://www.vanharen.net), or [freezone.vanharen.net](http://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](http://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](mailto:info@vanharen.net)

© All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

The views expressed in this document are not necessarily those of any particular member of The Open Group.

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](mailto: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](http://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](http://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](http://www.opengroup.org/bookstore).

## Trademarks

Boundaryless Information Flow™ is a trademark and ArchiMate®, Jericho Forum®, Making Standards Work®, Motif®, 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 registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute.

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

OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a registered trademark of CERT at Carnegie Mellon University (see [www.cert.org/octave](http://www.cert.org/octave)).

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

### 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](http://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](http://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](http://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](http://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](http://www.isaca.org)
- COSO (Committee of Sponsoring Organizations) Enterprise Risk Management Framework; refer to [www.coso.org](http://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](http://www.itil-officialsite.com/home)
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation); refer to [www.cert.org/octave](http://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 Technology – 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

Preface ..... V

Acknowledgements..... VI

References .....VII

Introduction .....XIII

## Part 1 The Open Group Technical Standard

Risk Taxonomy ..... 1

**Chapter 1 Introduction to risk taxonomy** ..... 2

1.1 Scope ..... 2

1.2 Purpose/objective..... 3

1.3 Context..... 3

1.4 The risk language gap..... 3

1.5 Using FAIR with other risk assessment frameworks..... 5

1.5.1 The ability of a FAIR-based approach to complement other standards ..... 5

1.5.2 An example: using FAIR with OCTAVE ..... 5

1.5.3 Conclusion ..... 6

**Chapter 2 Business case for a risk taxonomy** ..... 7

2.1 What makes this the standard of choice?.....9

2.2 Who should use this Technical Standard? ..... 10

2.3 Related dependencies.....11

**Chapter 3 Risk management model** ..... 12

3.1 Risk assessment approach..... 12

3.2 Why is a tightly-defined taxonomy critical? ..... 12

**Chapter 4 Functional aspects** ..... 13

4.1 What is defined? ..... 13

4.2 What is in/out of scope and why? ..... 13

4.3 How should it be used? ..... 13

<b>Chapter 5 Technical aspects</b>	<b>14</b>
5.1 Risk taxonomy overview .....	14
5.2 Component definitions.....	15
5.2.1 Risk.....	15
5.2.2 Loss Event Frequency (LEF) .....	15
5.2.3 Threat Event Frequency (TEF) .....	16
5.2.4 Contact.....	16
5.2.5 Action.....	17
5.2.6 Vulnerability.....	17
5.2.7 Threat Capability .....	19
5.2.8 Control Strength (CS).....	19
5.2.9 Probable Loss Magnitude (PLM) .....	20
5.2.10 Forms of loss .....	21
5.2.11 Loss factors.....	22
5.2.12 Primary loss factors.....	23
5.2.13 Secondary loss factors.....	26
 <b>Chapter 6 Example application</b>	 <b>31</b>
6.1 The scenario.....	31
6.2 The analysis: FAIR basic risk assessment methodology.....	31
6.2.1 Stage 1: Identify scenario components .....	32
6.2.2 Stage 2: Evaluate Loss Event Frequency (LEF) .....	33
6.2.3 Stage 3: Evaluate Probable Loss Magnitude (PLM) .....	36
6.2.4 Stage 4: Derive and articulate risk.....	41
6.3 Further information.....	42
 <b>Appendix A Risk taxonomy considerations</b>	 <b>43</b>
A.1 Complexity of the model .....	43
A.2 Availability of data .....	44
A.3 Iterative risk analyses .....	44
A.4 Perspective .....	45

## **Part 2** The Open Group Technical Guide

### **Requirements for risk assessment methodologies**

47

#### **Chapter 1 Introduction to requirements for risk assessment methodologies** 48

1.1	Business case for risk assessment methodologies .....	48
1.2	Scope .....	49
1.3	Using this Technical Guide .....	49
1.4	Definition of terms .....	49
1.5	Key operating assumptions.....	50

#### **Chapter 2 What makes a good risk assessment methodology?** 51

2.1	Key component: taxonomy.....	51
2.2	Key risk assessment traits .....	51
2.2.1	Probabilistic.....	51
2.2.2	Accurate.....	52
2.2.3	Consistent (repeatable).....	53
2.2.4	Defensible .....	53
2.2.5	Logical.....	53
2.2.6	Risk-focused.....	54
2.2.7	Concise and meaningful.....	54
2.2.8	Feasible.....	54
2.2.9	Actionable.....	55
2.2.10	Prioritized.....	55
2.2.11	Important note.....	55

#### **Chapter 3 Risk assessment methodology considerations** 56

3.1	Use of qualitative versus quantitative scales .....	56
3.1.1	When is using numbers not quantitative?.....	57
3.2	Measurement scales .....	57
3.2.1	Nominal scale.....	57
3.2.2	Ordinal scale .....	57
3.2.3	Interval scale .....	57
3.2.4	Ratio scale.....	58
3.2.5	Important note.....	58

3.3	How frequent is ‘likely’?.....	58
3.4	Risk and the data owners.....	59

## **Chapter 4 Assessment elements** **60**

4.1	Identifying risk issues .....	60
4.1.1	Interviews and questionnaires .....	60
4.1.2	Testing.....	61
4.1.3	Sampling .....	62
4.1.4	Types of sampling.....	62
4.2	Evaluating the severity/significance of risk issues.....	62
4.3	Identifying the root cause of risk issues.....	63
4.4	Identifying cost-effective solution options.....	63
4.5	Communicating the results to management .....	64
4.5.1	What to communicate .....	64
4.5.2	How to communicate.....	64

# **Part 3** The Open Group Technical Guide

## **FAIR–ISO/IEC 27005 Cookbook** **67**

### **Chapter 1 Introduction to the FAIR–ISO/IEC 27005 Cookbook** **68**

1.1	Purpose.....	68
1.2	Scope .....	68
1.3	Intended audience .....	68
1.4	Operating assumptions.....	69
1.5	Using this Cookbook .....	69

### **Chapter 2 How to manage risk** **70**

2.1	Information Security Management System (ISMS) overview .....	70
2.2	How FAIR plugs into the ISMS.....	72
2.3	Major differences in approach .....	76
2.4	Recommended approach .....	78
2.5	Points to consider .....	78
2.5.1	Concerns about the complexity of the model.....	78
2.5.2	Availability of data to support statistical analysis.....	79
2.5.3	The iterative nature of risk analyses .....	79