

*The Open Group Guide*

**Open FAIR™ Risk Analysis Example Guide**



Copyright © 2021, The Open Group. All rights reserved.

The Open Group hereby authorizes you to use this document for any purpose, PROVIDED THAT any copy of this document, or any part thereof, which you make shall retain all copyright and other proprietary notices contained herein.

This document may contain other proprietary notices and copyright information.

Nothing contained herein shall be construed as conferring by implication, estoppel, or otherwise any license or right under any patent or trademark of The Open Group or any third party. Except as expressly provided above, nothing contained herein shall be construed as conferring any license or right under any copyright of The Open Group.

Note that any product, process, or technology in this document may be the subject of other intellectual property rights reserved by The Open Group, and may not be licensed hereunder.

This document is provided “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Any publication of The Open Group may include technical inaccuracies or typographical errors. Changes may be periodically made to these publications; these changes will be incorporated in new editions of these publications. The Open Group may make improvements and/or changes in the products and/or the programs described in these publications at any time without notice.

Should any viewer of this document respond with information including feedback data, such as questions, comments, suggestions, or the like regarding the content of this document, such information shall be deemed to be non-confidential and The Open Group shall have no obligation of any kind with respect to such information and shall be free to reproduce, use, disclose, and distribute the information to others without limitation. Further, The Open Group shall be free to use any ideas, concepts, know-how, or techniques contained in such information for any purpose whatsoever including but not limited to developing, manufacturing, and marketing products incorporating such information.

If you did not obtain this copy through The Open Group, it may not be the latest version. For your convenience, the latest version of this publication may be downloaded at [www.opengroup.org/library](http://www.opengroup.org/library).

The Open Group Guide

**Open FAIR™ Risk Analysis Example Guide**

ISBN: 1-947754-79-9

Document Number: G21A

Published by The Open Group, July 2021.

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:

[ogspeccs@opengroup.org](mailto:ogspeccs@opengroup.org)

# Contents

1	Introduction.....	1
1.1	Objective.....	1
1.2	Overview.....	1
1.3	Future Directions .....	1
2	Qualitative and Quantitative Analysis Comparison.....	2
2.1	Analysis Using Qualitative Scale .....	2
2.1.1	Stage 1: Identify the Loss Scenario (Scope the Analysis).....	3
2.1.2	Stage 2: Evaluate the Loss Event Frequency .....	4
2.1.3	Stage 3: Evaluate Loss Magnitude .....	8
2.1.4	Stage 4: Derive and Articulate Risk .....	13
2.2	Analysis Using the Open FAIR Risk Analysis Tool .....	14
2.2.1	Stage 1: Identify the Loss Scenario (Scope the Analysis).....	14
2.2.2	Stage 2: Evaluate Loss Event Frequency .....	14
2.2.3	Stage 3: Evaluate Loss Magnitude .....	17
2.2.4	Stage 4: Derive and Articulate Risk .....	23
2.3	Quantitative and Qualitative Analysis Result Comparison.....	23
2.3.1	Risk Analysis Quality Considerations.....	24
3	Using Open FAIR Risk Analysis to Inform Business Decisions .....	26
3.1	Risk Associated with Unstructured Data .....	26
3.1.1	Background .....	26
3.1.2	Current Scenario.....	27
3.1.3	Proposed Scenario .....	33
3.1.4	Analyze Risk .....	38
3.1.5	Prepare Business Case.....	42

# Preface

## The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 800 organizations includes customers, systems and solutions suppliers, tools vendors, integrators, academics, and consultants across multiple industries.

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

The Open Group publishes a wide range of technical documentation, most of which is focused on development of 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/library](http://www.opengroup.org/library).

## This Document

This document is The Open Group Open FAIR™ Risk Analysis Example Guide. It has been developed and approved by The Open Group.

Chapter 2 provides two examples of Open FAIR risk analysis that are based on the same risk scenario – the first example uses qualitative analysis tools that reference quantitative scales, and the second example uses the Open FAIR™ Risk Analysis Tool with calibrated estimates used for inputs. These analysis results are then compared. Chapter 3 develops a business case utilizing results from an Open FAIR risk analysis, and provides examples of communicating Open FAIR risk analysis results to decision-makers.

## Trademarks

ArchiMate, DirecNet, Making Standards Work, Open O logo, Open O and Check Certification logo, Platform 3.0, The Open Group, TOGAF, UNIX, UNIXWARE, and the Open Brand X logo are registered trademarks and Boundaryless Information Flow, Build with Integrity Buy with Confidence, Commercial Aviation Reference Architecture, Dependability Through Assuredness, Digital Practitioner Body of Knowledge, DPBoK, EMMM, FACE, the FACE logo, FHIM Profile Builder, the FHIM logo, FPB, Future Airborne Capability Environment, IT4IT, the IT4IT logo, O-AA, O-DEF, O-HERA, O-PAS, Open Agile Architecture, Open FAIR, Open Footprint, Open Process Automation, Open Subsurface Data Universe, Open Trusted Technology Provider, OSDU, Sensor Integration Simplified, SOSA, and the SOSA logo are trademarks of The Open Group.

Microsoft, PowerPoint, SharePoint, and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.

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

## Acknowledgements

(Please note affiliations were current at the time of approval.)

The Open Group gratefully acknowledges the contribution of the following people in the development of this document:

- Joel Baese, Mosaic451
- Steven Bradley, The SABSA Institute
- Christopher T. Carlson, C T Carlson LLC (Principal Author)
- Jack Freund, Cyber Assessments, Inc.
- Apolonio (Apps) Garcia, HealthGuard
- Mike Jerbic, Trusted Systems Consulting
- Eva Kuiper, The Open Group Invited Expert (Primary Contributor)
- Tyanna Smith, Trusted Systems Consulting
- John Linford, Security & OTTF Forum Director, The Open Group

The Open Group gratefully acknowledges the Member organizations and their representatives of The Open Group Security Forum who participated in the review of this document.

## Referenced Documents

The following documents are referenced in this Guide.

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

- ISO Guide 73:2009: Risk Management – Vocabulary; refer to: <https://www.iso.org/standard/44651.html>
- Problems with Scoring Methods and Ordinal Scales in Risk Assessment, D. Hubbard, D. Evans, 2010, published by IBM Journal of Research & Development; refer to: <https://pdfs.semanticscholar.org/8c89/6b5700c801a512a91f17803299715858d23f.pdf>
- Risk Analysis (O-RA), Version 2.0, The Open Group Standard (C20A), November 2020, published by The Open Group; refer to: [www.opengroup.org/c20a](http://www.opengroup.org/c20a)  
This standard provides a set of standards for various aspects of information security risk analysis.
- Risk Taxonomy (O-RT), Version 3.0, The Open Group Standard (C20B), published by The Open Group, November 2020; refer to: [www.opengroup.org/library/c20b](http://www.opengroup.org/library/c20b)  
This standard defines a taxonomy for the factors that drive information security risk.
- The Open FAIR™ Risk Analysis Process Guide (G180), January 2018, published by The Open Group; refer to: [www.opengroup.org/library/g180](http://www.opengroup.org/library/g180)  
This guide offers some best practices for performing an Open FAIR risk analysis. It aims to help risk analysts understand how to apply the Open FAIR risk analysis methodology.
- The Open FAIR™ Risk Analysis Tool Beta (I181), January 2018; refer to: [www.opengroup.org/library/i181](http://www.opengroup.org/library/i181)  
This tool can be used to perform a quantitative Open FAIR risk analysis as defined in The Open Group Risk Analysis (O-RA) and Risk Taxonomy (O-RT) standards. It is provided in the form of a Microsoft® Excel spreadsheet.





# 1 Introduction

---

## 1.1 Objective

This document augments the Risk Analysis Methodology and Process section of The Open Group Risk Analysis (O-RA) Standard by illustrating the four steps using an example scenario. It demonstrates use of the Open FAIR™ Risk Analysis Tool that implements The Open Group Risk Taxonomy (O-RT) Standard.

This document also provides examples of utilizing Open FAIR risk analysis results to inform business decisions about proposed security changes. This component is a critical aspect of determining the value of implementing controls or otherwise acting to prevent losses from occurring or to mitigate losses when they occur.

This document is intended to be a *living document*. The sections are deliberately organized to allow additional examples to be added easily as they are contributed/developed.

## 1.2 Overview

This document is intended to supplement the Open FAIR Body of Knowledge by providing examples of Open FAIR risk analyses and informing business decisions about proposed security changes. It is complementary to the Open FAIR™ Risk Analysis Process Guide, relying on the Process Guide to describe *how* to complete an Open FAIR risk analysis.

## 1.3 Future Directions

Since this is intended to be a living document, as examples are contributed, they will be added to Chapter 3, following a similar structure and presentation. The Security Forum welcomes contributions of example analyses of varying complexity.

Depending on contributions, there is potential to expand the document by adding a section on communicating Open FAIR risk analysis results to decision-makers of an organization. These example reports would communicate the results within other frameworks, such as the NIST Cybersecurity Framework (CSF)<sup>1</sup>, ISO/IEC 27005,<sup>2</sup> or ISO 31000.<sup>3</sup> The Security Forum welcomes contributions of risk analysis reports to decision-makers of an organization.

---

<sup>1</sup> Refer to: <https://www.nist.gov/cyberframework>.

<sup>2</sup> ISO/IEC 27005:2018: Information Technology – Security Techniques – Information Security Risk Management; refer to: <https://www.iso.org/standard/75281.html>.

<sup>3</sup> ISO 31000: Risk Management; refer to: <https://www.iso.org/iso-31000-risk-management.html>.

## 2 Qualitative and Quantitative Analysis Comparison

---

This chapter contains the entirely fictional example<sup>4</sup> using a qualitative scale that was previously found in the O-RA Standard, Version 1.0 and the O-RT Standard, Version 2.0. This example was removed from these documents when the O-RA Standard was updated to Version 2.0 and the O-RT Standard was updated to Version 3.0.<sup>5</sup>

The example scenario will first be analyzed qualitatively based on the risk matrices included in the O-RA Standard, Version 1.0 and the O-RT Standard, Version 2.0. It will then be analyzed quantitatively, using the Open FAIR Risk Analysis Tool and providing the assumptions and rationale used for the included estimates. Finally, the qualitative results and the quantitative results will be compared to demonstrate the value of an Open FAIR approach to risk analysis.

The example scenario used throughout these two analyses is the same:

*A Human Resources (HR) executive within a large bank has her username and password written on a sticky-note stuck to her computer monitor. These authentication credentials allow her to log onto the network and access the HR applications she is entitled to use.*

Both analyses utilize the stages described in the O-RA Standard, Version 2.0, beginning with identifying the Loss Scenario before evaluating Loss Event Frequency (LEF), evaluating Loss Magnitude, and finally deriving and articulating risk.

### 2.1 Analysis Using Qualitative Scale

The qualitative analysis in this section demonstrates use of example qualitative scales to establish the intersection on a 5x5 risk matrix.

The scales in this example analysis are arbitrary but might act as a starting point for an organization attempting to implement a quantitative process while still utilizing qualitative scales – it is assumed that the decision-makers in this example have given approval to these scales and understand the labels and ranges in them. The example qualitative scales are not meant to offer standardized scales for organizations; rather, any qualitative scales used by an organization (if the organization uses qualitative scales) should be adapted based on organizational capacity for loss, management’s tolerance for loss, and management’s judgment for the resulting qualitative values of Very High, High, Moderate, etc. when risk factors are combined within risk matrices.

---

<sup>4</sup> This example is not based on any real-world scenario, but instead depicts a common potential scenario; any similarities to a real scenario are entirely coincidental, and the example should not be interpreted as being typical of the banking sector.

<sup>5</sup> This chapter does not demonstrate implementing a control; rather, it merely presents the *status quo* analysis both qualitatively and quantitatively to demonstrate their differences. Chapter 3 demonstrates changes from implementing controls.

## 2.1.1 Stage 1: Identify the Loss Scenario (Scope the Analysis)

### 2.1.1.1 *Identify the Primary Stakeholder*

In the example scenario provided at the start of this section, there are two possible Primary Stakeholders: the HR executive, and the large bank employing her. Given that it is the bank that is accountable for the HR applications and other sensitive employee information, the bank will be the Primary Stakeholder.

### 2.1.1.2 *Identify the Asset*

In the example scenario, there are multiple possible Assets: these are the credentials as well as the applications, systems, and information to which the credentials provide access. For this Loss Scenario, the Asset will be the credentials because their value is inherited from the assets they are intended to protect.

### 2.1.1.3 *Identify the Threat Community*

Within this scenario, there are several possible Threat Communities:

- The cleaning crew
- Other HR workers with regular access to the executive's office
- Visitors to the executive's office
- Job applicants
- Technical support staff

This Loss Scenario will focus on the cleaning crew as the most likely Threat Community: they have regular contact with the Asset; unless there are cameras spread throughout the office, there is a low risk of detection/capture, and there is minimal level of effort required to use the credentials.

### 2.1.1.4 *Identify the Threat Event*

In the example scenario, the most likely Threat Event is for the malicious use of the Asset by one or more members of the cleaning crew. The Threat Event would not be the result of error, failure, or a natural event.

The threat vector, therefore, would be one or more members of the cleaning crew using the authentication credentials written on the sticky-note to log into the HR executive's computer and gaining unauthorized access to the information they are intended to protect.

### 2.1.1.5 *Identify the Loss Event*

In the example scenario, the Threat Community could take one or more actions against the Asset: They could use the credentials to access, misuse, disclose, modify, or deny access to the sensitive employee information they are intended to protect.

The Loss Scenario will focus on the malicious access to and misuse of sensitive employee information by one or more members of the cleaning crew, using the executive's log-on credentials posted on a sticky-note. The malicious access to and misuse of the sensitive employee information will result in primary productivity and response losses for the bank – there

might be some employees who lose access, and the bank will need to investigate and assess the breach. There could also be Secondary Losses from fines and judgments by regulators, which would also create secondary response losses.

The specificity of this description excludes events whereby a cleaning crew member used the credentials to log on and surf the Internet, check their social media accounts, or even send illicit email. It also stipulates that the intent be malicious, which excludes acts of simple curiosity, and involves misuse *versus* destruction. These other scenarios could be separate analyses of their own if they were deemed relevant enough.

**2.1.1.6**     *Decompose the Loss Scenario*

Now that the Primary Stakeholder, Asset, Threat Community, Threat Event, and Loss Event have all been identified, the Loss Scenario can be decomposed and written as a single sentence to tell the story of the loss.

*Cleaning crew member(s) find and copy an 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.*

**2.1.2**     **Stage 2: Evaluate the Loss Event Frequency**

This section works to evaluate the LEF. For the sake of the example, this estimate is derived by estimating values for Contact Frequency, Probability of Action, Threat Capability, and Resistance Strength. This is done deliberately to demonstrate finding estimates for all risk factors, despite guidance in the O-RA Standard, Version 2.0 to utilize a top-down approach, only estimating lower-level risk factors if necessary for the purpose of the analysis.

**2.1.2.1**     *Estimate the Threat Event Frequency*

Threat Event Frequency (TEF) is based upon how frequently contact between the Threat Agent and the Asset occurs (the Contact Frequency) *and* the probability that the Threat Agent would act against the Asset (the Probability of Action).

As stated previously, TEF will be estimated by considering Contact Frequency and Probability of Action.

Contact has already been determined to be regular between the cleaning crew and the Asset, though a specific number of times/week or times/month was not initially determined. Based on typical business operations, this analysis *assumes* that the cleaning crew visits the bank once per week – this is the Contact Frequency, and it would be estimated as High, based on the example qualitative scale below.

Rating	Description
Very High (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year

Rating	Description
Low (L)	Between 0.1 and 1 times per year
Very Low (VL)	< 0.1 times per year (less than once every 10 years)

**Figure 1: Example Qualitative Scale for Contact Frequency**

This analysis also *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 means the Probability of Action is Very Low – cleaning crew members are extremely unlikely to act against the Asset, even if contact is made – based on the example qualitative scale below.

Rating	Description
Very High (VH)	> 99% probability of acting
High (H)	70% to 99% probability of acting
Moderate (M)	30% to 70% probability of acting
Low (L)	1% to 30% probability of acting
Very Low (VL)	< 1% probability of acting

**Figure 2: Example Qualitative Scale for Probability of Action**

As a result, TEF can be estimated to be Very Low, using the example risk matrix below.

		Threat Event Frequency (TEF)					
		VH	M	H	VH	VH	VH
Probability of Action (PoA)	VH	M	H	VH	VH	VH	
	H	L	M	H	H	H	
	M	VL	L	M	M	M	
	L	VL	VL	L	L	L	
	VL	VL	VL	VL	VL	VL	
		VL	L	M	H	VH	
		Contact Frequency (CF)					

**Figure 3: Example Risk Matrix for Threat Event Frequency**

As a result, based on the example qualitative scale below, a Threat Event would only be estimated to occur less than once every ten years.

Rating	Description
Very High (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between 0.1 and 1 times per year
Very Low (VL)	< 0.1 times per year (less than once every 10 years)

**Figure 4: Example Qualitative Scale for Threat Event Frequency**

A cleaning crew could contain an employee with motive, sufficient computing experience to recognize the potential value of these credentials, and with a high enough risk tolerance to try their hand at illicit use. However, the *probable* TEF is Very Low.

The example scenario is missing information that could impact TEF by reducing Probability of Action:

- The cleaning crew could be escorted through their rounds by a member of the physical security team
- The premises could be well covered by CCTV
- The cleaning crew employees could be bonded and undergo thorough background checks
- The cleaning crew employees could have been with the company for years

None of these are guarantees of TEF being 0, of course, but they are relevant considerations that affect the likelihood of misbehavior.

#### 2.1.2.2 *Estimate Vulnerability*

Vulnerability is the probability that a Threat Event results in a Loss Event, and it can either be estimated directly by comparing the number of Loss Events to the total Threat Events or by considering how Threat Capability compares to Resistance Strength.

This example will estimate Vulnerability by comparing Threat Capability to Resistance Strength and working at the lower level of the Open FAIR taxonomy.

In this example scenario, Threat Capability is based on the skill (in this case, reading ability) and resources (time) the average member of this Threat Community can use against a password written on a sticky-note. Based on the example qualitative scale below, the Threat Capability of the cleaning crew can be estimated to be Moderate (meaning average skill and resources), as compared to the overall threat population.

Rating	Description
Very High (VH)	Top 2% when compared against the overall threat population
High (H)	Top 16% when compared against the overall threat population
Moderate (M)	Average skill and resources (between bottom 16% and top 16%)
Low (L)	Bottom 16% when compared against the overall threat population
Very Low (VL)	Bottom 2% when compared against the overall threat population

**Figure 5: Example Qualitative Scale for Threat Capability**

Note: Threat Capability is always estimated relative to the scenario. If the scenario was different, and instead was evaluating the cleaning crew’s capability to execute a Structured Query Language (SQL) injection attack, Threat Capability would likely be estimated to be Low or even Very Low.

In this example scenario, because the credentials are in plain sight and in plain text, the Resistance Strength is Very Low, based on the example qualitative scale below. This would mean the Asset is protected from *only the bottom 2% of an average threat population*.

Rating	Description
Very High (VH)	Protects against all but the top 2% of an average threat population
High (H)	Protects against all but the top 16% of an average threat population
Moderate (M)	Protects against the average Threat Agent
Low (L)	Only protects against bottom 16% of an average threat population
Very Low (VL)	Only protects against bottom 2% of an average threat population

**Figure 6: Example Qualitative Scale for Resistance Strength**

Based on the estimates of Threat Capability being Moderate and Resistance Strength being Very Low, Vulnerability can then be estimated to be Very High using the example risk matrix below.

Threat Capability (TCap)	Vulnerability (Vuln)					
	VH	VH	VH	VH	H	M
	H	VH	VH	H	M	L
	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL
		VL	L	M	H	VH
	Resistance Strength (RS)					

Figure 7: Example Risk Matrix for Vulnerability

2.1.2.3 Estimate Loss Event Frequency

In this example scenario, given a TEF of Low and Vulnerability of Very High, the LEF would likely be Low, based on the example risk matrix below.

Threat Event Frequency (TEF)	Loss Event Frequency (LEF)					
	VH	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL
		VL	L	M	H	VH
	Vulnerability (Vuln)					

Figure 8: Example Risk Matrix for Loss Event Frequency

Note: Vulnerability is depicted as a percentage, which means that a Primary Stakeholder can never be more than 100% vulnerable. Consequently, the LEF will never be greater than the TEF.

2.1.3 Stage 3: Evaluate Loss Magnitude

This section works to evaluate Loss Magnitude. Loss Magnitude is comprised of the Primary Loss Magnitude (PLM), which is the direct consequence(s) of the Loss Event, and Secondary Loss, which is in turn comprised of the Secondary Loss Event Frequency (SLEF) and Secondary Loss Magnitude (SLM).



### 2.1.3.1 Estimate the Primary Loss Magnitude

Within this scenario, there were two actions identified as being most likely for the Threat Community to take that would cause a Primary Loss:

- **Access** – the cleaning crew does not have authorized access to the sensitive employee information
- **Misuse** – employee records typically have information that can be used to execute identity theft, which introduces potential legal and reputation loss

The Loss Scenario focuses on access and misuse (e.g., identity theft) because it is a common concern for scenarios such as this.

A key *assumption* in the Loss Magnitude portion of this analysis is that the volume of compromised employee information is limited to the number of employee records in the system. This is relevant because even a loss of, for example, 15,000 employee records pales in comparison to breaches of customer records, which can number in the millions. It may also be reasonable to assume that the volume of compromised employee records would be much smaller, due to factors such as:

- Cleaning crew member concerns regarding higher risk from taking more data
- Cleaning crew intent to personally execute identity theft *versus* selling the information for others to abuse

When performing an analysis, the analyst needs to develop a rationale that supports their foundational assumptions. When using the qualitative values such as in this example, it sometimes makes sense to perform multiple scenario analyses: one for best-case, another for most likely, and a third for worst-case.

The next step is to estimate the PLM for access and misuse based on the Open FAIR forms of loss.

Forms of Loss					
Productivity	Response	Replacement	Fines and Judgments	Competitive Advantage	Reputation
L	M	—	—	—	—

The example qualitative scale below presents a set of ranges to characterize Loss Magnitude. The ranges within the scale reflect this example organization's capacity for loss and/or management's tolerance for loss.

Magnitude	Range Low End	Range High End
Very High (VH)	\$10,000,000	—
High (H)	\$1,000,000	\$9,999,999
Moderate (M)	\$100,000	\$999,999
Low (L)	\$10,000	\$99,999
Very Low (VL)	\$0	\$9,999

**Figure 9: Example Qualitative Scale for Primary Loss Magnitude**

The estimate for PLM – comprised of productivity and response losses – in this scenario is Moderate based on the following rationale:

- **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; for these reasons, monetary loss severity would be expected to be low
- **Response** – primary response costs in this scenario will involve, at a minimum, the following activities: investigation of the breach, assessment and audit, crisis management, and internal communications

Since the breach involved employee data, which is protected Personally Identifiable Information (PII) in many localities, this will trigger notifications to all employees within the compromised application. It is likely that outside experts will be required to determine the notification requirements, per locality of employee (whether residence or nationality, depending on the specific breach notification law).

This rationale is based on *what is expected to happen versus* best and worst-case. This highlights the fact that ordinal matrices tied to numeric ranges are limited in how effectively they represent the full range of possible outcomes. As stated earlier, the analyst might need to perform multiple scenario analyses to present all results: one for best-case, another for most likely, and a third for worst-case.

This example analysis does not estimate PLM for replacement, fines and judgments, competitive advantage, or reputation. Given the definitions for Primary and Secondary Loss, as well as the individual definitions for each of these forms of loss, some of these forms of loss are more relevant for Secondary Loss in this scenario.

### 2.1.3.2 Estimate Secondary Loss

Secondary Loss is comprised of the SLEF and the SLM, and Secondary Loss only occurs if reactions from Secondary Stakeholders cause one or more additional losses for the Primary Stakeholder.

In this scenario, regulators may react negatively to an event where a large loss of employee-sensitive information was compromised, at least in part because of questions the event might raise regarding controls over customer information. How severely regulators react will likely be a function of their perception of the existing overall control environment.

Since customer information is not involved in this scenario, this 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.

Although most Loss Scenarios will not treat employees as Secondary Stakeholders, there are exceptions in this example that make it reasonable to treat them as Secondary Stakeholders: the affected employees could potentially leave the organization and/or file lawsuits. These possible actions mean Secondary Losses would come from fines and judgments by regulators, which would also create secondary response losses.

SLEF is the conditional probability that a Primary Loss will result in a Secondary Loss. Because this event involves the compromise of personal information, it is highly likely that one or more of the Secondary Stakeholder communities would be required to be informed and have to be “managed”. Consequently, the probability of Secondary Loss Events occurring is Very High, or around 90 to 100% probability of occurring, based on the example qualitative scale below.

Rating	Description
Very High (VH)	90% to 100%
High (H)	70% to 90%
Moderate (M)	30% to 70%
Low (L)	10% to 30%
Very Low (VL)	0% to 10%

**Figure 10: Example Qualitative Scale for Secondary Loss Event Frequency**

This analysis *assumes* that all 15,000 employee records are taken. The rationale behind this assumption is that if someone is going to take the personal risk of performing this sort of illicit action, they are likely to try to maximize the value proposition. This rationale can be used to estimate the SLM for response losses and fines and judgments (by regulators) based on the Open FAIR forms of loss.

Forms of Loss					
Productivity	Response	Replacement	Fines and Judgments	Competitive Advantage	Reputation
—	M	—	L	—	—

The example qualitative scale below presents a set of ranges to characterize SLM. The ranges within the scale reflect this example organization’s capacity for loss and/or management’s tolerance for loss.

Magnitude	Range Low End	Range High End
Very High (VH)	\$10,000,000	—
High (H)	\$1,000,000	\$9,999,999
Moderate (M)	\$100,000	\$999,999
Low (L)	\$10,000	\$99,999
Very Low (VL)	\$0	\$9,999

**Figure 11: Example Qualitative Scale for Secondary Loss Magnitude**

The estimate for SLM – comprised of response losses and fines and judgments – in this scenario is Moderate based on the following rationale:

- **Response** – in this scenario, response costs would include executive time spent in meetings, notification costs, credit monitoring, and expenses associated with inside and outside legal counsel

A specific breakdown is:

- Executive time: 40 hours @ \$300 per hour = \$12,000
- Notification costs: \$5 per employee
- Credit monitoring: \$25 \* 15,000 employees \* 5% acceptance rate = \$18,750
- Legal expenses: \$100,000
- **TOTAL**: \$200,000 (approx.)

- **Fines and Judgments** – provided that the company was not negligent in handling the event, and made a concerted effort to protect employee interests, fines and judgments are assumed to be low (if any at all)

No productivity loss would occur as a Secondary Loss because the organization is still able to provide its goods and services.

No material reputation damage is expected to occur because it was an internal event, no customers were affected, and the organization had a security program in place that included policies and education. If, however, the organization had a problematic relationship with its employees or community, an argument could be made that the employee turnover and challenges with hiring could result, the effects of which could be characterized as reputation damage.

No damage to competitive position would occur because their competitors would not have improved their products and services, nor did the products and services of the organization diminish.

Note: If any employees actually suffered loss through identify theft, it is possible that the organization would have to cover those losses. In such a case, those losses would be accounted for as secondary replacement costs.

The value of Moderate is selected based on the approximate TOTAL value and these rationales.

Based on the estimates for SLEF being Very High and SLM being Moderate, the Secondary Loss would be Moderate, as shown in the example risk matrix below.

Secondary Loss Magnitude (SLM)	Secondary Loss					
	VH	L	M	M	H	VH
	H	L	L	M	M	H
	M	L	L	L	M	M
	L	VL	L	L	L	M
	VL	VL	VL	L	L	L
		VL	L	M	H	VH
	Secondary Loss Event Frequency (SLEF)					

Figure 12: Example Risk Matrix for Secondary Loss

2.1.3.3 Estimate Loss Magnitude

In this example scenario, given a PLM of Moderate and Secondary Loss of Moderate, the Loss Magnitude would likely be Moderate, based on the example risk matrix below.

Primary Loss Magnitude (PLM)	Loss Magnitude (LM)					
	VH	M	H	VH	VH	VH
	H	L	M	H	VH	VH
	M	VL	L	M	H	VH
	L	VL	VL	L	M	H
	VL	VL	VL	VL	L	M
		VL	L	M	H	VH
	Secondary Loss					

Figure 13: Example Risk Matrix for Loss Magnitude

2.1.4 Stage 4: Derive and Articulate Risk

Now that LEF and Loss Magnitude (including Secondary Loss) have been evaluated, Risk is simply derived from the probable LEF and probable Loss Magnitude.

Assuming that the example risk matrix below has been “approved” by the leadership of the fictional bank, the Risk associated with this scenario would be Low – based upon a Low

probable LEF (between 0.1 and 1 times per year) and a Moderate probable Loss Magnitude (between \$100K and \$1M).

	Risk					
	VH	M	H	VH	VH	VH
Loss Magnitude (LM)	H	L	M	H	VH	VH
	M	VL	L	M	H	VH
	L	VL	VL	L	M	H
	VL	VL	VL	VL	L	M
		VL	L	M	H	VH
	Loss Event Frequency (LEF)					

Figure 14: Example Risk Matrix for Risk

## 2.2 Analysis Using the Open FAIR Risk Analysis Tool

The quantitative analysis in this section demonstrates use of the Open FAIR Risk Analysis Tool. The example scenario is the same as the analysis using the example qualitative scales. Some of the simulated calibrated estimates for minimum, most likely, and maximum may vary from the values in the qualitative approach.

### 2.2.1 Stage 1: Identify the Loss Scenario (Scope the Analysis)

For consistency, the Loss Scenario for the quantitative analysis of the example scenario is exactly the same as the qualitative analysis.

*Cleaning crew member(s) find and copy an 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.*

### 2.2.2 Stage 2: Evaluate Loss Event Frequency

For consistency, this quantitative version of the analysis evaluates LEF by estimating values for Threat Capability and Resistance Strength. This is done deliberately to demonstrate finding estimates for more risk factors, despite guidance in the O-RA Standard, Version 2.0 to utilize a top-down approach only estimating lower-level risk factors if necessary for the purpose of the analysis.

However, this quantitative version of the analysis estimates TEF directly instead of attempting to derive it by estimating Contact Frequency and Probability of Action – rarely in a real-world analysis will a risk analyst need or be able to derive TEF from Contact Frequency and Probability of Action, so this quantitative version of the analysis utilizes the same approach.

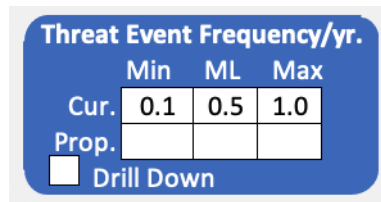
### 2.2.2.1 Estimate the Threat Event Frequency

As stated previously, contact has been determined to occur regularly between the cleaning crew and the Asset – once per week. However, not every Contact Event always results in a Threat Event, so TEF will be less than Contact Frequency.

This quantitative version of the analysis also *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.

As a result, TEF is estimated to have a minimum of 0.1 events per year, a maximum of 1 event per year, and a most likely of 0.5 events per year. The minimum and maximum values come from the ends of the qualitative TEF scale from Section 2.1.2.1, with the most likely value being chosen as the median.

The values for TEF are input to the Open FAIR Risk Analysis Tool.



Threat Event Frequency/yr.			
	Min	ML	Max
Cur.	0.1	0.5	1.0
Prop.			

Drill Down

**Figure 15: Threat Event Frequency in the Open FAIR Risk Analysis Tool**

Note: Values are only input into the boxes for Current (Cur.) risk analysis; no changes have been proposed that would impact the analysis and provide values for boxes for a Proposed (Prop.) risk analysis. Therefore, these boxes are left empty. This will be the case for future figures, too.

### 2.2.2.2 Estimate Vulnerability

In this quantitative version of the risk analysis, Threat Capability is still based on the skill (in this case, reading ability) and resources (time) the average member of this Threat Community can use against a password written on a sticky-note.

For consistency, this quantitative version of the analysis will also estimate Vulnerability by comparing Threat Capability to Resistance Strength and working at the lower level of the Open FAIR taxonomy.

However, Threat Capability in this case is estimated without a qualitative scale. 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. These values are input to the Open FAIR Risk Analysis Tool.

Threat Capability		
	Cur.	Pro.
Min	25%	
ML	50%	
Max	75%	

**Figure 16: Threat Capability in the Open FAIR Risk Analysis Tool**

Resistance Strength is also estimated without a qualitative scale. As a result, the calibrated estimate for Resistance Strength maximum is 4%, the minimum is 0%, and the most likely is 2%, which are input to the Open FAIR Risk Analysis Tool.

Resistance Strength		
	Cur.	Pro.
Min	0%	
ML	2%	
Max	4%	

**Figure 17: Resistance Strength in the Open FAIR Risk Analysis Tool**

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 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.



### 2.2.2.3 Estimate Loss Event Frequency

Figure 18 displays the result of the analysis of TEF and Vulnerability from the Open FAIR Risk Analysis Tool.

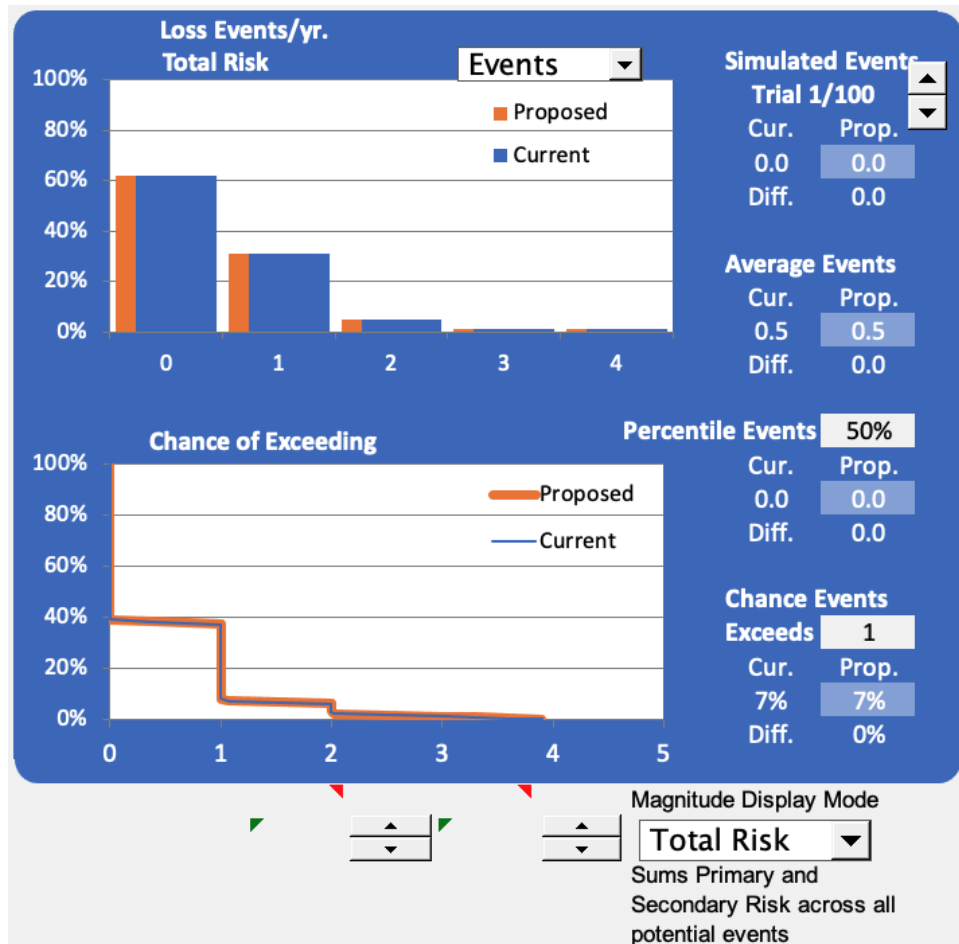


Figure 18: Loss Event Frequency in the Open FAIR Risk Analysis Tool

Figure 18 indicates that 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.

### 2.2.3 Stage 3: Evaluate Loss Magnitude

This section works to evaluate Loss Magnitude. Loss Magnitude is comprised of the PLM, which is the direct consequence of the Loss Event, and Secondary Loss, which is in turn comprised of the SLEF and SLM. This quantitative version of the analysis uses calibrated estimates for these risk factors instead of qualitative scales.

2.2.3.1 *Estimate the Primary Loss Magnitude*

This quantitative version of the risk analysis will also focus on the two actions identified as being most likely for the Threat Community to take that would cause a Primary Loss:

- **Access** – the cleaning crew does not have authorized access to the sensitive employee information
- **Misuse** – employee records typically have information that can be used to execute identity theft, which introduces potential legal and reputation loss

This quantitative version of the risk analysis also *assumes* that the volume of compromised employee information would be limited to the number of employee records in the system.

The next step is to estimate the PLM for access and misuse, which would directly cause productivity and responses losses for the Primary Stakeholder.

Forms of Loss					
Productivity	Response	Replacement	Fines and Judgments	Competitive Advantage	Reputation
✓	✓	—	—	—	—

The estimates for PLM 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  
The calibrated estimate for PLM minimum is \$10,000, the most likely is \$45,000, and the maximum is \$60,000, which are input to the Open FAIR Risk Analysis Tool (in thousands).
- **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  
A common source for this data would be other incidents the organization may have experienced, or in some cases, industry data. The calibrated estimate for PLM minimum is \$100,000, the most likely is \$300,000, and the maximum is \$800,000, which are input to the Open FAIR Risk Analysis Tool (in thousands).

Primary Loss Magnitude			
Current	Min	ML	Max
Productivity	10	45	60
Replacement			
Response	100	300	800
Reputation			
Competitive Adv.			
Judgments			
Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

**Figure 19: Primary Loss Magnitude in the Open FAIR Risk Analysis Tool**

This quantitative version of the risk analysis also does not estimate PLM for replacement, fines and judgments, competitive advantage, or reputation. Given the definitions for Primary and Secondary Loss, as well as the individual definitions for each of these forms of loss, some of these forms of loss are more relevant for Secondary Loss in this scenario.

**2.2.3.2 Estimate the Secondary Loss**

In this quantitative version, little is changed for any Secondary Losses. Regulators may still react negatively to an event where a large loss of employee-sensitive information was compromised, at least in part because of questions the event might raise regarding controls over customer information, and how severely regulators react will likely be a function of their perception of the existing overall control environment.

Since customer information is still not involved in this scenario, this quantitative version of the risk analysis also *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.

Although most Loss Scenarios will not treat employees as Secondary Stakeholders, there are the same exceptions in this example that make it reasonable to treat them as Secondary Stakeholders: the affected employees could potentially leave the organization and/or file lawsuits. These possible actions mean Secondary Losses would come from fines and judgments by regulators, which would also create secondary response losses.

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

This quantitative version of the risk analysis also *assumes* that all 15,000 employee records are taken. The rationale is the same: If someone is going to take the personal risk of performing this sort of illicit action, they are likely to try to maximize the value proposition. This means that the Primary Stakeholder will experience secondary response losses and fines and judgments (by regulators) for the SLM.

Forms of Loss					
Productivity	Response	Replacement	Fines and Judgments	Competitive Advantage	Reputation
—	✓	—	✓	—	—

Estimates for the volume of response losses and fines and judgments can then be estimated using the following rationale:

- Response** – in this scenario, response costs would include executive time spent in meetings, notification costs, credit monitoring, and expenses associated with inside and outside legal counsel

The calibrated estimate for SLM minimum is \$100,000, the most likely is \$200,000, and the maximum is \$300,000, which are input to the Open FAIR Risk Analysis Tool (in thousands). A specific breakdown is:

  - Executive time: 40 hours @ \$300 per hour = \$12,000
  - Notification costs: \$5 per employee
  - Credit monitoring: \$25 \* 15,000 employees \* 5% acceptance rate = \$18,750
  - Legal expenses: \$100,000
  - **TOTAL:** \$200,000 (most likely value)
- Fines and Judgments** – provided that the company was not negligent in handling the event, and made a concerted effort to protect employee interests, fines and judgments should be low (if any at all)

The calibrated estimate for SLM minimum is \$0, the most likely is \$10,000, and the maximum is \$20,000, which are input to the Open FAIR Risk Analysis Tool (in thousands).

No productivity loss would occur as a Secondary Loss because the organization is still able to provide its goods and services.

No material reputation damage is expected to occur because it was an internal event, no customers were affected, and the organization had a security program in place that included policies and education. If, however, the organization had a problematic relationship with its employees or community, an argument could be made that the employee turnover and challenges with hiring could result, the effects of which could be characterized as reputation damage.

No damage to competitive position would occur because their competitors would not have improved their products and services, nor did the products and services of the organization diminish.

Note: If any employees actually suffered loss through identify theft, it is possible that the organization would have to cover those losses. In such a case, those losses would be accounted for as secondary replacement costs.

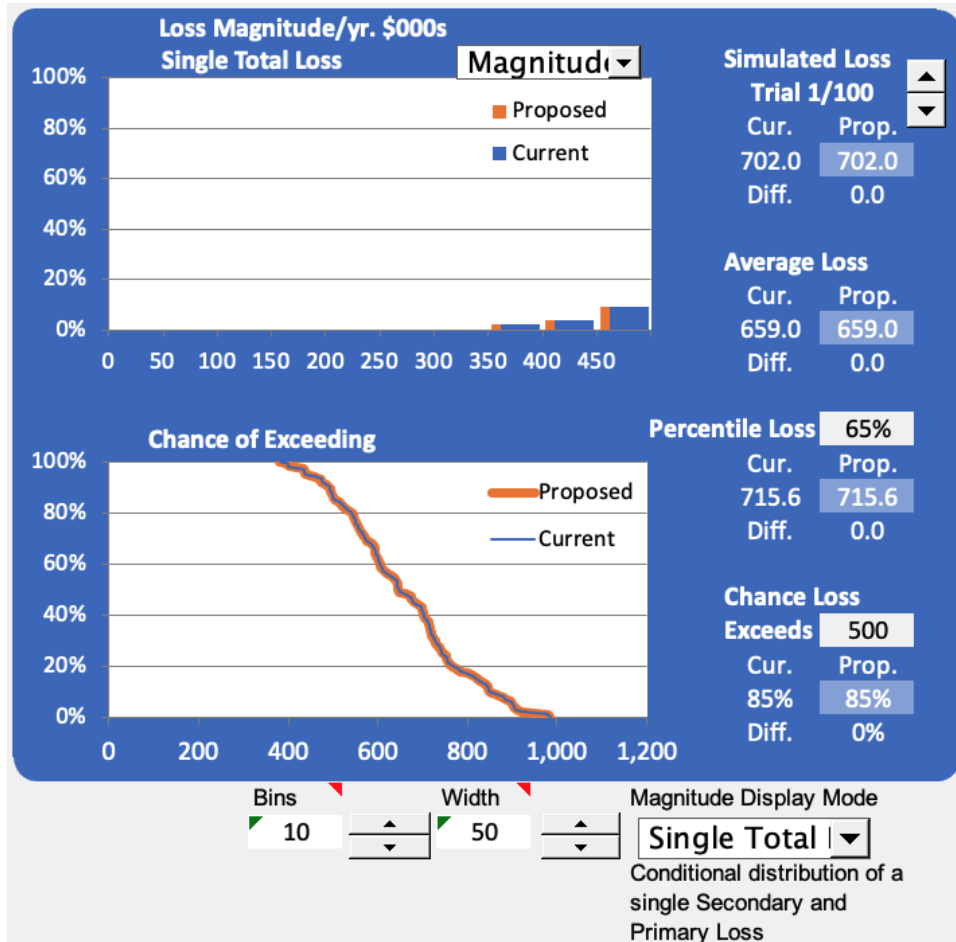
The most likely values for SLM for response losses and fines and judgments were derived from calculations and rationale above and are input to the Open FAIR Risk Analysis Tool along with the calibrated estimates for SLEF from above.

Secondary Loss				
		Min	ML	Max
SLEF	Current	90%	95%	99%
	Proposed			
Current SLM		Min	ML	Max
	Productivity			
	Replacement			
	Response	100	200	300
	Reputation			
	Competitive Adv.			
	Judgments	0	10	20
Proposed		Min	ML	Max
	Productivity			
	Replacement			
	Response			
	Reputation			
	Competitive Adv.			
	Judgments			

Figure 20: Secondary Loss in the Open FAIR Risk Analysis Tool

2.2.3.3 Estimate Loss Magnitude

Figure 21 displays the combined Loss Magnitude results for a single estimated Loss Event from the Open FAIR Risk Analysis Tool.



**Figure 21: Loss Magnitude for a Single Total Loss in the Open FAIR Risk Analysis Tool**

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 21 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.

## 2.2.4 Stage 4: Derive and Articulate Risk

Figure 22 displays the results of the quantitative risk analysis performed by the Open FAIR Risk Analysis Tool.

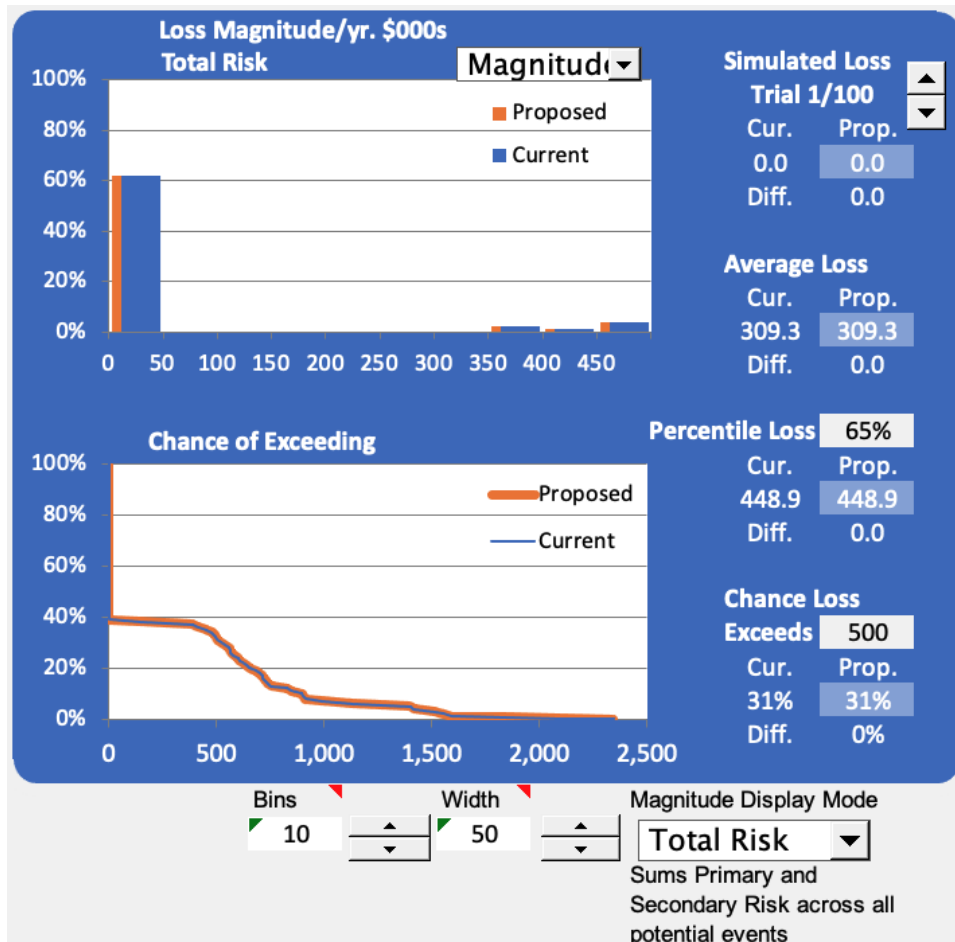


Figure 22: Total Risk in the Open FAIR Risk Analysis Tool

Figure 22 indicates the total risk (accounting for both LEF and Loss Magnitude) estimated in the quantitative version of the analysis. Figure 22 depicts 100 trials<sup>6</sup> 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.

## 2.3 Quantitative and Qualitative Analysis Result Comparison

The qualitative version of the risk analysis result is a Low risk of \$10,000 to \$99,999. This result presents an issue with range compression,<sup>7</sup> though: The Very Low category encompasses up to \$10,000 of loss; the Low category encompasses \$89,999 of loss (from \$10,001 to \$100,000); the

<sup>6</sup> The Open FAIR Risk Analysis Tool simulates 100 years of outcomes by default, which can be adjusted according to preference.

<sup>7</sup> For more information on this subject, see Hubbard & Evans (2010).

Moderate category encompasses \$899,999 of loss (from \$101,001 to \$1,000,000); the High category encompasses \$8,999,999 (from \$1,000,001 to \$10,000,000); and the Very High category encompasses loss above \$10,000,000. This loss of resolution increases the difficulty of making a decision based on the results because the categories are so broad and increase in size as losses become larger. Moreover, there is no indication of the frequency of Loss Events.

The quantitative version of the risk analysis shows an average loss of around \$300,000. This falls within the Moderate range of the example qualitative scale for Loss Magnitude from the qualitative version of the analysis, shown below. This contrasts with the estimate of Low from the qualitative version of the analysis.

Magnitude	Range Low End	Range High End
Very High (VH)	\$10,000,000	—
High (H)	\$1,000,000	\$9,999,999
Moderate (M)	\$100,000	\$999,999
Low (L)	\$10,000	\$99,999
Very Low (VL)	\$0	\$9,999

**Figure 23: Example Qualitative Scale for Loss Magnitude**

In Figure 22, the bar graph for Loss Magnitude from the quantitative version of the analysis also shows that in about 60% of the simulated trials, the losses would be considered Low if using the example qualitative scale for Loss Magnitude from the qualitative version of the analysis that is shown in Figure 23. In other words, about 60% of losses fall between \$10,000 and \$99,999.

However, the shorter bars starting at \$350,000 coupled with a chance of loss exceeding \$500,000 as 31% (or the chance of loss exceeding \$500,000 occurring once every ~3 years) shows a probability of a Moderate loss, if utilizing the example qualitative scale for Loss Magnitude from the qualitative version of the analysis.

In this example, the quantitative version of the risk analysis result indicates higher average risk than the qualitative analysis. The quantitative analysis also provides specifics on the potential frequency and magnitude of loss, making the results more defensible to decision-makers who must determine what, if anything, they should do.

### 2.3.1 Risk Analysis Quality Considerations

There are several other areas that would impact the usefulness of a qualitative risk analysis *versus* a quantitative risk analysis.

- For a qualitative risk analysis, cells in a matrix that intersect similar levels of loss (e.g., High Primary Loss and High Secondary Loss) could be shown as the next higher level. In other words, the cell that intersects High loss for both Primary and Secondary could be labeled “VH” and colored red; i.e., interpreting that two “High-risk” conditions result in Very High Overall Risk. This is a conservative view, which may be appropriate depending on the organization’s capacity for loss or management’s tolerance for loss.



- Qualitative statements of risk (e.g., “High”, “Moderate”) should reflect the organization’s capacity for loss or management’s tolerance for loss

For example, the scale below essentially can be interpreted to mean that loss exposures of greater than \$10M will be considered “Very High” risk and typically treated as such through the application of resources to mitigate the exposure. Organizations of different sizes and risk tolerances will define a different scale based on how management would like results communicated; these different labels may be influenced by actions management will take based on magnitude.

Magnitude	Range Low End	Range High End
Very High (VH)	\$10,000,000	—
High (H)	\$1,000,000	\$9,999,999
Moderate (M)	\$100,000	\$999,999
Low (L)	\$10,000	\$99,999
Very Low (VL)	\$0	\$9,999

**Figure 24: Example Qualitative Scale for Risk based on Range for Loss Magnitude**

In a real analysis, the risk analyst may choose to evaluate and report on more than one Threat Community or more than one type of Loss Event. However, sometimes by initially assessing the most probable and perceived significant scenario, that single scenario may provide enough information to lead to a well-informed decision, particularly if the results are expressed quantitatively according to the preference of the decision-maker(s).

## 3 Using Open FAIR Risk Analysis to Inform Business Decisions

---

This chapter presents examples<sup>8</sup> of using Open FAIR risk analysis results to inform business decisions about proposed security changes. The examples use a spreadsheet based on Appendix A of the Open FAIR Risk Analysis Process Guide to organize the analysis. The Open FAIR Risk Analysis Tool is used to perform the risk analysis. The examples include the full rationale for calibrated estimates used. The intent of each case is to answer the question: “What do we do about the identified risk?”

Each section presents a different example of using Open FAIR risk analysis results in a business case. These different examples include considerations such as the risk assessment framework used by the organization (e.g., from NIST, ISO/IEC). The sections follow the same structure as the stages described in the O-RA Standard, Version 2.0, beginning with identifying the Loss Scenario before evaluating LEF, evaluating Loss Magnitude, and finally deriving and articulating risk; they conclude by preparing the business case.

### 3.1 Risk Associated with Unstructured Data

This is an entirely fictional example<sup>9</sup> but uses a real product (with its name obfuscated) to demonstrate how an Open FAIR risk analysis can be used to demonstrate business value of a risk mitigation proposal.

#### 3.1.1 Background

An organization executive, John T. Boss, has become concerned by reports of new features in a competitor’s product that are suspiciously like proprietary capabilities in his organization’s product. He engages the risk analyst to initiate a risk analysis in which John T. Boss is identified as the Primary Stakeholder.

The Primary Stakeholder identifies an initial risk question with a defined scope. The risk analyst facilitates documenting the Primary Stakeholder’s perspective which is refined into the Loss Scenario that will be analyzed.

At this point the risk analyst works with appropriate staff to identify investment options for reducing risk and possibly cost. This example assumes that one risk reduction investment, implementing Product X, has been identified. Ultimately the analysis must demonstrate the expected business benefits of implementing Product X.

The example begins with the current risk scenario, then follows with the scenario accounting for implementing the proposed security product. It concludes with the Open FAIR analysis results.

---

<sup>8</sup> Version 1.0 of this document is published with only one example, but The Open Group Security Forum welcomes additional, contributed examples to expand this section (see Section 1.3: Future Directions).

<sup>9</sup> This example is not based on any real-world scenario, but instead depicts a common potential scenario; any similarities to a real scenario are entirely coincidental, and the example should not be interpreted as being typical.

### 3.1.2 Current Scenario

#### 3.1.2.1 Stage 1: Identify the Loss Scenario

Table 1 defines the current scenario.

**Table 1: Current Scenario**

<b>Risk Analysis Introduction</b>	
<b>Primary Stakeholder</b>	John T. Boss
<b>Risk Analyst</b>	C.T. Carlson
<b>Initial Risk Question</b>	What is the risk associated with employees selling product development information to competitors?
<b>Scope of Analysis</b>	Enterprise
<b>Purpose of Analysis</b>	Initial “Greenfield” risk analysis of current state.
<b>Primary Stakeholder Perspective</b>	
<b>Asset at Risk</b>	Product development information (intellectual property/trade secrets).
<b>Asset Details</b>	Product development information in the form of unstructured data, including a broad array of files related to the business, all in a human-intelligible form (e.g., Microsoft® Word, Excel, PowerPoint® files). These files are all proprietary information.
<b>Threat Actor</b>	Organization employee motivated by monetary gain.
<b>Indication of Loss</b>	Our new-to-market capabilities appearing in competitor products much shorter than likely development cycle.
<b>Risk Title</b>	Threat of trade secrets by an employee motivated by potential monetary gain.
<b>Short Risk Title</b>	Insider Threat
<b>Loss Scenario</b>	
<b>Asset Type</b>	Trade secrets
<b>Asset Details</b>	Information found in Microsoft Office documents stored on Windows® file sharing and SharePoint® sites.
<b>Loss Category</b>	Confidentiality
<b>Threat Actor Category</b>	Insider disgruntled.
<b>Threat Action</b>	Insider Threat Agent removes copies of files from the Windows or UNIX® host to a location outside the organization.

Loss Scenario Analysis	
<b>Current Scenario</b>	Insider Threat
<b>Current Risk Scenario</b>	An insider removes copies of files from Windows or UNIX host to a location outside the organization with the intent to sell proprietary information to a competitor.

### 3.1.2.2 Stage 2: Evaluate Loss Event Frequency

A Loss Event occurs when unstructured proprietary data is sold to a competitor who uses the information to enhance their product to improve their competitive position. First, an insider must intentionally export files containing the unstructured proprietary information (e.g., words and images developed with typical applications) by sending them to an Internet location outside the organization (e.g., their home).

The analysis begins with the risk analyst determining the Open FAIR taxonomy level at which calibrated estimates can be developed for LEF.

#### 3.1.2.2.1 Estimate the Loss Event Frequency – Threat Event Frequency

The risk analyst determines that LEF cannot be estimated directly, but that TEF can.

**Table 2: Current Scenario Loss Event Frequency**

Loss Event Frequency (LEF)			
Determining the LEF for a risk scenario. If performing a comparison, enter first scenario and second scenario in different workbooks.	Response/ Detailed Comments	Assumptions	Additional Comments
Is there sufficient data about the chosen scenario to determine the LEF?	No		

**Table 3: Current Scenario Loss Event Frequency Drilldown**

LEF Drilldown – Threat Event Frequency (TEF)			
Determining the TEF.	Response/ Detailed Comments	Assumptions	Additional Comments
Drill down to TEF level for the analysis?	Yes		
Are TEF values known directly?	Yes		

<b>LEF Drilldown – Threat Event Frequency (TEF)</b>			
Provide TEF details on data available	The organization has daily authorized access to computing files (Windows file shares, SharePoint) by its 10,000 organization employees (Contact Frequency). Personnel security controls reduce the Probability of Action (i.e., theft) to a very low frequency. However, an FBI investigation of cyber crime identified a large volume of stolen computing files in the possession of an outsider, apparently for sale to a competitor.	The organization's employees are expected to have: <ul style="list-style-type: none"> <li>• Been screened prior to being hired</li> <li>• Signed an employee agreement establishing their responsibility to protect information</li> </ul> The organization's threat monitoring is able to detect and respond to perimeter and network Threat Events, but lacks the capability to detect abnormal accesses to computing files.	
Is the data available current?	Yes		
Have there been any changes to the environment since the data was collected?	No		
If sufficient data exists and is determined to be stable and reliable, TEF may be determined directly. Many times it is possible to determine TEF without drilling down to Contact Frequency and Probability of Action.			
Check response above for next action.	Proceed to answers below.		
Provide the timeframe to be used for the LEF measure (e.g., data for 10-year period).	Annual		

<b>LEF Drilldown – Threat Event Frequency (TEF)</b>			
Over that timeframe what are the number of Threat Events where the Threat Agent(s) in the Loss Scenario may come into contact with the asset(s)?	The computing files collected by the FBI suggests at least five separate events in one year based on file date stamps. As there are multiple competitors, it is probable that activities of other cyber criminals have not been detected.	All employees have daily contact with some data files. It is reasonable to anticipate that a very small number would not be deterred by having signed an information protection agreement, stealing proprietary information.	As a result, the estimate of TEF is a minimum of five events/year and a maximum events/year of 15, with a most likely value of 10 events/year.
Based upon the timeframe and number of events, what is the derived TEF in units of events per unit time? Provide a range: min, most likely, max. If the Threat Event occurs less than once per year, represent as a fraction; e.g., once every ten years = 1/10 = .1			
Threat Event Frequency	TEF – Min Value	TEF – Most Likely Value	TEF – Max Value
Input Values	5	10	15

3.1.2.2.2 Estimate the Current Loss Event Frequency – Vulnerability

The risk analyst determines that the current Vulnerability can be estimated directly.

**Table 4: Current Scenario Vulnerability**

<b>LEF Drilldown – Vulnerability (Vuln)</b>			
Determining the Vulnerability or Susceptibility of the Asset to a compromise by the Threat Agent.	Response/ Detailed Comments	Assumptions	Additional Comments
May we drill down to the Vulnerability level for the analysis?	LEF unknown; please enter Vulnerability information.		
Are Vulnerability values known directly? Input Yes if we think we know Vulnerability; otherwise, enter No to drill down into Threat Capability and Resistance Strength.	Yes		
Evaluate answer above.	Enter Vulnerability information below.		

**Table 5: Current Scenario Vulnerability Analysis**

<p>If sufficient data exists and is determined to be stable and reliable, Vulnerability may be determined directly. It is sometimes possible to determine Vulnerability without drilling down to Threat Capability and Resistance Strength when sufficient data is available.</p>			
<p>If you have chosen to input Vulnerability directly, how was Vulnerability derived? Provide details.</p>	<p>Vulnerability is related to the quantity of files that categories of employees are authorized to access (i.e., have at least a “read” access authorization). The Vulnerability related to newer employees (i.e., files for which they do have authorized access) will be far less than for the most senior employees. While these senior employees have greater authorized access, the authorization is likely constrained to their specialty (engineering, finance, marketing, personnel, etc.).</p> <p>The estimate for Vulnerability maximum is 80% for the senior employees who have authorized access to many but not all files; the estimate for Vulnerability minimum is 5% for the most junior employees; and the estimate for Vulnerability most likely value is 40% for the average employee.</p>	<p>By default, employees cannot access any group of Windows file shares or SharePoint sites. Access for a specific group is granted (access authorization) through an access management process resulting in the user being allowed for read-only access or full access.</p>	<p>While employees have unlimited frequency of access to files for which they are authorized, the access management process does limit the number of files they are authorized to access. However, the access management process rarely removes access once authorized (even in the case when the employee leaves the organization). As employees move to different functions of the organization, they will collect more access authorizations over time. Therefore, an insider has the capability of stealing any file to which they have previously been granted access.</p>
<p>Is the available data current?</p>	<p>Yes</p>		
<p>Have there been any changes to the environment since the data was collected?</p>	<p>No</p>		
<p>Provide the percentage of Threat Events that become Loss Events.</p>			

Vulnerability	Vuln – Min Value	Vuln – Most Likely Value	Vuln – Max Value
Input Values	5%	40%	80%

### 3.1.2.3 Stage 3: Evaluate Loss Magnitude

#### 3.1.2.3.1 Estimate the Proposed Primary Loss Magnitude

Currently there is no means of detecting and therefore responding to Loss Events for this situation; hence, there is no estimate for PLM which is composed only of response loss.

#### 3.1.2.3.2 Estimate the Secondary Loss

The risk analyst identifies the Secondary Stakeholder as a competitor. While they do not suffer a loss, they are considered a Secondary Stakeholder<sup>10</sup> as a best fit to the definition<sup>11</sup> in the Open FAIR Body of Knowledge, since they potentially cause an additional loss to the Primary Stakeholder as a result of fallout from the Primary Loss.

**Table 6: Current Scenario Secondary Loss Event Frequency**

Secondary Loss Event Frequency (SLEF) – The percentage of Primary Loss Events resulting in Secondary Loss Events; e.g., minimum 90%, most likely 95%, maximum 100%.				
Secondary Stakeholders affected	SLEF – Minimum	SLEF – Most Likely	SLEF – Maximum	Assumptions
Competitors	0%	10%	20%	Potential financial reward is the likely motivation for intellectual property theft. Data from the FBI investigation shows roughly five attacks by one criminal, suggesting difficulty finding valuable information, which suggests at best a 1 in 5 chance of loss being realized from a Threat Event. Also, the potential of translating stolen information into a competitive product is not assured. Together a low frequency of Secondary Loss is assumed for each Threat Event.

<sup>10</sup> According to Section 4.5.2 of the O-RT Standard, Version 3.0: “Although called ‘Secondary Stakeholders’, they are most accurately viewed as ‘Secondary Threat Agents’ when they begin acting against the Primary Stakeholder’s Assets.”

<sup>11</sup> Use the terms within the Open FAIR Body of Knowledge to the best extent you can in your analysis. They may not always work perfectly, so be pragmatic. Document how you interpreted and utilized the Open FAIR terms in your analysis, particularly if they do not exactly match the Open FAIR Body of Knowledge.



**Table 7: Current Scenario Secondary Loss Magnitude**

Secondary Competitive Losses				
Competitive Loss Type	Minimum	Most Likely	Maximum	Assumptions
Revenue lost to competitor	\$100,000	\$600,000	\$900,000	Competitive advantage resulting from stolen intellectual property would begin sometime in the future. Estimates provided by the marketing organization suggest estimated annual values of revenue losses, with a minimum loss of \$100,000, a maximum loss of \$900,000, and a most likely loss of \$600,000, considering both loss of sales and discounting.
Competitive Loss Totals	\$100,000.00	\$600,000.00	\$900,000.00	

**3.1.3 Proposed Scenario**

The proposed scenario accounts for the implementation of Product X. Capabilities include:

- Empowering data owners to view and manage permissions to files, folders, SharePoint sites, and security groups
- Facilitating consistent review of access to groups, distribution lists, and sensitive business data by the right people
- Providing an easy-to-use web form for users to request access to Windows files and SharePoint sites, with each request automatically routed to the proper stakeholders who approve access
- Providing alerts on potential Threat Events, such as unusual access to sensitive data by insiders

**3.1.3.1 Stage 1: Identify the Loss Scenario**

Table 8 defines the proposed scenario.

**Table 8: Proposed Scenario**

Proposed Improvement	Implement Product X
<b>Current Loss Scenario</b>	An insider removes copies of files from the Windows or UNIX host to a location outside the organization.

<b>Proposed Improvement</b>	<b>Implement Product X</b>
<b>Improvement Overview</b>	Product X (fictitious name) will be evaluated as follows: <ul style="list-style-type: none"> <li>• Processing access requests – reduced cost for employees awaiting access</li> <li>• Removing unneeded access – reduced Vulnerability</li> </ul>
<b>Selection Rationale</b>	A market survey and an options analysis were performed, resulting in the identification of a product that meets requirements.
<b>Security Control Improvement Opportunity</b>	An organization’s Chief Information Security Officer (CISO) has identified a collection of issues with the protection and management of unstructured data stored in Windows file shares, SharePoint, and in UNIX files: <ul style="list-style-type: none"> <li>• Processing access requests – request initiation, manager approval, data owner approval, update access</li> <li>• Removing unneeded access – discover unneeded access, request removal, update access</li> <li>• Detecting anomalous behavior – discover a user performing unusual action (e.g., sending a large quantity of files to a non-organization address)</li> </ul>
<b>Potential Risk/Cost Reduction</b>	Product X (fictitious name) will be evaluated as follows: <ul style="list-style-type: none"> <li>• Processing access requests – reduced cost for employees awaiting access</li> <li>• Removing unneeded access – reduced Vulnerability</li> <li>• Detecting anomalous behavior – reduced cost for individual incident response</li> </ul>

3.1.3.2 *Stage 2: Evaluate Loss Event Frequency*

A Loss Event for unstructured data occurs when the insider exfiltrates files from the Windows or UNIX host to a location outside the organization’s control. In this case, the insider exports files containing the unstructured data (e.g., words and images developed with typical applications) by sending them to an Internet location outside the organization (e.g., their home).

The risk analyst determines the level at which calibrated estimates can be developed.

3.1.3.3 *Estimate the Loss Event Frequency – Threat Event Frequency*

Product X is implemented in the organization without employees being informed. Therefore, the proposed scenario does not change TEF.<sup>12</sup>

<sup>12</sup> If employees are informed that Product X is being implemented, the Probability of Action of an insider acting against the organization might be reduced due to perceiving an increased risk of being caught and suffering undesirable consequences – the reduced Probability of Action, in turn, would result in a reduced TEF. If the organization chose to inform employees, it could potentially further reduce risk by removing or reducing the incentive of employee(s) acting.

3.1.3.4 *Estimate the Current Loss Event Frequency – Vulnerability*

The risk analyst determines that Vulnerability can be estimated directly for the proposed scenario.

**Table 9: Proposed Scenario Vulnerability**

<b>LEF Drilldown – Vulnerability (Vuln)</b>			
Determining the Vulnerability or Susceptibility of the Asset to a compromise by the Threat Agent.	Response/ Detailed Comments	Assumptions	Additional Comments
May we drill down to the Vulnerability level for the analysis?	LEF unknown; please enter Vulnerability information.		
Are Vulnerability values known directly? Input Yes if we think we know Vulnerability; otherwise, enter No to drill down into Threat Capability and Resistance Strength.	Yes		
Evaluate answer above.	Enter Vulnerability information below.		
If sufficient data exists and is determined to be stable and reliable, Vulnerability may be determined directly. It is sometimes possible to determine Vulnerability without drilling down to Threat Capability and Resistance Strength when sufficient data is available.			
If you have chosen to input Vulnerability directly, how was Vulnerability derived? Provide details.	The projected situation after implementing Product X is that employees will have access only to the files they need. Senior employees may still have more authorized access than junior employees, but not nearly as many. Therefore, the estimates for Vulnerability are reduced assuming most users have only needed authorized access, while some portion of unnecessary authorized access remains.	Product X prompts people in access approval roles to review and validate current access authorizations. While implementation will occur in phases with significant effort at the beginning, it is assumed that the majority of unneeded access authorizations to groups of file shares or SharePoint sites will be removed by the end of one year.	
Is the data available current?	Yes		

LEF Drilldown – Vulnerability (Vuln)			
Have there been any changes to the environment since the data was collected?	No		
Provide the percentage of Threat Events that become Loss Events.			
Vulnerability	Vuln – Min Value	Vuln – Most Likely Value	Vuln – Max Value
Input Values	5%	15%	40%

3.1.3.5 *Stage 3: Evaluate Loss Magnitude U R HERE*

3.1.3.5.1 Estimate the Proposed Primary Loss Magnitude

The risk analyst provides an estimate for response loss since the proposed scenario includes an incident detection capability.

**Table 10: Proposed Scenario Primary Loss Magnitude**

Primary Response Losses				
Response Loss Type	Minimum	Most Likely	Maximum	Assumptions
Internal incident response costs	500	1,000	1,500	One feature of Product X is the capability to detect and alert anomalous behavior, such as an unusual pattern of file reads that could represent theft. In the case of the insider, their identity is known, so the investigation amounts to confronting the individual to ascertain what occurred. The cost would include the time of the investigator, the manager, and the employee. The response loss estimate for maximum is \$1,500 and for minimum is \$500, with the most likely value being \$1,000.
Response Loss Totals	\$500.00	\$1,000.00	\$1,500.00	

3.1.3.5.2 Estimate the Secondary Loss

Finally, the risk analyst provides an estimate for SLEF. SLM is not affected by implementing Product X.

**Table 11: Proposed Scenario Secondary Loss Event Frequency**

<b>Secondary Loss Event Frequency (SLEF) – The percentage of Primary Loss Events resulting in Secondary Loss Events; e.g., minimum 90%, most likely 95%, maximum 100%.</b>				
Secondary Stakeholders affected	SLEF – Minimum	SLEF – Most Likely	SLEF – Maximum	Assumptions
Competitors	0%	1%	2%	Product X provides alerting on anomalous events (e.g., reading file reads far in excess of a user’s normal pattern), triggering incident response within a day or two of the Threat Event. SLEF is assumed to be reduced because the employee may be confronted well before they deliver the files to a competitor. Also, employee awareness of this capability likely deters action which is also reflected in this estimate for simplicity rather than being considered in Probability of Action.

### 3.1.4 Analyze Risk

#### 3.1.4.1 Stage 4: Derive and Articulate Risk

##### 3.1.4.1.1 Record Calibrated Estimates

Figure 25 shows how the calibrated estimates of TEF and Vulnerability are recorded in the Open FAIR Risk Analysis Tool.

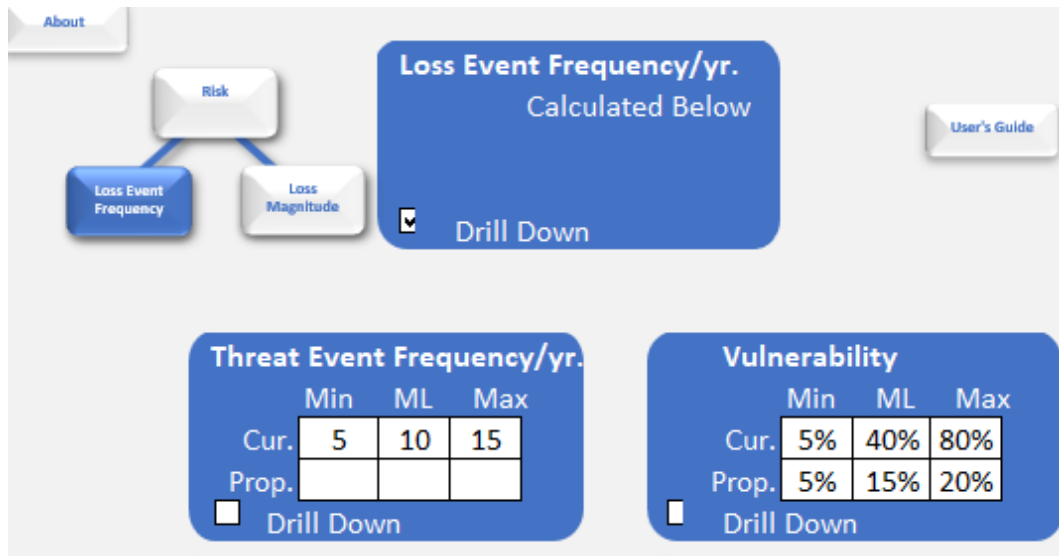


Figure 25: Record Loss Event Frequency in the Open FAIR Risk Analysis Tool

Figure 26 shows how the calibrated estimates of Loss Magnitude are recorded in the Open FAIR Risk Analysis Tool.

The screenshot displays the 'Loss Magnitude' section of the Open FAIR Risk Analysis Tool. At the top, a navigation menu includes 'About', 'Risk', 'Loss Event Frequency', and 'Loss Magnitude'. A blue box indicates 'Loss Magnitude Calculated Below' with a 'Drill Down' checkbox. A 'User's Guide' button is also present.

The interface is divided into two main panels: 'Primary Loss Magnitude' and 'Secondary Loss Magnitude'. Each panel contains tables for 'Current' and 'Proposed' states, with columns for 'Min', 'ML', and 'Max'.

**Primary Loss Magnitude Data:**

Current	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Proposed	Min	ML	Max
Productivity			
Replacement			
Response	0.5	1.0	1.5
Reputation			
Competitive Adv.			
Judgments			

**Secondary Loss Magnitude Data:**

SLEF	Current	Min	ML	Max
	Current	0%	10%	20%
	Proposed	0%	1%	2%

Current	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.	1000	6000	9000
Judgments			

Proposed	Min	ML	Max
Productivity			
Replacement			
Response			
Reputation			
Competitive Adv.			
Judgments			

Copyright © 2018 The Open Group®. All Rights Reserved.  
 Open FAIR™ is a trademark of The Open Group.  
 SIPmath™ is a trademark of ProbabilityManagement.org.

Figure 26: Record Loss Magnitude in the Open FAIR Risk Analysis Tool

3.1.4.1.2 View Risk Analysis Results

The results for frequency of Loss Events are shown in the Open FAIR Risk Analysis Tool.

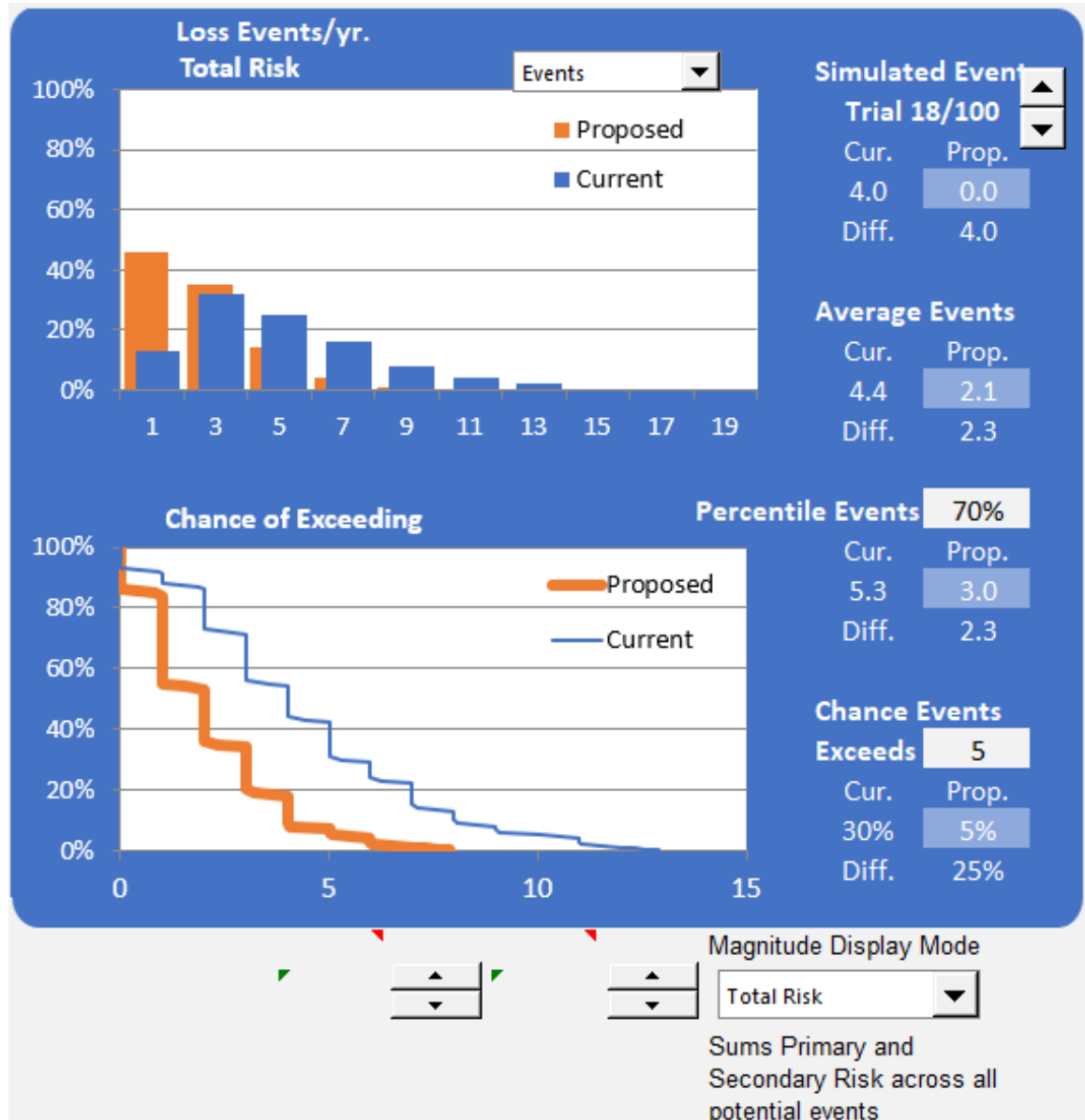
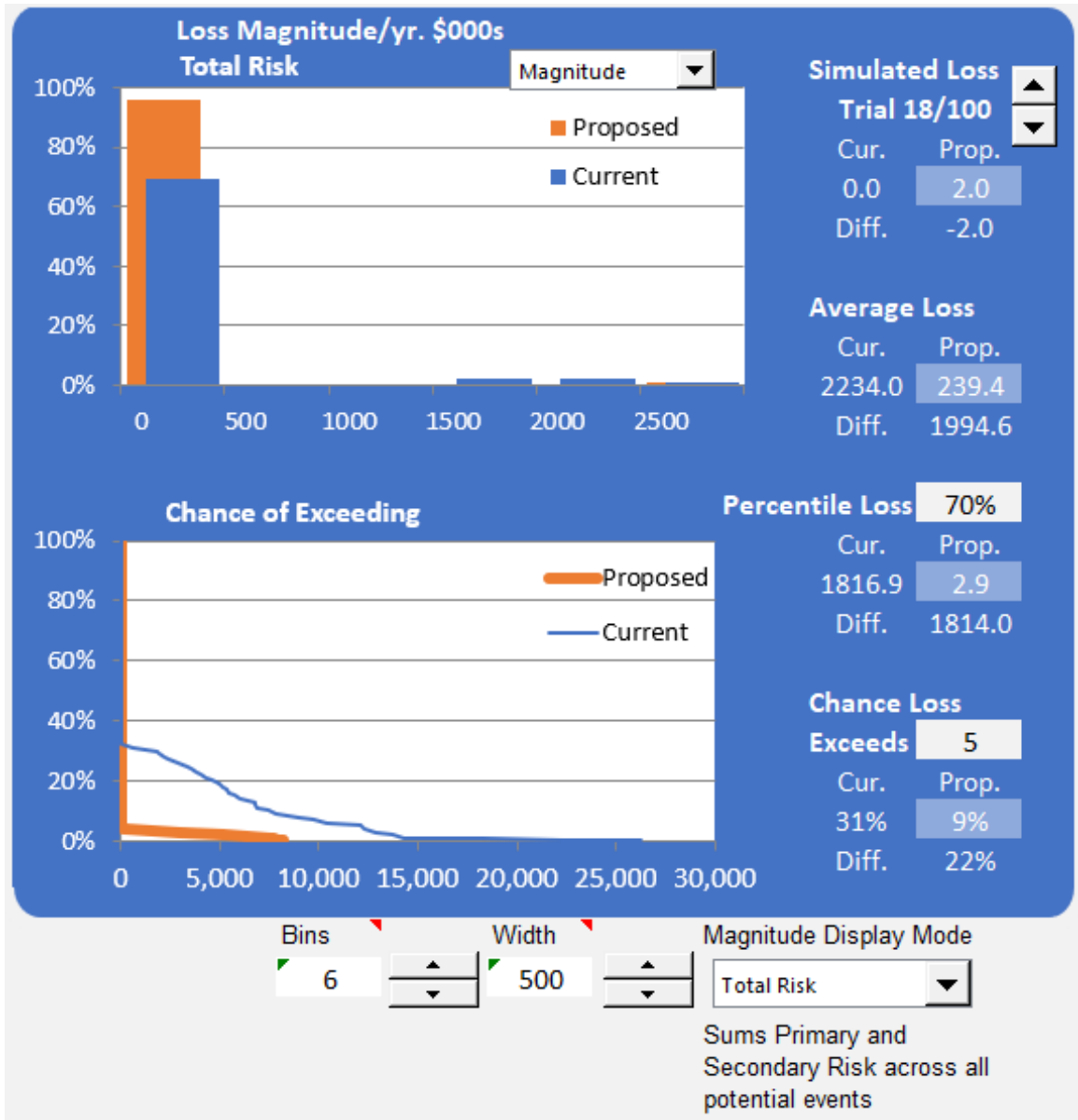


Figure 27: Display Loss Events in the Open FAIR Risk Analysis Tool

This analysis shows a significant reduction of Loss Events per year.



The Loss Magnitude results from the Open FAIR Risk Analysis Tool are shown in Figure 28.



**Figure 28: Adjust Percentile Loss in the Open FAIR Risk Analysis Tool**

These results show that risk before implementing Product X is about \$2.2 million<sup>13</sup> (average annualized loss exposure) and after implementing Product X is about \$240,000 (average annualized loss exposure). These values can then be used to prepare the business case.

<sup>13</sup> Estimates are kept at this level of precision to avoid presenting falsely overly precise estimates generated by the Open FAIR Risk Analysis Tool; this is a common issue of most tools.

### 3.1.5 Prepare Business Case

This section uses the relevant analysis results for both the current situation and then for implementing the proposed solution of Product X. The reduced risk (difference in average annualized loss exposure) is about \$2 million.

There is one additional benefit from Product X not related to risk: reduced delay of authorizing access for new employees, which would otherwise delay their productivity. In this case, the organization has 10,000 employees. The average turnover rate for employees in the organization is about 1,200 to 1,500 employees each year. The estimate for lost productivity is 20 to 30% for 2 to 10 days for delay in gaining access. The variation arises based on the number of different accesses required (time to request and to administer access), the number of different access requests required, and the variation in the delay associated with processing multiple access requests. An average employee fully-loaded hourly value is \$100. Averages are used to compute an annual productivity loss of:

$$1,350 \text{ employees} * (6 * 8 * .25) \text{ hours lost} * \$100 = \sim \$1.6 \text{ million annually}$$

The proposed project costs include the initial and annual costs of Product X plus the costs of selecting and implementing the product. For simplicity, the business case compares the current average Loss Magnitude against the proposed average Loss Magnitude plus the product's annual cost.

**Table 12: Return on Investment Analysis**

**Capital Budgeting – Return-on-Investment (ROI) Analysis**

<b>Investment overview</b>	
<b>Project name:</b>	Product X
<b>Project sponsor:</b>	John T. Boss
<b>Date of request:</b>	<Date>
<b>General description of benefits:</b>	Reduce risk of insider threat (employee)

<b>Cash flow and ROI statement</b>				
<b>BENEFIT DRIVERS</b>	<b>YEAR</b>			
	<b>0</b>	<b>1</b>	<b>2</b>	<b>3</b>
Reduced risk (mean of estimated annual)		\$2,000,000	\$2,000,000	\$2,000,000
Reduced productivity loss – new employee access		1,600,000	1,600,000	1,600,000
<b>Total annual benefits</b>		\$3,600,000	\$3,600,000	\$3,600,000
Implementation filter		33%	66%	100%
<b>Total annual benefits realized</b>		\$1,188,000	\$2,376,000	\$3,600,000

<b>Costs</b>	<b>Year 0</b>	<b>Year 1</b>	<b>Year 2</b>	<b>Year 3</b>
<b>Total</b>	\$1,300,000	\$800,000	\$800,000	\$500,000

<b>Benefits</b>	<b>Year 0</b>	<b>Year 1</b>	<b>Year 2</b>	<b>Year 3</b>
Annual benefit flow	(\$1,300,000)	\$388,000	\$1,576,000	\$3,100,000
Cumulative benefit flow	-1,300,000	-912,000	664,000	3,764,000

<b>Discounted benefit flow</b>	<b>Year 0</b>	<b>Year 1</b>	<b>Year 2</b>	<b>Year 3</b>
Discounted costs	\$1,300,000	\$761,905	\$725,624	\$431,919
Discounted benefits	0	1,131,429	2,155,102	3,109,815
Total discounted benefit flow	-1,300,000	369,524	1,429,478	2,677,897
Total cumulative discounted benefit flow	-1,300,000	-930,476	499,002	3,176,899

<b>Initial investment</b>	<b>Year 0</b>	<b>Year 1</b>	<b>Year 2</b>	<b>Year 3</b>
Initial investment	\$1,000,000	\$0	\$0	\$0
Implementation costs	300,000	300,000	300,000	0
Ongoing support costs	0	500,000	500,000	500,000
<b>Total costs</b>	\$1,300,000	\$800,000	\$800,000	\$500,000

<b>ROI measures</b>				
Cost of capital	5%			
Net present value	\$3,176,899			
Return on investment		55%	118%	199%
Payback (in years)	1.58			

This analysis could include more details, such as by replacing the average values, including those for acquiring and implementing the product, in the calculations with distributions and spreading them across multiple years. This example compares the discounted cash flows to determine payback on the investment.

# Glossary

## Action

An act taken against an Asset by a Threat Agent. Requires first that contact occurs between the Asset and Threat Agent.

## Asset

The information, information system, or information system component that is breached or impaired by the Threat Agent in a manner whereby its value is diminished or the act introduces liability to the Primary Stakeholder.

## Contact Event

Occurs when a Threat Agent establishes a physical or virtual (e.g., network) connection to an Asset.

## Contact Frequency (CF)

The probable frequency, within a given timeframe, that a Threat Agent will come into contact with an Asset.

## Control

Any person, policy, process, or technology that has the potential to reduce the Loss Event Frequency (LEF) – Loss Prevention Controls – and/or Loss Magnitude (LM) – Loss Mitigation Controls.

## FAIR

Factor Analysis of Information Risk.

## Loss Event

Occurs when a Threat Agent's action (Threat Event) is successful in breaching or impairing an Asset.

## Loss Event Frequency (LEF)

The probable frequency, within a given timeframe, that a Threat Agent will inflict harm upon an Asset.

## Loss Flow

The structured decomposition of how losses materialize when a Loss Event occurs.

**Loss Magnitude (LM)**

The probable magnitude of loss resulting from a Loss Event.

**Loss Scenario**

The story of loss that forms a sentence from the perspective of the Primary Stakeholder.

**Primary Stakeholder**

The person or organization that owns or is accountable for an Asset.

**Probability of Action (PoA)**

The probability that a Threat Agent will act against an Asset once contact occurs.

**Resistance Strength (RS)**

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.

**Risk**

The probable frequency and probable magnitude of future loss.

**Risk Analysis**

The process to comprehend the nature of risk and determine the level of risk. [Source: ISO Guide 73:2009]

**Risk Assessment**

The overall process of risk identification, risk analysis, and risk evaluation. [Source: ISO Guide 73:2009]

**Risk Factors**

The individual components that determine risk, including Loss Event Frequency, Loss Magnitude, Threat Event Frequency, etc.

**Risk Management**

Coordinated activities to direct and control an organization with regard to risk. [Source: ISO Guide 73:2009]

**Secondary Stakeholder**

Individuals or organizations that may be affected by events that occur to Assets outside of their control. For example, consumers are Secondary Stakeholders in a scenario where their personal private information may be inappropriately disclosed or stolen.

**Threat**

Anything that is capable of acting in a manner resulting in harm to an Asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.

**Threat Agent**

Any agent (e.g., object, substance, human) that is capable of acting against an Asset in a manner that can result in harm.

**Threat Capability (TCap)**

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.

**Threat Community**

A subset of the overall Threat Agent population that shares key characteristics.

**Threat Event**

Occurs when a Threat Agent acts against an Asset.

**Threat Event Frequency (TEF)**

The probable frequency, within a given timeframe, that a Threat Agent will act against an Asset.

**Vulnerability (Vuln)**

The probability that a Threat Event will become a Loss Event; probability that Threat Capability is greater than Resistance Strength. (Synonym: Susceptibility)

## Index

5x5 risk matrix .....	2	Primary Loss .....	9, 18
access.....	9, 18	Primary Stakeholder.....	3
Asset .....	3	Probability of Action.....	4
business case .....	26	qualitative analysis .....	2
Contact Frequency.....	4	qualitative scale .....	9
examples.....	26	Resistance Strength .....	4, 6
identity theft .....	9	Risk .....	13
LEF.....	2, 4, 8, 14, 26, 28	Secondary Loss .....	8, 10
Loss Event .....	3	SLEF .....	8, 10, 17, 37
Loss Magnitude ....	2, 8, 17, 22, 26, 39	SLM .....	8, 10, 17, 37
Loss Scenario .....	2, 4	TEF .....	4, 15, 28, 34
misuse.....	9, 18	Threat Capability.....	4, 6
Open FAIR Body of Knowledge .....	1	Threat Community .....	3
Open FAIR Risk Analysis Tool .	1, 14	Threat Event.....	3
O-RA Standard.....	1	threat vector.....	3
O-RT Standard .....	1	value proposition.....	11
PII.....	10	Vulnerability .....	6, 30, 35
PLM.....	8, 17, 18, 32		