SECURITY SERIES

The Open FAIR™ Body of Knowledge

A Pocket Guide

A Taxonomy and Method for Risk Analysis

Van Haren PUBLISHING

THE Open GROUP

Andrew Josey et al.

THE OPEN FAIR^{TM} BODY OF KNOWLEDGE – A POCKET GUIDE

The Open Group Publications available from Van Haren Publishing

The TOGAF Series:
TOGAF® Version 9.1
TOGAF® Version 9.1 – A Pocket Guide
TOGAF® 9 Foundation Study Guide, 3rd Edition
TOGAF® 9 Certified Study Guide, 3rd Edition

The Open Group Series:
The IT4IT™ Reference Architecture, Version 2.0 – A Pocket Guide
Cloud Computing for Business – The Open Group Guide
ArchiMate® 2.1 – A Pocket Guide
ArchiMate® 2.1 Specification
ArchiMate® 2 Certification – Study Guide

The Open Group Security Series:
Open Information Security Management Maturity Model (O-ISM3)
Open Enterprise Security Architecture (O-ESA)
Risk Management – The Open Group Guide
The Open FAIR™ Body of Knowledge – A Pocket Guide

All titles are available to purchase from:
www.opengroup.org
www.vanharen.net
and also many international and online distributors.

The Open FAIR™ Body of Knowledge

A POCKET GUIDE

A Taxonomy and Method for Risk Analysis

Prepared by Andrew Josey et al.

THE Open GROUP

Van Haren PUBLISHING

Title:	The Open FAIR™ Body of Knowledge – A Pocket Guide
Subtitle:	A Taxonomy and Method for Risk Analysis
A publication of:	The Open Group
Authors:	Andrew Josey et al.
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN Hard copy:	978 94 018 0018 1
ISBN eBook:	978 94 018 0561 2
ISBN ePub:	978 94 018 0562 9
Edition:	First edition, first impression, November 2014 First edition, second impression, December 2015
Layout and Cover design:	CO2 Premedia, Amersfoort-NL
Copyright:	© 2014 The Open Group

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

In the event of any discrepancy between text in this document and the official Open FAIR documentation, the Open FAIR documentation remains the authoritative version for certification, testing by examination, and other purposes. The official Open FAIR documentation can be obtained online at www.opengroup.org/certifications/openfair.

The Open FAIR® Body of Knowledge – A Pocket Guide

Document Number: G144

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

This Document

This document is the Pocket Guide for the Open FAIR Body of Knowledge. It is designed to provide a reference for Risk Analysts.

The Open FAIR Body of Knowledge provides a taxonomy and method for understanding, analyzing, and measuring information risk. The outcomes are more cost-effective information risk management, greater credibility for the information security profession, and a foundation from which to develop a scientific approach to information risk management. This allows organizations to:

- Speak in one language concerning their risk
- Consistently study and apply risk analysis principles to any object or asset
- View organizational risk in total
- Challenge and defend risk decisions

The audience for this Pocket Guide is:

- Individuals who require a basic understanding of the Open FAIR Body of Knowledge
- Professionals who are working in roles associated with a risk analysis project, such as those responsible for information system security planning, execution, development, delivery, and operation
- Risk analysts who are looking for a first introduction to the Open FAIR Body of Knowledge

A prior knowledge of risk analysis is advantageous but not required.

The Pocket Guide is structured as follows:

- Chapter 1 (Introduction) provides an introduction to the Open FAIR Body of Knowledge.

- Chapter 2 (Basic Risk Analysis Concepts) introduces the basic concepts of risk analysis.
- Chapter 3 (Risk Taxonomy) describes the Open FAIR taxonomy of terms used for risk analysis.
- Chapter 4 (Risk Terminology) describes the terminology of risk analysis.
- Chapter 5 (Measurement) describes how risk analysis can be best measured.
- Chapter 6 (Risk Analysis Process) describes the process of risk analysis.
- Chapter 7 (Risk Analysis Results) describes how to develop and interpret Open FAIR risk analysis results.

Conventions Used in this Pocket Guide

The following conventions are used throughout this Pocket Guide in order to help identify important information and avoid confusion over the intended meaning.

- Ellipsis (…)
  Indicates a continuation; such as an incomplete list of example items, or a continuation from preceding text.
- **Bold**
  Used to highlight specific terms.
- *Italics*
  Used for emphasis. May also refer to other external documents.

About The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 400 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community – customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers – to:

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices

- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

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

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

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

About the Authors

Andrew Josey, The Open Group

Andrew Josey is Director of Standards within The Open Group. He is currently managing the standards process for The Open Group, and has recently led the standards development projects for the ArchiMate 2.1 Specification and the TOGAF 9.1 Standard, IEEE Std 1003.1 2013 Edition (POSIX), and the core specifications of the Single UNIX Specification, Version 4. He is a member of the IEEE, USENIX, UKUUG, and the Association of Enterprise Architects (AEA).

Jack Jones, CISSP, CISM, CISA

Jack Jones has specialized in information security and risk management for 21 years. During this time, he has worked in the US military, government intelligence, consulting, as well as the financial and insurance industries. Jack has over eight years of experience as a CISO, with five of those years at a Fortune 100 financial services company. His work there was recognized in 2006 when he received the 2006 RSA/ISSA Excellence in the Field of Security Practices award. In 2007, he was selected as a finalist for the Information Security Executive of the Year, Central US, and in 2012 was honored with the CSO Compass award for leadership in risk management. He is also the author and creator of the Factor Analysis of Information Risk (FAIR) framework.

Jim Hietala, The Open Group

Jim Hietala, CISSP, GSEC, Open FAIR Certified Risk Analyst, is Vice President, Security for The Open Group, where he manages all security and risk management programs and standards activities, including the Security Forum. He has participated in the development of numerous industry standards including the Risk Taxonomy (O-RT) standard, Risk Analysis (O-RA) standard, O-ISM3, and O-ACEML. He also led the development of The Open Group FAIR Certification Program. He holds a BS in Marketing from Southern Illinois University, and holds three technical security certifications, GSEC-Gold from GIAC/SANS, CISSP from ISC2, and Open FAIR from The Open Group.

Trademarks

ArchiMate®, DirecNet®, Jericho Forum®, Making Standards Work®, Open FAIR®, OpenPegasus®, The Open Group®, TOGAF®, and UNIX® are registered trademarks and Boundaryless Information Flow™, Build with Integrity Buy with Confidence™, Dependability Through Assuredness™, FACE™, Open Platform 3.0™, Open Trusted Technology Provider™, and The Open Group Certification Mark™ are trademarks of The Open Group.

FAIR™ is a trademark of CXOWARE Inc., used with permission.

All other brand, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

Acknowledgements

The Open Group gratefully acknowledges:

- Past and present members of The Open Group Security Forum for developing the Open FAIR Body of Knowledge.
- CXOWARE Inc., for their valued original work, which we have drawn on in preparation of this Study Guide.
- The following reviewers of this document:
  - Steve Else
  - Bill Estrem
  - Jack Freund
  - Chad Weinman

References

The following documents are referenced in this Pocket Guide:

- *How to Measure Anything: Finding the Value of Intangibles in Business*, Douglas W. Hubbard, John Wiley & Sons, 2010.
- *Open Group Guide: FAIR – ISO/IEC 27005 Cookbook* (C103), published by The Open Group, November 2010; refer to www.opengroup.org/bookstore/catalog/c103.htm.
- *Open Group Guide: Requirements for Risk Assessment Methodologies* (G081), published by The Open Group, January 2009; refer to www.opengroup.org/bookstore/catalog/g081.htm.
- *Open Group Standard: Risk Analysis* (O-RA) (C13G), published by The Open Group, October 2013; refer to www.opengroup.org/bookstore/catalog/c13g.htm.
- *Open Group Standard: Risk Taxonomy* (O-RT), Version 2.0 (C13K), published by The Open Group, October 2013; refer to www.opengroup.org/bookstore/catalog/c13k.htm.

The following web links are referenced in this Pocket Guide:

- The Open Group Risk Management information website; refer to www.opengroup.org/subjectareas/security/risk.

Chapter 1 Introduction

This Pocket Guide provides a first introduction to the Open FAIR Body of Knowledge. It will be of interest to individuals who require a basic understanding of the Open FAIR Body of Knowledge, and professionals who are working in roles associated with a risk analysis project, such as those responsible for information system security planning, execution, development, delivery, and operation.

This chapter provides an introduction to the Open FAIR Body of Knowledge.

Topics addressed in this chapter include:

- An Introduction to risk analysis and the Open FAIR Body of Knowledge
- The need for an accurate model and taxonomy
- A simple risk analysis scenario
- The benefits of using the Open FAIR Body of Knowledge
- The constituent parts of the Open FAIR Body of Knowledge
- The relationship of Open FAIR to other Open Group standards and to other risk frameworks and methodologies

1.1 An Introduction to Risk Analysis and the Open FAIR

The Open FAIR Body of Knowledge provides a taxonomy (see Chapter 3) and method (see Chapter 5, Chapter 6, and Chapter 7) for understanding, analyzing, and measuring information risk. It allows organizations to:

- Speak in one language concerning their risk using the standard taxonomy and terminology

- Consistently study and apply risk analysis principles to any object or asset
- View organizational risk in total
- Challenge and defend risk decisions

What does FAIR stand for?
FAIR is an acronym for Factor Analysis of Information Risk.

1.1.1 Risk Analysis: The Need for an Accurate Model and Taxonomy

Organizations seeking to analyze and manage risk encounter some common challenges. Put simply, it is difficult to make sense of risk without having a common understanding of both the factors that (taken together) contribute to risk, and the relationships between those factors. The Open FAIR Body of Knowledge provides such a taxonomy.

Here's an example that will help to illustrate why a standard taxonomy is important. Let's assume that you are an information security risk analyst tasked with determining how much risk your company is exposed to from a "lost or stolen laptop" scenario. The degree of risk that the organization experiences in such a scenario will vary widely depending on a number of key factors. To even start to approach an analysis of the risk posed by this scenario to your organization, you will need to answer a number of questions, such as:

- Whose laptop is this?
- What data resides on this laptop?
- How and where did the laptop get lost or stolen?
- What security measures were in place to protect the data on the laptop?
- How strong were the security controls?

The level of risk to your organization will vary widely based upon the answers to these questions. The degree of overall organizational risk posed by lost laptops must also include an estimation of the frequency of occurrence of lost or stolen laptops across the organization.

In one extreme, suppose the laptop belonged to your CTO, who had IP stored on it in the form of engineering plans for a revolutionary product in a significant new market. If the laptop was unprotected in terms of security controls, and it was stolen while he was on a business trip to a country known for state-sponsored hacking and IP theft, then there is likely to be significant risk to your organization. On the other extreme, suppose the laptop belonged to a junior salesperson a few days into their job, it contained no customer or prospect lists, and it was lost at a security checkpoint at an airport. In this scenario, there's likely to be much less risk. Or consider a laptop which is used by the head of sales for the organization, who has downloaded Personally Identifiable Information (PII) on customers from the CRM system in order to do sales analysis, and has his or her laptop stolen. In this case, there could be Primary Loss to the organization, and there might also be Secondary Losses associated with reactions by the individuals whose data is compromised.

The Open FAIR Body of Knowledge is designed to help you to ask the right questions to determine the asset at risk (is it the laptop itself, or the data?), the magnitude of loss, the skill level and motivations of the attacker, the resistance strength of any security controls in place, the frequency of occurrence of the threat and of an actual loss event, and other factors that contribute to the overall level of risk for any specific risk scenario.

1.1.2 Scenario – A Bald Tire

We will look in detail at the Open FAIR taxonomy and method in subsequent chapters, starting with the risk taxonomy that enables us to speak in one language concerning risk. Before we do that we use the following scenario as a first introduction to some of the key concepts of risk analysis.

1. Consider a scenario of a bald tire; it is so bald you can hardly see any tread on it. How much risk is associated with that tire?
2. The tire is now hanging from a rope attached to a tree. How much risk is there?
3. You notice that the rope attached to the tree is badly frayed. How much risk is there?
4. The bald tire is hanging from the badly frayed rope over the edge of a cliff with jagged rocks at the bottom.

What are the threats, vulnerabilities, and risk within this scenario?

Many readers assume that the risk is highest in 4. The answer, however, is that there is very little probability of significant loss given the scenario as described. Who cares that an empty, old bald tire falls to the rocks below? Many readers assume that someone will climb up and swing on the tire. This is a reasonable assumption and illustrates that assumptions are easy to make when performing a risk analysis. Unexamined assumptions about key aspects of the risk environment can seriously weaken an analysis.

A first point we take away from this scenario is that the risk landscape is so complex that we must make assumptions – there will always be assumptions in any analysis. What is most important when using the Open FAIR method is that we document, examine, and challenge our assumptions to ensure we can effectively communicate and defend our results.

The second point from this scenario is that multiple readers will typically provide different descriptions of what constitutes the threat, vulnerability, and risk in this scenario. Some readers describe the frayed rope as a threat, vulnerability, and risk. Similarly, other readers describe the jagged rocks as threat, vulnerability, and risk. The simple fact is that, up to this point, we have not adopted standard definitions for these terms. This lack of agreement on terms is important when trying to communicate effectively, especially with executive management.

The Open FAIR taxonomy introduces a standard set of definitions for these terms that will be described in more detail in later sections of this document.

So, what are the asset, threat, vulnerability, and risk components within the bald tire scenario? The definitions and rationale are described more specifically further on, but, simply stated:

- The asset is the bald tire.
- The threat is the earth and the force of gravity that it applies to the tire and rope.
- The potential vulnerability is the frayed rope (disregarding the potential for a rotten tree branch, etc.).

An *asset* is what you want to protect. It can be money, buildings, human life, etc. In the context of information risk, we can define asset as any data, device, or other component of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss.

The question is often asked whether corporate reputation is an asset. Clearly, reputation is an important asset to an organization, yet it does not qualify as an information asset given our definition. Yes, reputation can be damaged, but that is a downstream outcome of an event rather than the primary asset within an event. For example, reputation damage can result from public disclosure of sensitive customer information, but the primary asset in such an event is the customer information.

A *threat* acts directly against the asset. The threat can steal money, burn buildings, and kill people; etc. A reasonable definition for threat is anything (e.g., object, substance, human, etc.) that is capable of acting against an asset in a manner that can result in harm. A tornado is a threat, as is a flood, as is a hacker. The key consideration is that threats apply the force (water, wind, exploit code, etc.) against an asset that can cause a loss event to occur.

Vulnerability is a derived value. An example of a derived value is Speed = Time x Distance. Vulnerability is computed by comparing Threat Capability (Tcap) to Resistance Strength (RS). When Tcap is greater than RS we are "vulnerable". When Tcap is less than RS we are not vulnerable.

You may have wondered why "potential" is emphasized when we identified the frayed rope as a potential vulnerability. The reason it's only a potential vulnerability is that we first have to ask the question: "Vulnerable to what?". If our frayed rope still had a tensile strength of 2,000 pounds per square inch, its vulnerability to the weight of a tire would, for all practical purposes, be virtually zero. If our scenario had included a squirrel gnawing on the frayed rope, then he also would be considered a threat, and the rope's hardness would determine its vulnerability to that threat. A steel cable (even a frayed one) would not be particularly vulnerable to our furry friend. The point is that vulnerability is always dependent upon the type and level of force being applied. Vulnerability is also not simply a Yes or No answer, it is a derived value and assets typically have some level of vulnerability. As an example, consider how vulnerable people are to catching a common cold. It can vary. Different people have various factors that influence how vulnerable they may be (e.g., age, sleep, stress, health, immune system, etc.).

What about risk? Which part of the scenario represents risk? The fact is that there is not a single component within the scenario that can be pointed to and identified as the risk. Risk is not a thing – we cannot see it, touch it, or measure it directly. Similar to speed, which is a derived value, risk is a derived value – risk equals the probable frequency and probable magnitude of future loss – in formal terms risk is derived from the combination of Threat Event Frequency (TEF), Vulnerability (Vuln), and asset value and liability characteristics.

1.1.3 Why use the Open FAIR Body of Knowledge?

The following are five reasons why you should use Open FAIR Body of Knowledge for risk analysis:

1. Emphasis on risk

   Often the emphasis in such analyses is placed on controls; for example, we have a firewall protecting all our customer information – but what if the firewall is breached and the customer information stolen or changed? By using the Open FAIR Body of Knowledge, the analyst emphasizes the risk, which is what management cares about.
2. Logical and rational framework

   It provides a framework that explains the how and why of risk analysis. It improves consistency in undertaking analyses.
3. Quantitative

   It's easy to measure things without considering the risk context – for example, the systems should be maintained in full patch compliance – but what does that mean in terms of loss frequency or the magnitude of loss? The Open FAIR taxonomy and method provide the basis for meaningful metrics.
4. Flexible

   It can be used at different levels of abstraction to match the need, the available resources, and available data.
5. Rigorous

   There is often a lack of rigor in risk analysis: statements are made such as: "that new application is high risk, we could lose millions …" with no formal rationale to support them. The Open FAIR risk analysis method provides a more rigorous approach that helps to reduce gaps and analyst bias. It improves the ability to defend conclusions and recommendations.

1.2 The Open FAIR Body of Knowledge

The Open FAIR Body of Knowledge consists of the following Open Group standards:

- **Risk Taxonomy (O-RT), Version 2.0** (C13K, October 2013) defines a taxonomy for the factors that drive information security risk – Factor Analysis of Information Risk (FAIR).
- **Risk Analysis (O-RA)** (C13G, October 2013) describes process aspects associated with performing effective risk analysis.

The Open Group has also published the following additional risk analysis guidance, which may be useful to risk practitioners, and provide additional background information for those seeking Open FAIR Foundation certification:

- **The Open Group Guide: Requirements for Risk Assessment Methodologies** (G081, January 2009) identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements.
- **The Open Group Guide: FAIR – ISO/IEC 27005 Cookbook** (C103, November 2010) describes in detail how to apply the Factor Analysis of Information Risk (FAIR) methodology to ISO/IEC 27005.

1.2.1 Relationship to Other Open Group Standards

The Open FAIR Body of Knowledge provides a model with which to decompose, analyze, and measure risk. Risk analysis and management is a horizontal enterprise capability that is common to many aspects of running a business. Risk management in most organizations exists at a high level as Enterprise Risk Management, and it exists in specialized parts of the business such as project risk management and IT security risk management. Because the proper analysis of risk is a fundamental requirement for different areas of Enterprise Architecture (EA), and for IT system operation, the Open FAIR Body of Knowledge can be used to support several other Open Group standards and frameworks.

The TOGAF® Framework

In the TOGAF 9.1 standard, risk management is described in Part III: ADM Guidelines and Techniques. Open FAIR can be used to help improve the measurement of various types of risk, including IT security risk, project risk, operational risk, and other forms of risk. Open FAIR can help to improve architecture governance through improved, consistent risk analysis and better risk management. Risk management is described in the TOGAF framework as a necessary capability in building an EA practice. Use of the Open FAIR Body of Knowledge as part of an EA risk management capability will help to produce risk analysis results that are accurate and defensible, and that are more easily communicated to senior management and to stakeholders.

O-ISM3

The Open Information Security Management Maturity Model (O-ISM3) is a process-oriented approach to building an Information Security Management System (ISMS). Risk management as a business function exists to identify risk to the organization, and in the context of O-ISM3, information security risk. Open FAIR complements the implementation of an O-ISM3-based ISMS by providing more accurate analysis of risk, which the ISMS can then be designed to address.

O-ESA

The Open Enterprise Security Architecture (O-ESA) from The Open Group describes a framework and template for policy-driven security architecture. O-ESA (in Sections 2.2 and 3.5.2) describes risk management as a governance principle in developing an enterprise security architecture. Open FAIR supports the objectives described in O-ESA by providing a consistent taxonomy for decomposing and measuring risk. Open FAIR can also be used to evaluate the cost and benefit, in terms of risk reduction, of various potential mitigating security controls.

O-TTPS

The O-TTPS standard, developed by The Open Group Trusted Technology Forum, provides a set of guidelines, recommendations, and requirements that help assure against maliciously tainted and counterfeit products throughout commercial off-the-shelf (COTS) information and communication technology (ICT) product lifecycles. The O-TTPS standard includes requirements to manage risk in the supply chain (SC_RSM). Specific requirements in the risk management section of O-TTPS include identifying, assessing, and prioritizing risk from the supply chain. The use of the Open FAIR taxonomy and risk analysis method can improve these areas of risk management.

The ArchiMate® Modeling Language

The ArchiMate modeling language, as described in the *ArchiMate Specification*, can be used to model EAs. The ArchiMate Forum is also working to extend the ArchiMate language to include modeling security and risk. Basing this risk modeling on the Risk Taxonomy (O-RT) standard will help to ensure that the relationships between the elements that create risk are consistently understood and applied to enterprise security and risk models.

O-DA

The O-DA standard (Dependability Through Assuredness), developed by The Open Group Real-time and Embedded Systems Forum, provides the framework needed to create dependable system architectures. The requirements process used in O-DA requires that risk be analyzed before developing dependability requirements. Open FAIR can help to create a solid risk analysis upon which to build dependability requirements.

1.2.2 Relationship to Other Risk Frameworks and Methodologies

The practice of risk analysis and management is supported by a number of industry standards and frameworks. These include general standards and frameworks that deal specifically with enterprise risk management, such as:

- ISO 31000
- COSO Enterprise Risk Management
- SABSA
- COBIT

In addition, there are a number of industry, national, and international standards and frameworks that deal specifically with information security risk analysis and management such as CRAMM, FRAP, OCTAVE, NIST 800-30, and ISO 27001 and ISO 27005. While it is beyond the scope of this section to describe how the Open FAIR standards relate to each of these, Open FAIR supports many of them by providing a consistent means to effectively measure and analyze risk. Open FAIR is most often used to quantitatively measure risk (although it can be used in support of qualitative risk analysis as well). The Risk Taxonomy (O-RT) standard and the Risk Analysis (O-RA) standard describe the "how" of risk analysis at a deeper level than most of these other standards and frameworks, and as such can be used in concert with them to create solid risk analysis in support of risk management programs based on these frameworks. To map specific Open FAIR elements, processes, inputs, and outputs to ISO 27005, The Open Group Security Forum created a detailed mapping guide: the *FAIR – ISO/IEC 27005 Cookbook*.