An Introduction to the Open FAIR™ Body of Knowledge

A Taxonomy and Method for Risk Analysis

Version 1.1

A White Paper by:

John Linford, The Open Group
Andrew Josey, The Open Group
Jim Hietala, The Open Group
Jack Jones, (formerly of) CXOWARE, Inc.

September 2022

An Introduction to the Open FAIR™ Body of Knowledge: A Taxonomy and Method for Risk Analysis, Version 1.1
Document No.: W148

Published by The Open Group, June 2014
Updated in September 2022 to align with updates to the Open FAIR™ Body of Knowledge.
Any 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 email to:
ogpubs@opengroup.org

Table of Contents

Boundaryless Information Flow™
achieved through global interoperability
in a secure, reliable, and timely manner

Executive Summary

The Open FAIR Body of Knowledge provides a taxonomy and method for understanding, analyzing, and measuring information risk. It 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, and challenge and defend risk decisions.

This document 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 to 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.

The vision for The Open Group is Boundaryless Information Flow™, achieved through global interoperability in a secure, reliable, and timely manner. The Open FAIR Body of Knowledge, as described in The Open Group Standard for Risk Analysis (O-RA) and The Open Group Standard for Risk Taxonomy (O-RT), supports this vision by providing a methodology with which to analyze risk, including IT security risk. Gaining an understanding of risk is critical to both security and Boundaryless Information Flow.

Introduction

The Open FAIR Body of Knowledge provides a taxonomy and method for risk analysis, that enables understanding, analyzing, and measuring information risk. It allows organizations to:

- Speak in one language with well-defined terms concerning their risk
- Consistently study and apply risk analysis principles to any object or Asset
- View organizational risk in total
- Measure risk associated with information and information systems in the same economic terms as other enterprise risks
- Challenge and defend risk decisions

What does FAIR Stand For?

FAIR is an acronym for Factor Analysis of Information Risk.

The Open FAIR Body of Knowledge

The Open FAIR Body of Knowledge consists of two standards:

- **The Open Group Standard for Risk Analysis (O-RA)** [C20A 2021] describes process aspects associated with performing effective risk analysis
- **The Open Group Standard for Risk Taxonomy (O-RT)** [C20B 2021] provides a standard definition and taxonomy for information security risk, as well as information regarding how to use the taxonomy

The Open FAIR Body of Knowledge is supported by multiple other publications, describing the risk analysis process, providing examples of analyses, and demonstrating fit within risk assessment frameworks. For a full list of publications related to or supporting the Open FAIR Body of Knowledge, visit: https://publications.opengroup.org/security-library/risk-analysis.

Risk Analysis: The Need for an Accurate Model and Taxonomy

Organizations seeking to analyze, communicate about, 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.

As an example to illustrate why a standard taxonomy is important, 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 amount of risk that the organization experiences in such a scenario will vary 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 based upon the answers to these questions. The degree of overall organizational risk posed by lost laptops must also include an estimate of the frequency of occurrence of lost or stolen laptops across the organization and the impact of the loss of a stolen laptop.

In one extreme, suppose the laptop belonged to your Chief Technical Officer (CTO), who had Intellectual Property (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. At the other extreme, suppose that 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 Transportation Security Administration (TSA) checkpoint at an airport. In this scenario there is 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 Customer Relationship Management (CRM) system in order to do sales analysis and has the laptop stolen. In this case, there could be a direct loss to the organization, but there might also be losses associated with reactions by the individuals whose data is compromised.

The risk analysis method within 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 actions and of an actual Loss Event, and other factors that contribute to the overall level of risk for any specific risk scenario.

Why Use the Open FAIR Body of Knowledge?

The following are five reasons why you should use the 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 network traffic – but what if the firewall is breached and customer information within the network 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 analyses. It improves consistency in undertaking analyses.
3. **Quantitative**: It is easy to measure things without considering the risk context; for example, if systems are not maintained in full patch compliance, what does that mean in terms of loss frequency or the magnitude of loss? The Open FAIR risk taxonomy and risk analysis method provides the basis for meaningful quantitative 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 that improves the ability to defend conclusions and recommendations.

Relationship to Other Standards of The Open Group

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 (ERM), 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 and for IT system operation, the Open FAIR risk taxonomy and risk analysis method can support several other standards of The Open Group and frameworks as well as other industry schema.

Because the Open FAIR Body of Knowledge is a risk analysis framework and taxonomy, it is easily and readily usable within risk assessments and as part of risk management, regardless of the type of risk being analyzed. Therefore, when other standards, frameworks, schema, etc. require completion of a risk analysis but do not specify *how* that risk analysis must be completed, the Open FAIR Body of Knowledge provides the means to produce a defensible and consistent quantitative estimate of risk. This supports making better decisions based on risk, improves communication on risk to management, and allows comparisons of costs and benefits in business terms.

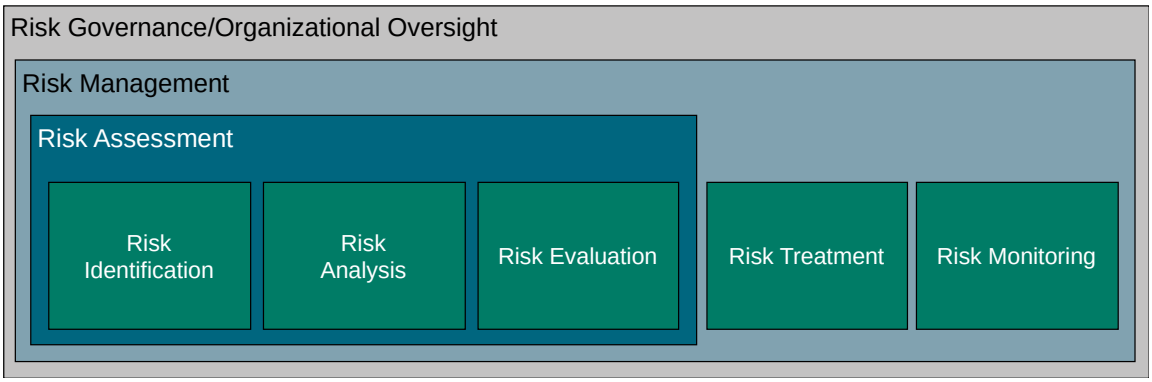

Figure 1: Risk Analysis in Context

Among the standards of The Open Group, the Open FAIR Body of Knowledge can be immediately used within the following:

- The TOGAF® Standard [TOGAF 2022]
- Open Information Security Management Maturity Model (O-ISM3) [C17B 201]
- Open Enterprise Security Architecture (O-ESA) [G112 2011]
- The Open Trusted Technology Provider™ Standard (O-TTPS) [C185-1 2018, C185-2 2018]
- The ArchiMate® Standard [C197 2019]

- Dependability Through Assuredness™ (O-DA) Framework [C13F 2013]

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 ERM, such as:

- ISO 31000:2018: Risk Management – Guidelines [ISO 31000]
- COSO Enterprise Risk Management (ERM)
- 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:

- CCTA Risk Analysis and Management Method (CRAMM)
- Facilitated Risk Analysis Process (FRAP)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
- NIST SP 800-30: Guide for Conducting Risk Assessments [NIST 800-30]
- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27001: Information Security Management [ISO/IEC 27001] and ISO 27005: Information Security Risk Management [ISO/IEC 27005]

While it is beyond the scope of this document to describe how the Open FAIR Body of Knowledge relates to each of these, the Open FAIR Body of Knowledge supports many of them by providing a consistent means to effectively measure and analyze risk. The Open FAIR Body of Knowledge is most often used to quantitatively measure risk in economic terms (although it can be used in support of qualitative risk analysis as well). It describes 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/IEC 27005, The Open Group Security Forum created a detailed mapping guide: The Open FAIR™ – ISO/IEC 27005 Cookbook [C103 2010].

An Introduction to Risk and the Risk Taxonomy

The Open FAIR Body of Knowledge defines risk as the probable frequency and magnitude of future loss. It focuses solely on risk that results in loss as opposed to speculative risk (which might generate either a loss or a gain).[1]

Risk is not tangible – we cannot see it, touch it, or measure it directly, and an expression such as "our computers are corporate risks" is inaccurate. Risk is a derived value, similar to speed – risk is the probable frequency and probable magnitude of future economic loss, as viewed from the perspective of the Primary Stakeholder who will bear the loss and subjectively values it.

With this as a starting point, the Open FAIR Body of Knowledge defines a logical, tightly defined taxonomy that describes the factors that drive risk, their definitions, and relationships. The first two components of risk are loss frequency and loss magnitude. These are referred to in the taxonomy as Loss Event Frequency and Loss Magnitude, respectively, as shown in Figure 2. If either of these components are missing then you are not talking about risk – you are likely talking about a subcomponent of risk.

Figure 2: Risk

Without a logical, tightly defined taxonomy, risk assessment approaches will be significantly impaired by an inability to measure and/or estimate risk factor variables. This, in turn, means that management will not have the necessary information for making well-informed comparisons and choices, which will lead to inconsistent and often cost-ineffective risk management decisions. The relationship between these elements is known as the Risk Management Stack, and can be illustrated as shown in Figure 3.

[1] This differs from other standards, such as ISO 31000 [ISO 31000].

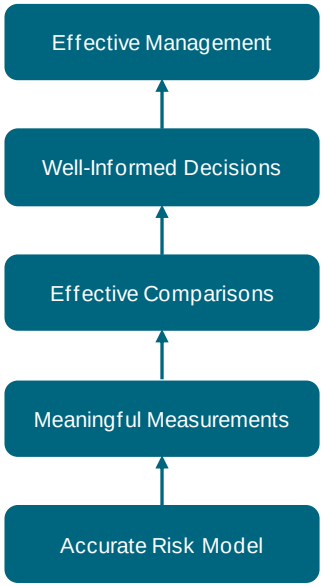

Figure 3: Risk Management Stack

The Open FAIR Risk Taxonomy

The complete risk taxonomy is comprised of two main branches: Loss Event Frequency and Loss Magnitude. Within those two branches are the factors that drive the occurrence and magnitude of losses. Figure 4 sets out the layered abstractions within the framework.

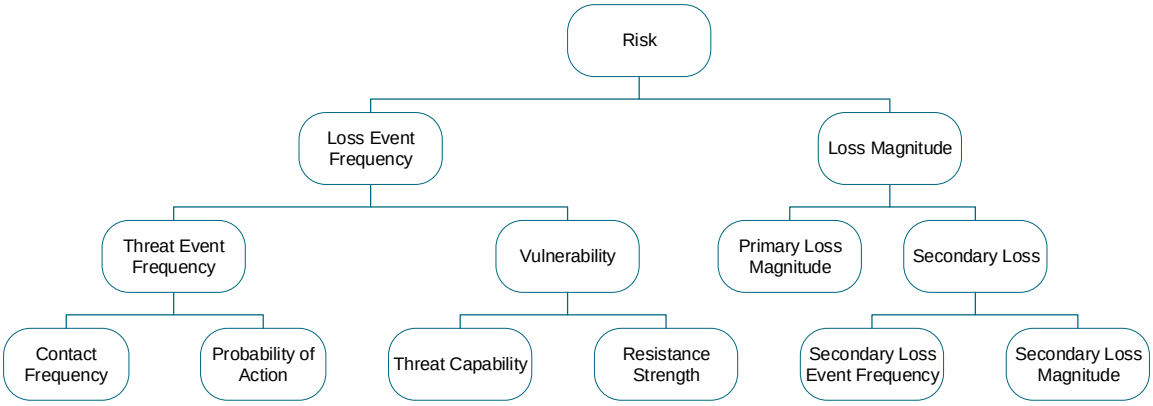

Figure 4: Layered Risk Taxonomy Abstractions

Loss Event Frequency

Loss Event Frequency is the probable frequency, within a given timeframe, that a Threat Agent will inflict harm upon an Asset. In basic terms this can be thought of as how often a bad thing happens to something that the Primary Stakeholder values; for example, how often money is stolen or how many times per year hackers perform a denial of service attack against an online banking system.

Threat Event Frequency

Threat Event Frequency is the probable frequency, within a given timeframe, that a Threat Agent will act against an Asset. For example, the probable frequency, within a given timeframe, that a thief tries to steal the money, a tornado hits a building, hackers perform a denial of service attack on your computer system, etc.

Contact Frequency

Contact Frequency is the probable frequency, within a given timeframe, that a Threat Agent will come into contact with an Asset. Contact can be physical or "logical" (e.g., over the network).

Probability of Action

Probability of Action is the probability that a Threat Agent will act against an Asset once contact occurs. Once contact occurs between a Threat Agent and an Asset, action against the Asset may or may not take place. For some Threat Agent types, especially natural Threat Agents, action always takes place. For example, all tornado contacts with a house represent potential losses – that is, Threat Events – to the homeowner.

Vulnerability

The definition of Vulnerability in the Open FAIR risk taxonomy departs from the casual or informal use of the term. Vulnerability, or its synonym "susceptibility", is the probability that a Threat Event will become a Loss Event. Vulnerability exists when there is a difference between the force being applied by the Threat Agent and an object's ability to resist that force. This simple analysis provides us with the two primary factors that drive Vulnerability: Threat Capability and Resistance Strength.

Threat Capability

Threat Capability is the probable level of force (as embodied by the time, resources, and technological capability) that a Threat Agent is capable of applying against an Asset. Not all Threat Agents are created equal. In fact, Threat Agents within a single Threat Community are not all going to have the same capabilities.

Resistance Strength

Resistance Strength is the strength of a control as compared to the probable level of force (as embodied by the time, resources, and technological capability; measured as a percentile) that a Threat Agent is capable of applying against an Asset. In simple terms, this can be considered the degree of difficulty faced by the Threat Agent. For example, a wireless network secured by Wireless Protected Access, Version 2 (WPA2) has a higher Resistance Strength to a hacker community than one secured by Wired Equivalent Privacy (WEP).

Loss Magnitude

Loss Magnitude is the probable magnitude of economic loss (measured in units of currency) resulting from a Loss Event. The Loss Magnitude side of the taxonomy describes the other half of the risk equation – the factors that drive the size of the loss when events occur.

Primary Loss Magnitude

Primary Loss Magnitude is the direct result or harm to the Primary Stakeholder of a Threat Agent's action upon an Asset and often represents the intention in acting against the Asset. Usually, the owner of the affected Asset is the Primary Stakeholder in an analysis.

Secondary Loss

Secondary Loss is a result of Secondary Stakeholders (e.g., customers, stockholders, regulators, etc.) whose negative reaction exposes the Primary Stakeholder to additional losses beyond the Primary Loss – this can be thought of as "fallout". Secondary Loss has two primary components: Secondary Loss Event Frequency and Secondary Loss Magnitude.

Secondary Loss Event Frequency

Secondary Loss Event Frequency is the conditional probability that a Primary Loss will result in a Secondary Loss. In other words, it is an estimate of the chance (percentage of time) that a scenario is expected to have secondary effects.

Secondary Loss Magnitude

Secondary Loss Magnitude is an estimate of the losses that materialize from dealing with Secondary Stakeholder reactions (e.g., fines and judgments, loss of market share).

An Example Analysis

The Open FAIR risk analysis method leverages well-established quantitative methods, including statistical distributions, calibrated estimates to support data, and Monte Carlo stochastic simulation, to let analysts faithfully represent the quality/confidence in data and estimates of future loss.

Any Open FAIR risk analysis begins with a Loss Scenario, the single-sentence story of loss from the perspective of the Primary Stakeholder. For this example analysis,[2] the Loss Scenario is:

Cleaning crew member(s) find and copy a Human Resources (HR) executive's user ID and password found on a sticky-note and, using those credentials, they maliciously access and misuse sensitive employee information; when this event occurs, the bank always suffers primary productivity and response losses, and the bank may also suffer secondary response costs and fines and judgments.

This example analysis[3] assumes that cleaning crews are generally comprised of honest people, that an HR executive's credentials typically would not be viewed or recognized as especially valuable to them, and that the perceived risk associated with illicit use might be high. This results in the following estimates for Threat Event Frequency (Figure 5).

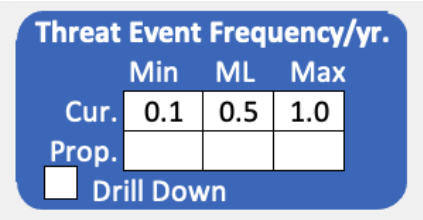

Figure 5: Threat Event Frequency

As a result, these values for Threat Event Frequency mean that the minimum expected frequency is once every ten years (0.1), the most likely frequency is once every two years (0.5), and the maximum frequency is once a year (1).

Figure 6: Threat Capability & Resistance Strength

[2] For full details of this example analysis as well as a comparison of results from a qualitative version of the same Loss Scenario, see the Open FAIR™ Risk Analysis Example Guide §2 [G21A 2021]

[3] Estimates for this example analysis will be presented using screengrabs from the Open FAIR™ Risk Analysis Tool [I181 2018].

As shown in Figure 6, the calibrated estimate for most likely Threat Capability is 50%, with a minimum of 25% and a maximum of 75% based on a reasonable comparison to the overall threat population. The maximum Resistance Strength in this example is only 4%, which is well below the Threat Capability minimum of 25%. As a result, the Open FAIR Risk Analysis Tool [I181 2018] calculates Vulnerability as 100%. In other words, if one or more members of the cleaning crew decide to use the credentials, they would be expected to gain access every time. Every unauthorized access is assumed to result in a loss to the Primary Stakeholder.

With these inputs, the Open FAIR Risk Analysis Tool produces the following charts (Figure 7) that indicate that in a given year no loss is estimated to occur about 60% of the time and that one Loss Event would occur about 33% of the time. In other words, one Loss Event is only estimated to occur once every three years. There is also only a 7% chance that more than one Loss Event would occur in a single year.

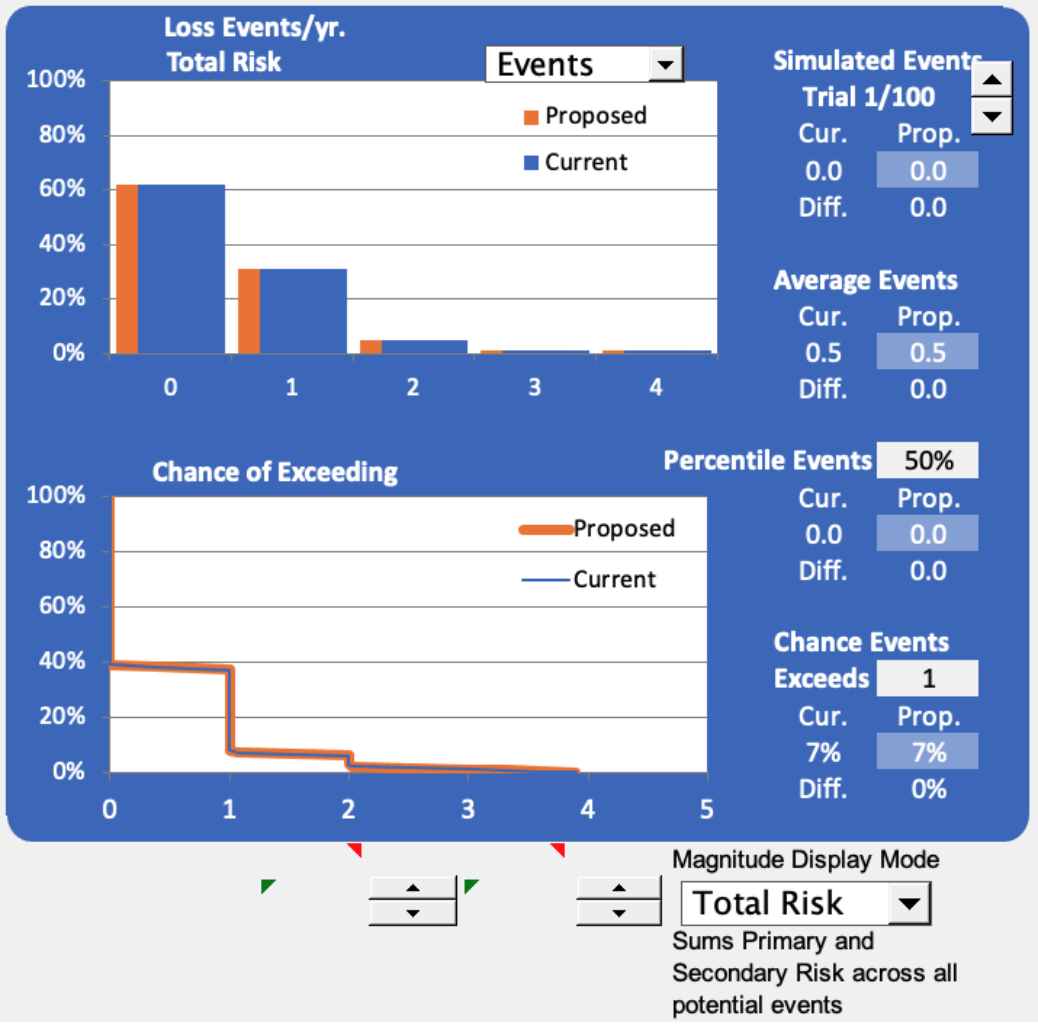

Figure 7: Total Risk (Frequency)

On the Loss Magnitude side of things, the expected forms of loss for the Primary Loss Magnitude are productivity loss and replacement loss, with the estimates (in thousands of dollars) for minimum, most likely, and maximum shown in Figure 8.

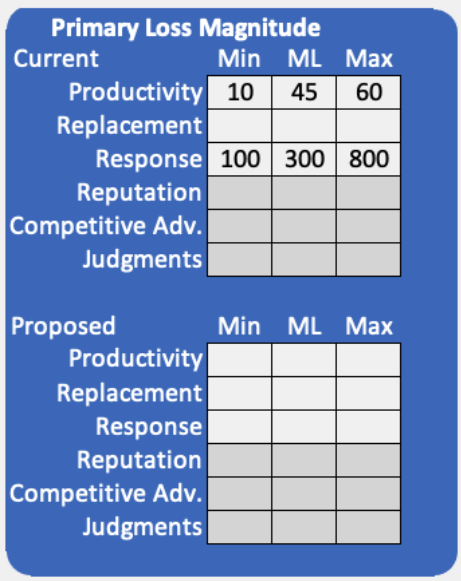

Figure 8: Primary Loss Magnitude

The estimates for Primary Loss Magnitude are based on the following rationale, which is still based on what is expected to happen *versus* best and worst-case:

- Productivity – although there may be some amount of disruption to the organization, there is no operational outage associated with this scenario and the organization should continue to be able to deliver its goods and services to its customers
- Response – primary response costs in this scenario are limited to person-hours involved in the investigation, any costs related to dealing with the agency that provides the cleaning crew, as well as any forensic expenses that might arise

There are also expected to be Secondary Losses resulting from the actions of Secondary Stakeholders. However, since customer information is not involved in this scenario, the risk analysis assumes minimal, if any, negative reaction from customers. Likewise, a compromise of employee information is unlikely to generate much concern with shareholders because the event does not reflect badly on the fundamental value proposition of the institution.

With this in mind and because this event involves the compromise of personal employee information, it is virtually guaranteed that one or more of the Secondary Stakeholder communities would be informed and have to be "managed". Consequently, the estimate for most likely Secondary Loss Event Frequency is 95%, with a minimum of 90% and a maximum of 100%.

Therefore, the expected forms of loss for Secondary Loss are response costs and fines and judgments, with the estimates (in thousands of dollars) for minimum, most likely, and maximum shown in Figure 9.

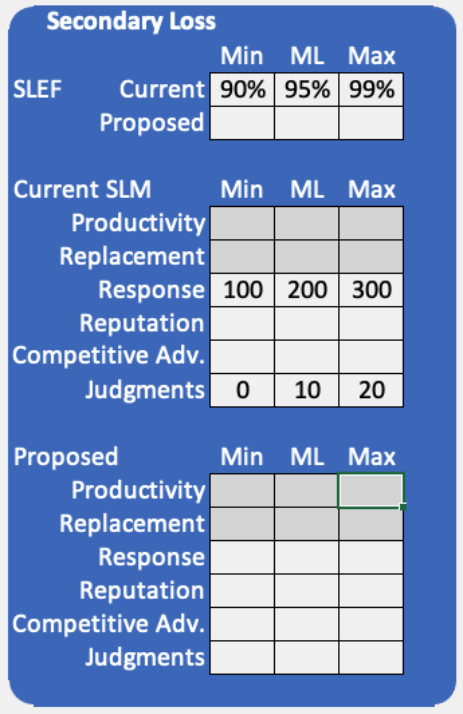

Figure 9: Secondary Loss Magnitude

This indicates that from all of the simulated trials generated by the Open FAIR Risk Analysis Tool, a single Loss Event would have an average loss of $659,000. The single simulated trial (out of 100) presented in Figure 10 would result in loss of $702,000. Moreover, there is a 65% chance of loss exceeding $715,000 and an 85% chance of loss exceeding $500,000. Figure 10 displays the combined Loss Magnitude results for a single estimated Loss Event from the Open FAIR Risk Analysis Tool.

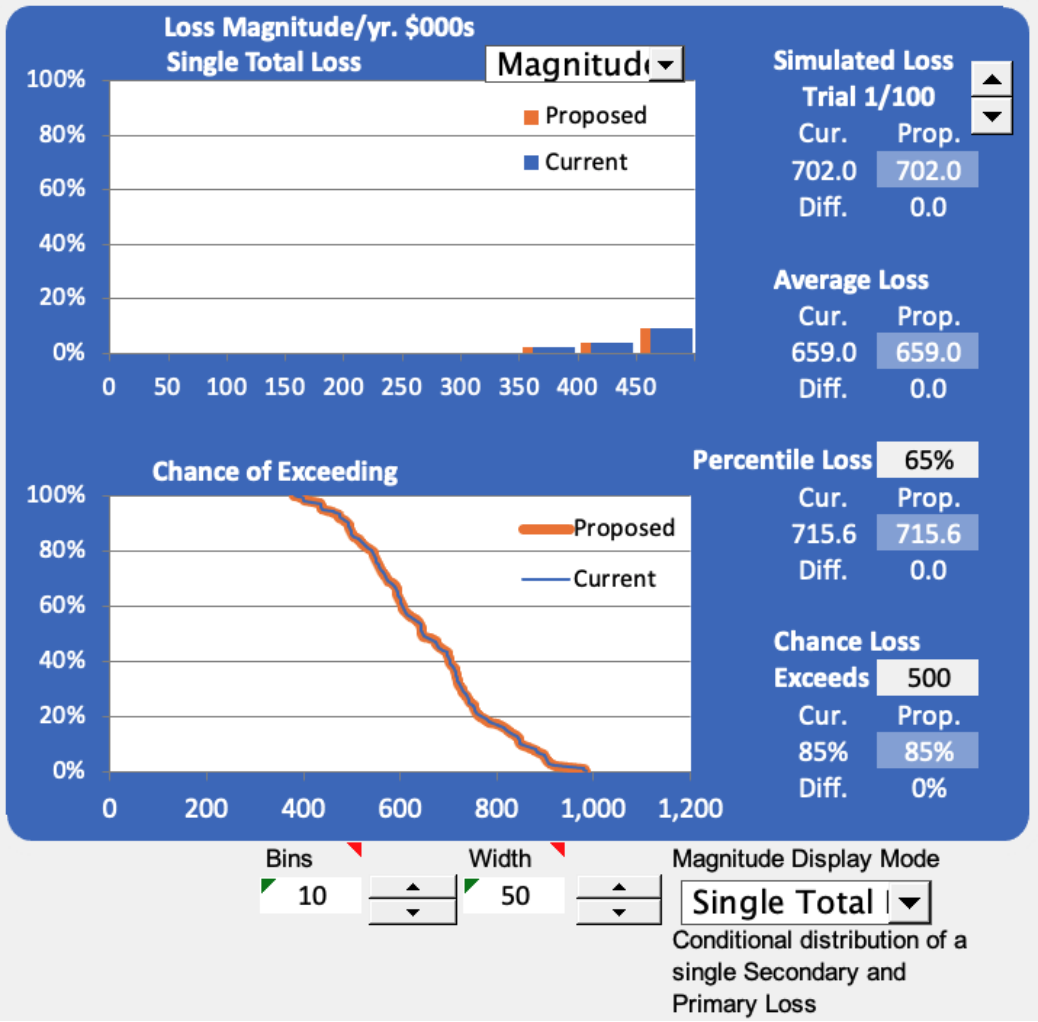

Figure 10: Single Total Loss

Figure 11 visualizes the total risk (accounting for both Loss Event Frequency and Loss Magnitude) estimated in the analysis. It depicts 100 trials[4] and plots the distribution of them. In these 100 trials, the average annualized loss exposure is $309,000. In about 60% of simulated trials, the annualized loss exposure would be less than $50,000. However, there is a 31% chance that loss will exceed $500,000. In other words, a loss exceeding $500,000 is estimated to occur once every roughly three years.

[4] The Open FAIR Risk Analysis Tool simulates 100 years of outcomes by default, which can be adjusted according to preference.

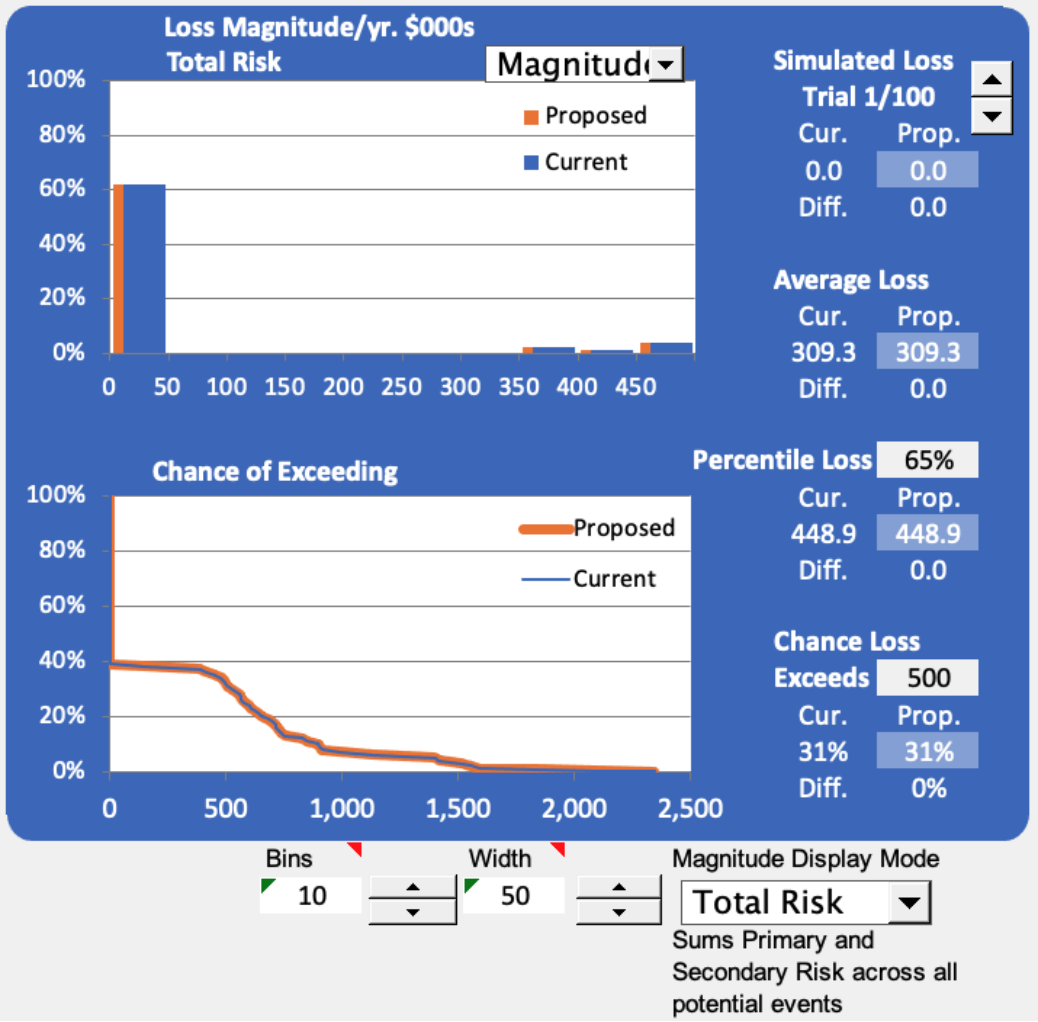

Figure 11: Total Risk (Magnitude)

Making Standards Work®: Open FAIR Certification

Bringing value to risk practitioners, and to the entire risk analysis ecosystem, requires more than just publishing industry standards. The Open Group risk activities extend to publishing additional guidance on the use of the Open FAIR Body of Knowledge, and to a certification program for risk analysts based upon the Open FAIR Body of Knowledge. By certifying individuals with Open FAIR knowledge, The Open Group is helping to develop and accredit risk analysts and meet the demand for qualified personnel. The Open Group also runs an accreditation program for Open FAIR training course providers, which ensures that quality training is available worldwide.

Open FAIR certification is complementary to other industry certifications in the area of risk. The ISACA® Certified in Risk and Information Systems Control (CRISC) certification is the best example here. The CRISC certification program deals broadly with risk management. Open FAIR certification complements the CRISC by providing a deeper treatment on the "how to" aspects of performing effective risk analysis.

Referenced Documents

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

[C103 2010] The Open FAIR™ – ISO/IEC 27005 Cookbook, The Open Group Guide (C103), published by The Open Group, October 2010; refer to: www.opengroup.org/library/c103

[C13F 2013] Dependability Through Assuredness™ (O-DA) Framework, a standard of The Open Group (C13F), published by The Open Group, July 2013; refer to: www.opengroup.org/library/c13f

[C17B 2017] Open Information Security Management Maturity Model (O-ISM3), Version 2.0, a standard of The Open Group (C17B), published by The Open Group, September 2017; refer to: www.opengroup.org/library/c17b

[C197 2019] ArchiMate® 3.1 Specification, a standard of The Open Group (C197), published by The Open Group, November 2019; refer to: www.opengroup.org/library/c197

[C20A 2021] The Open Group Standard for Risk Analysis (O-RA), Version 2.0.1 (C20A), published by The Open Group, November 2021; refer to: www.opengroup.org/library/c20a

[C20B 2021] The Open Group Standard for Risk Taxonomy (O-RT), Version 3.0.1 (C20B), published by The Open Group, November 2021; refer to: www.opengroup.org/library/c20b

[C185-1 2018] Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products: Part 1: Requirements and Recommendations, Version 1.1.1 (technically equivalent to ISO/IEC 20243-1:2018), a standard of The Open Group (C185-1), published by The Open Group, September 2018; refer to: www.opengroup.org/library/c185-1

[C185-2 2018] Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products: Part 2: Assessment Procedures for the O-TTPS and ISO/IEC 20243-1:2018, Version 1.1.1 (technically equivalent to ISO/IEC 20243-2:2018, a standard of The Open Group (C185-2), published by The Open Group, September 2018; refer to: www.opengroup.org/library/c185-2

[G112 2011] Open Enterprise Security Architecture (O-ESA): A Framework and Template for Policy-Driven Security, The Open Group Guide (G112), published by The Open Group, April 2011; refer to: www.opengroup.org/library/g112

[G21A 2021] Open FAIR™ Risk Analysis Example Guide (G21A), published by The Open Group, July 2021; refer to: www.opengroup.org/library/g21a

[I181 2018] The Open FAIR™ Risk Analysis Tool (I181), published by The Open Group, January 2018; refer to: www.opengroup.org/library/i181

[ISO 31000] ISO 31000:2018: Risk Management – Guidelines, February 2018; refer to https://www.iso.org/standard/65694.html

[ISO/IEC 27001] ISO/IEC 27001:2013: Information Technology – Security Techniques – Information Security Management Systems – Requirements; refer to: https://www.iso.org/standard/54534.html

[ISO/IEC 27005] ISO/IEC 27005:2018: Information Technology – Security Techniques – Information Security Risk Management; refer to: https://www.iso.org/standard/75281.html

[NIST 800-30] NIST Special Publication (SP) 800-30: Guide for Conducting Risk Assessments, April 2021; refer to: https://www.nist.gov/privacy-framework/nist-sp-800-30

[TOGAF 2022] The TOGAF® Standard, 10th Edition, a standard of The Open Group (C220), published by The Open Group, April 2022; refer to: www.opengroup.org/library/c220

For a full list of publications related to or supporting the Open FAIR Body of Knowledge, visit: https://publications.opengroup.org/security-library/risk-analysis.

About the Authors

John Linford, The Open Group

John Linford is the Forum Director of The Open Group Security Forum and Open Trusted Technology Forum. As staff at The Open Group, John supports the leaders and participants of the Security Forum in utilizing the resources of The Open Group to facilitate collaboration and follow The Open Group Standards process to publish their deliverables.

Andrew Josey, The Open Group

Andrew Josey is VP Standards and Certification, overseeing all certification and testing programs of The Open Group. He also manages the standards process for The Open Group. Since joining the company in 1996, Andrew has been closely involved with the standards development, certification, and testing activities of The Open Group. He has led many standards development projects including specification and certification development for the ArchiMate®, TOGAF®, POSIX™, Digital Practitioner, TOGAF Business Architecture, and UNIX® programs. Most recently he has led the development of the Open Agile Architecture™ Practitioner certification program. He is a member of the IEEE, USENIX, and the Association of Enterprise Architects® (AEA). He holds an MSc in Computer Science from University College London.

Jim Hietala, The Open Group

Jim Hietala is Vice-President, Business Development and Security for The Open Group, where he manages security and risk management programs and standards activities, as well as the business development team. He has led the development of several industry standards including the Open Information Security Management Maturity Model (O-ISM3) Standard, the Open Enterprise Security Architecture (O-ESA), and the Open FAIR™ Body of Knowledge, as well as the Open FAIR certification program for risk analysts. Jim is a frequent speaker at industry conferences worldwide. He has participated in the SANS Institute Analyst/Expert program and has also published numerous articles on information security, risk management, and compliance topics. An IT security industry veteran, he has held leadership roles at several IT security vendors. Jim holds a BS in Marketing from Southern Illinois University, and he is a holder of the Open FAIR, GSEC-Gold, and CISSP certifications.

Jack Jones, (formerly of) CXOWARE, Inc. (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 United States, 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.

About The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. With more than 870 member organizations, we have a diverse membership that spans all sectors of the technology community – customers, systems and solutions suppliers, tool vendors, integrators and consultants, as well as academics and researchers.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products

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