

*The Open Group Standard*

**Risk Taxonomy (O-RT), Version 3.0.1**



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

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

It is fair use of this specification for implementors to use the names, labels, etc. contained within the specification. The intent of publication of the specification is to encourage implementations of the specification.

This specification has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed.

Any use of this publication for commercial purposes is subject to the terms of the Annual Commercial License relating to it. For further information, see [www.opengroup.org/legal/licensing](http://www.opengroup.org/legal/licensing).

The Open Group Standard

**Risk Taxonomy (O-RT), Version 3.0.1**

ISBN: 1-947754-66-9

Document Number: C20B

Published by The Open Group, November 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	Conformance.....	2
1.4	Normative References.....	2
1.5	Terminology .....	3
1.6	Future Directions .....	3
2	Definitions.....	4
2.1	Action .....	4
2.2	Asset .....	4
2.3	Contact Event.....	4
2.4	Contact Frequency (CF).....	4
2.5	Control .....	4
2.6	FAIR .....	4
2.7	Loss Event .....	5
2.8	Loss Event Frequency (LEF).....	5
2.9	Loss Flow.....	5
2.10	Loss Magnitude (LM).....	5
2.11	Loss Scenario.....	5
2.12	Primary Stakeholder .....	5
2.13	Probability of Action (PoA).....	5
2.14	Resistance Strength (RS) .....	5
2.15	Risk .....	5
2.16	Risk Analysis .....	6
2.17	Risk Assessment .....	6
2.18	Risk Factors .....	6
2.19	Risk Management .....	6
2.20	Secondary Stakeholder .....	6
2.21	Threat.....	6
2.22	Threat Agent .....	6
2.23	Threat Capability (TCap).....	6
2.24	Threat Community.....	6
2.25	Threat Event.....	7
2.26	Threat Event Frequency (TEF) .....	7
2.27	Vulnerability (Vuln) .....	7
3	Risk Management Model.....	8
3.1	Why is a Tightly-Defined Taxonomy Critical? .....	8
4	Technical Requirements.....	10
4.1	Risk Taxonomy Overview .....	10
4.2	Risk.....	11
4.3	Loss Event Frequency (LEF).....	12

4.3.1	Threat Event Frequency (TEF).....	12
4.3.2	Vulnerability (Vuln) .....	14
4.3.3	Summary: Loss Event Frequency.....	16
4.4	Loss Magnitude (LM).....	17
4.4.1	Forms of Loss.....	18
4.4.2	Loss Flow .....	19
4.4.3	Loss Factors.....	21
4.4.4	Summary: Loss Magnitude .....	26
A	Risk Taxonomy in the Context of Risk Analysis.....	28
A.1	Complexity of the Model.....	28
A.2	Availability of Data .....	29
A.3	Iterative Risk Analyses .....	29
A.4	Perspective .....	29
B	Practical Use of the Open FAIR Method .....	30
B.1	The Risk Language Gap .....	30
B.2	Key Risk Concepts.....	30
B.3	Using the Open FAIR Model with Other Risk Assessment Frameworks .....	31

# 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 Standard for Risk Taxonomy (O-RT), Version 3.0.1. It has been developed and approved by The Open Group.

This document provides a standard definition and taxonomy for information security risk, as well as information regarding how to use the taxonomy. It is a companion document to the Risk Analysis (O-RA) Standard, Version 2.0.1.

The intended audience for this document includes anyone who needs to understand and/or analyze a risk condition. This includes, but is not limited to:

- Information security and risk management professionals
- Auditors and regulators
- Technology professionals

- Management

Note that this document is not limited to application in the information security space. It can, in fact, be applied to any risk scenario. This agnostic characteristic enables the O-RT Standard, and the companion O-RA Standard, to be used as a foundation for normalizing the results of risk analyses across varied risk domains.

This document is one of several publications from The Open Group dealing with risk management. Other publications include:

- **Risk Analysis (O-RA) Standard, Version 2.0.1**  
The Open Group Standard (C20A, November 2021)

This document provides a set of standards for various aspects of information security risk analysis. It was first published in October 2013, and has been revised as a result of feedback from practitioners using the standard and continued development of the Open FAIR™ taxonomy.

- **Requirements for Risk Assessment Methodologies**  
The Open Group Guide (G081, January 2009)

This document identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements. In this way, it explains what features to look for when evaluating the capabilities of any given methodology, and the value those features represent.

- **Open FAIR™ – ISO/IEC 27005 Cookbook**  
The Open Group Guide (C103, November 2010)

This document describes in detail how to apply the Open FAIR methodology to ISO/IEC 27002:2005. The Cookbook part of this document enables risk technology practitioners to follow by example how to apply FAIR to other frameworks of their choice.

- **The Open FAIR™ – NIST Cybersecurity Framework Cookbook**  
The Open Group Guide (G167, October 2016)

This document describes in detail how to apply the Open FAIR factor analysis for information risk methodology to the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework).

- **The Open FAIR™ Risk Analysis Process Guide**  
The Open Group Guide (G180, January 2018)

This document 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.

- **How to Put Open FAIR™ Risk Analysis Into Action: A Cost-Benefit Analysis of Connecting Home Dialysis Machines Online to Hospitals in Norway**  
The Open Group White Paper (W176, May 2017)

This document offers an Open FAIR analysis of security and privacy risks and compares those risks to the likely benefits of connecting home dialysis machines online to hospitals.

- **The Open FAIR™ Risk Analysis Tool Beta**  
(I181, January 2018)

This analysis tool can be used to perform a quantitative Open FAIR risk analysis as defined in the O-RA and O-RT Standards. It is provided in the form of a Microsoft® Excel® spreadsheet.

- **The Open FAIR™ Tool with SIPmath™ Distributions: Guide to the Theory of Operation**  
The Open Group Guide (G181, January 2018)

This document defines the algorithms that can be used to produce an acceptable implementation of the O-RA Standard.

### **Differences from Version 2.0 of the Standard**

This document includes changes to the O-RT Standard that have evolved since the original document was published. These changes came about as a result of feedback from practitioners using the standard:

- “Accomplish Assigned Mission” as a possible action taken by a Threat Agent was removed – it could apply to any of the other actions and be a component of any of them, but it is not its own action
- The external loss factor “Detection” was changed to “External Party Detection” and the organizational loss factor “Due Diligence” was changed to “Reasonable Care”
- The quantitative example that utilized a qualitative scale has been removed
- Open FAIR terms and definitions were clarified

## 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 and Excel are registered trademarks of Microsoft Corporation in the United States and/or other countries.

SIPmath is a trademark of ProbabilityManagement.org.

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

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

- Chris Carlson, C T Carlson LLC
- Jack Freund, Cyber Assessments, Inc.
- Mike Jerbic, Trusted Systems Consulting Group
- Eva Kuiper, The Open Group Invited Expert
- John Linford, Security Forum & OTTF Forum Director, The Open Group
- David Musselwhite, RiskLens
- Tyanna Smith, Trusted Systems Consulting Group

The Open Group gratefully acknowledges the contribution of members of The Open Group Security Forum, and the following people in the development of earlier versions of this document:

- Alex Hutton
- Jack Jones

## Referenced Documents

The following documents are referenced in this standard.

(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, November 2009; refer to <https://www.iso.org/standard/44651.html>
- ISO 31000:2018, Risk Management – Guidelines, February 2018; refer to <https://www.iso.org/standard/65694.html>
- Risk Analysis (O-RA) Standard, Version 2.0.1, The Open Group Standard (C20A), November 2021, published by The Open Group; refer to: [www.opengroup.org/library/c20a](http://www.opengroup.org/library/c20a)

# 1 Introduction

---

## 1.1 Objective

The objective of the Risk Taxonomy (O-RT) Standard is to provide a single logical and rational taxonomical framework for anyone who needs to understand and/or analyze information security risk.

This document can and should be used to:

- Educate information security, risk, and audit professionals
- Establish a common language for the information security and risk management profession
- Introduce rigor and consistency into analysis, which sets the stage for more effective risk modeling
- Explain the basis for risk analysis conclusions
- Strengthen existing risk assessment and analysis methods
- Create new risk assessment and analysis methods
- Evaluate the efficacy of risk assessment and analysis methods
- Establish metric standards and data sources

## 1.2 Overview

This document provides a taxonomy describing the factors that drive risk – their definitions and relationships. Each factor that drives risk is identified and defined. Furthermore, the relationships between factors are described so that mathematical functions can be defined and used to perform quantitative calculations.

This document is limited to describing the factors that drive risk and their relationships to one another. Measurement scales and specific assessment methodologies are not included because there are a variety of possible approaches to those aspects of risk analysis, with some approaches being better suited than others to specific risk problems and analysis objectives.

This document does not address how to assess or analyze risk.<sup>1</sup> This document also does not cover those elements of risk management that pertain to strategic and tactical risk decisions and execution.

---

<sup>1</sup> Refer to the separate standard for performing risk analysis: the Risk Analysis (O-RA) Standard; see [Referenced Documents](#).

This document should be used as a foundational reference of the problem space the profession is tasked with helping to manage; i.e., risk. Based on this foundation, methods for analyzing, calculating, communicating about, and managing risk can be developed.

Risk analysts can choose to make their measurements and/or estimates at any level of abstraction within the taxonomy. For example, rather than measure Contact Frequency, the analyst could move up a layer of abstraction and instead measure Threat Event Frequency. This choice may be driven by the nature or volume of data that is available, or the time available to perform the analysis (i.e., analyses at deeper layers of abstraction take longer).

Although the terms “risk” and “risk management” mean different things to different people, this document is intended to be applied toward the problem of managing the frequency and magnitude of loss that arises from a threat (whether human, animal, or natural event). In other words, managing “how often bad things happen, and how bad they are when they occur”.

In the overall context of risk management, it is important to appreciate that the business objective in performing risk assessments is to identify and estimate levels of exposure to the likelihood of loss, so that business managers can make informed business decisions on how to manage those risks of loss – either by accepting each risk, or by mitigating it – through investing in appropriate internal protective measures judged sufficient to lower the potential loss to an acceptable level, or by investing in external indemnity. Critical to enabling good business decision-making therefore is to use risk assessment methods which give objective, meaningful, consistent results.

Fundamental to risk assessments is a sound approach:

You can't effectively and consistently manage what you can't measure,  
and you can't measure what you haven't defined.

The problem here is that a variety of definitions exist, but the risk management community has not yet adopted a consistent definition for even the most fundamental terms in its vocabulary; e.g., threat, vulnerability, even risk itself. Without a sound common understanding of what risk is, what the factors are that drive risk, and a standard use of the terms used to describe it, risk analysts cannot be effective in delivering meaningful, comparable risk assessment results. This document provides the necessary foundation vocabulary, based on a fundamental analysis of what risk is, and then shows how to apply it to produce the objective, meaningful, and consistent results that business managers need.

## **1.3 Conformance**

Refer to The Open Group website for conformance requirements for this document.

## **1.4 Normative References**

The following standards contain provisions which, through references in this standard, constitute provisions of the Risk Taxonomy (O-RT) Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards.

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

## 1.5 Terminology

For the purposes of this document, the following terminology definitions apply:

Can	Describes a possible feature or behavior available to the user or application.
May	Describes a feature or behavior that is optional. To avoid ambiguity, the opposite of “may” is expressed as “need not”, instead of “may not”.
Shall	Describes a feature or behavior that is a requirement. To avoid ambiguity, do not use “must” as an alternative to “shall”.
Shall not	Describes a feature or behavior that is an absolute prohibition.
Should	Describes a feature or behavior that is recommended but not required.
Will	Same meaning as “shall”; “shall” is the preferred term.

## 1.6 Future Directions

None.

## 2 Definitions

---

For the purposes of this standard, the following terms and definitions apply. Merriam-Webster's Collegiate Dictionary<sup>2</sup> should be referenced for terms not defined in this section.

### 2.1 Action

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

### 2.2 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.

### 2.3 Contact Event

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

### 2.4 Contact Frequency (CF)

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

### 2.5 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.

### 2.6 FAIR

Factor Analysis of Information Risk.

---

<sup>2</sup> Merriam Webster: <https://www.merriam-webster.com/>.

## **2.7 Loss Event**

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

## **2.8 Loss Event Frequency (LEF)**

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

## **2.9 Loss Flow**

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

## **2.10 Loss Magnitude (LM)**

The probable magnitude of loss resulting from a Loss Event.

## **2.11 Loss Scenario**

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

## **2.12 Primary Stakeholder**

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

## **2.13 Probability of Action (PoA)**

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

## **2.14 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.

## **2.15 Risk**

The probable frequency and probable magnitude of future loss.

## **2.16 Risk Analysis**

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

## **2.17 Risk Assessment**

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

## **2.18 Risk Factors**

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

## **2.19 Risk Management**

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

## **2.20 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.

## **2.21 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.

## **2.22 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.

## **2.23 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.

## **2.24 Threat Community**

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



## **2.25 Threat Event**

Occurs when a Threat Agent acts against an Asset.

## **2.26 Threat Event Frequency (TEF)**

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

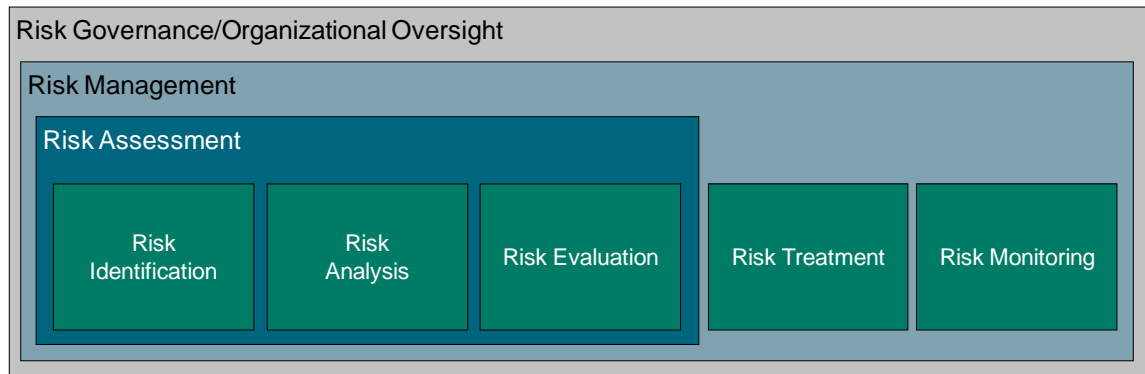
## **2.27 Vulnerability (Vuln)**

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

### 3 Risk Management Model

---

Per ISO Guide 73:2009 (see [Referenced Documents](#)), risk management refers to the “coordinated activities to direct and control an organization with regard to risk”. A risk assessment is the “overall process of risk identification, risk analysis, and risk evaluation”, and risk analysis refers to the “process to comprehend the nature of risk and determine the level of risk”.



**Figure 1: Risk Analysis in Context**

This document expands on this to add that all risk assessment approaches should include:

- An effort to clearly identify and characterize the assets, threats, controls, and impact/loss elements at play within the risk scenario being assessed
- An understanding of the organizational context for the analysis; i.e., what is at stake from an organizational perspective, particularly with regard to the organization’s leadership perspective
- Measurement and/or estimation of the various risk factors
- Calculation of risk
- Communication of the risk results to decision-makers in a form that is meaningful and useful

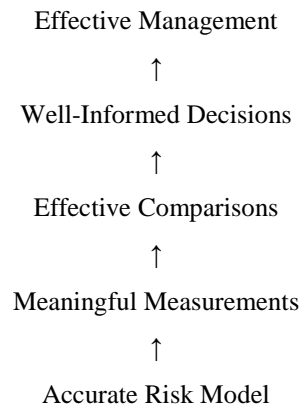
An Open FAIR risk analysis fits the Risk Analysis component described by ISO Guide 73:2009 and allows decision-makers to prioritize their consistently defined and identified risks but crucially adds the communication component, which distinguishes the risk assessment approach defined above and the risk analysis approach defined in the O-RA Standard (see [Referenced Documents](#)).

#### 3.1 Why is a Tightly-Defined Taxonomy Critical?

Without a logical, tightly defined taxonomy, risk assessment approaches will be significantly impaired by an inability to measure and/or estimate risk factor. 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.

This concept can be illustrated in what is referred to as a “risk management stack”, showing the relationship between these elements; see Figure 2.



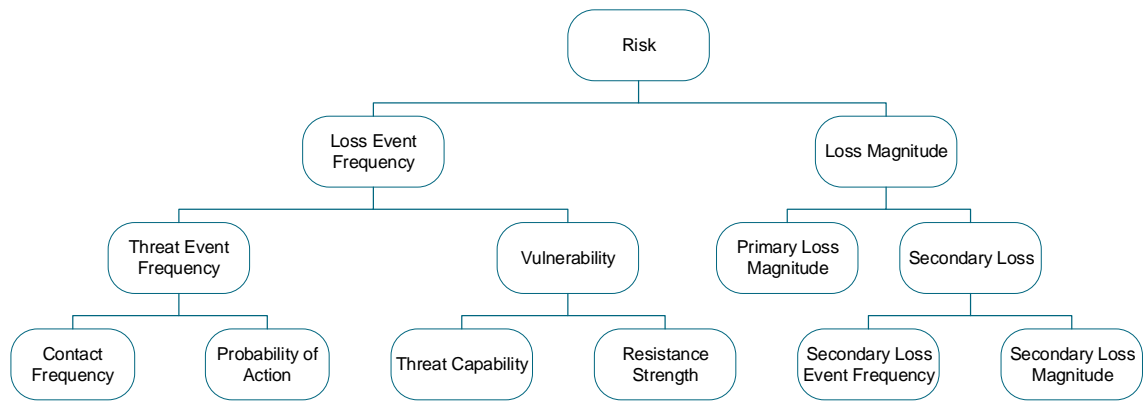
**Figure 2: Risk Management Stack**

As with similar relational constructs, it becomes immediately apparent that failures at lower levels of the stack cripple the ability to achieve effectiveness at higher levels.

## 4 Technical Requirements

### 4.1 Risk Taxonomy Overview

In this document, “risk” is defined as the probable frequency and probable magnitude of future loss; this is also known as the “loss exposure” that a Primary Stakeholder will bear within some defined time period. Risk is measured by making forward-looking estimates of the probable frequency and the probable magnitude of a loss should it occur, and it is measured and managed from the perspective of the Primary Stakeholder, the party who bears the economic loss of the adverse events. To further refine risk and its components, the complete risk taxonomy develops the two sub-factors of risk: Loss Event Frequency and Loss Magnitude, as shown in Figure 3.



**Figure 3: High-Level Risk Taxonomy Abstractions**

Figure 3 is not comprehensive, as deeper layers of abstraction exist that are not shown. Some of these deeper layers are discussed further on in this document, and theoretically, the layers of abstraction may continue indefinitely, much like the layers of abstraction that exist in the understanding of physical matter (e.g., molecules, atoms, particles). The deeper layers of abstraction can be useful for understanding but are not always necessary to perform effective analyses.

Moreover, the factors within the Loss Event Frequency side of the taxonomy have relatively clean and clear cause-and-effect relationships with one another, which simplifies calculation. Factors within the Loss Magnitude side of the taxonomy, however, have much more complicated relationships that defy simple calculation. As a result, Loss Magnitude measurements and estimates generally are aggregated by loss type (e.g., \$xxx of productivity loss, plus \$yyy of legal fines and judgments).

The Open FAIR risk factors are assumed to be independently identically distributed.

## 4.2 Risk

In this document, “risk” is defined as the probable frequency and probable magnitude of future loss (also known as “loss exposure”).

Note: This document defines risk as resulting in a loss; it does not consider speculative risk that may generate either a loss or a gain (e.g., as presented in ISO 31000, see [Referenced Documents](#)).

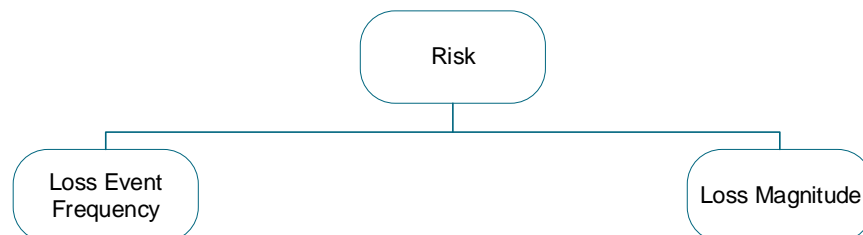
A risk measurement is an estimate of the likelihood and impact of adverse events (losses). Measuring risk is never a prediction of whether some adverse event will occur – such as an earthquake will destroy a data center causing a loss of \$1M within the next year – but instead is an estimate of the likelihood or probability of that adverse event happening within the year and the range of economic damage from that event.

Risk measurements are accurate if the actual result (how much earthquake damage occurred within a year) measured at the end of the year lies within the range of the estimate. A risk measurement of earthquake risk would be a reasoned, defensible analysis whose results are something like, “There is between a 10% to 20% probability of an earthquake damaging the data center with damage of between \$1,000 and \$5,000,000”. That estimate will either be found accurate or inaccurate after the next year, five years, ten years, or twenty years when losses from the earthquake are observed.

Analyzing risk requires differentiating between possibility and probability. Possibility can be thought of as binary: something is possible, or it is not. Probability, however, is a continuum that addresses the area between certainty and impossibility. Because risk is invariably a matter of future events, there is always some amount of uncertainty, which means executives cannot choose or prioritize effectively based upon statements of possibility. Effective risk decision-making can only occur when information about probabilities is provided.

Moreover, risk analyses should not be considered predictions of the future. The word “prediction” implies a level of certainty that rarely exists in the real world, and does not help people understand the probabilistic nature of analysis. For decision-makers, even though it is impossible to know which roll of the dice will come up, knowing that the probability is 1-in-36 is valuable information.

With this as a starting point, the first two risk factors are loss frequency and magnitude of loss. In this document, these are referred to as Loss Event Frequency and Loss Magnitude, respectively.

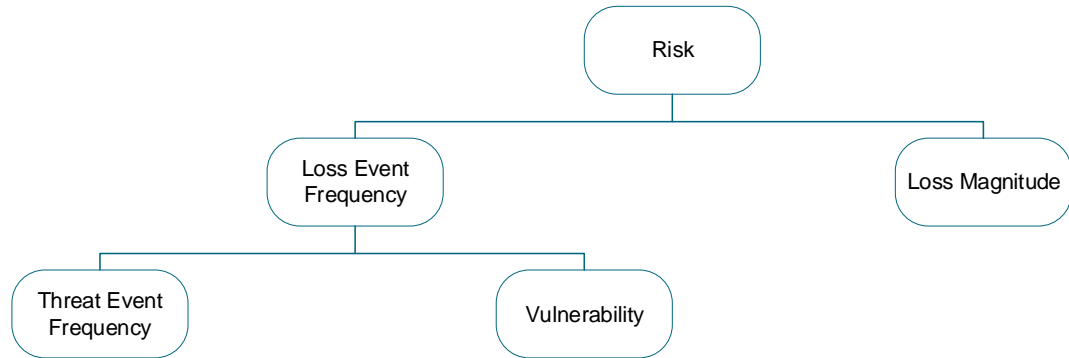


**Figure 4: Risk**

### 4.3 Loss Event Frequency (LEF)

Loss Event Frequency is the probable frequency, within a given timeframe, that a Threat Agent will inflict harm upon an Asset.

For a Loss Event to occur, a Threat Agent has to act upon an Asset, such that loss results, which leads to the next two factors: Threat Event Frequency and Vulnerability.



**Figure 5: Loss Event Frequency**

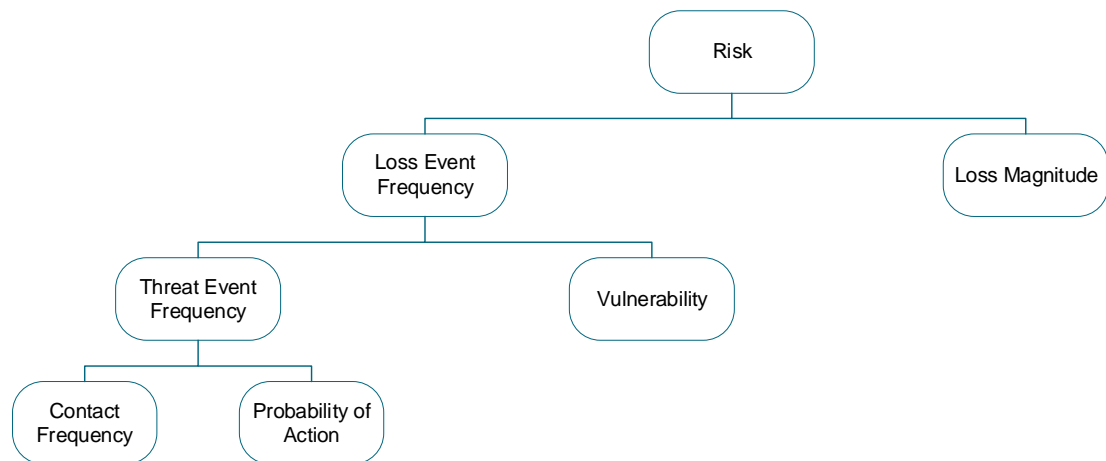
Note: The Loss Event Frequency of an event that can only occur once is specified as a probability within a specific timeframe (event X is 10% likely to occur over the next Y months) because almost any event is possible, and if it is possible, given enough time, the event will occur.

#### 4.3.1 Threat Event Frequency (TEF)

Threat Event Frequency is the probable frequency, within a given timeframe, that a Threat Agent will act against an Asset.

The only difference between this definition and the definition for Loss Event Frequency above is that the definition for Threat Event Frequency does not include whether Threat Agent actions are successful. In other words, Threat Agents may act against Assets but be unsuccessful in breaching or otherwise impairing the Asset. A common example of a malicious Threat Event (where harm or abuse is intended) would be the hacker who unsuccessfully attacks a web server. Such an attack would be considered a Threat Event, but not a Loss Event. An example of a non-malicious Threat Event would be a data center technician tripping over a system's power cord. The act of tripping would be the Threat Event, but a Loss Event would only occur if the technician unplugged the cord (or, depending on the scenario under analysis, if the technician were injured).

This definition also provides the two factors that drive Threat Event Frequency: Contact Frequency and Probability of Action.



**Figure 6: Threat Event Frequency**

#### 4.3.1.1 *Contact Frequency (CF)*

Contact Frequency is the probable frequency, within a given timeframe, that a Threat Agent will come into contact with an Asset. A Threat Agent coming into contact with the Asset is referred to as a Contact Event.

Contact can be physical or “logical” (e.g., over the network). Regardless of contact mode, three types of contact can occur:

- **Random** – the Threat Agent “stumbles upon” the Asset during the course of unfocused or undirected activity
- **Regular** – contact occurs because of the regular actions of the Threat Agent; for example, if a cleaning crew regularly comes by at 5:15pm, leaving cash on top of the desk during that timeframe sets the stage for contact
- **Intentional** – the Threat Agent seeks out specific targets

Each of these types of contact is driven by various factors. A useful analogy is to consider a container of fluid containing two types of suspended particles – threat particles and asset particles. The probability of contact between members of these two sets of particles is driven by various factors, including:

- Size (surface area) of the particles
- The number of particles
- Volume of the container
- How active the particles are
- Viscosity of the fluid
- Whether particles are attracted to one another in some fashion, etc.

#### 4.3.1.2 *Probability of Action (PoA)*

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, action always takes place. For example, if a tornado comes into contact with a house, action is a foregone conclusion. Action is only in question when considering “thinking” Threat Agents, such as humans and other animals, and artificially intelligent Threat Agents, such as malicious programs (which are extensions of their human creators).

The probability that an intentional act will take place – in other words, whether a Threat Agent will deliberately contact an Asset – is driven by three primary factors:

- **Value** – the Threat Agent’s perceived value proposition from performing the act
- **Level of effort** – the Threat Agent’s expectation of how much effort it will take to accomplish the act
- **Risk of detection/capture** – the probability of negative consequences *to the Threat Agent*; for example, the probability of getting caught and suffering unacceptable consequences for acting maliciously

#### 4.3.2 Vulnerability (Vuln)

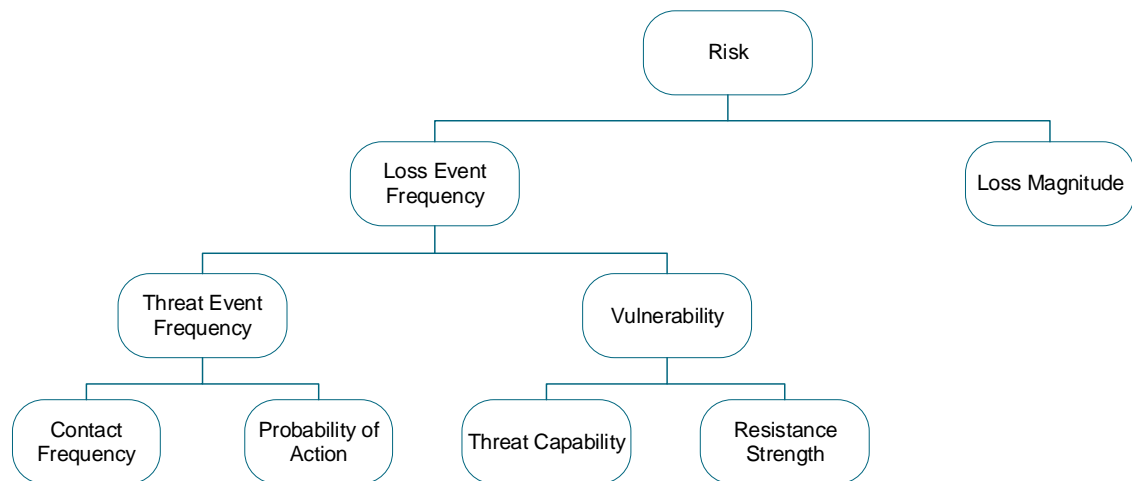
Vulnerability, or its synonym susceptibility, is the probability that a Threat Event becomes a Loss Event.

In stricter terms, Vulnerability is the conditional probability of a Loss Event given a Threat Event. This definition of Vulnerability is identical to saying that the probability that the Threat Agent’s force applied (the Threat Capability) against the Asset in a specific Loss Scenario exceeds the Resistance Strength of the Controls protecting that Asset.

This means that there are two ways to estimate Vulnerability, and each way arrives at the same result:

- If Threat Event Frequency and Loss Event Frequency data is available or estimated directly, Vulnerability can be observed (or estimated) as the fraction of Threat Events that become Loss Events
- Vulnerability can also be derived from knowing or estimating the Threat Capability and the Asset’s Resistance Strength to that Threat Capability and then estimating or simulating the probability that the Threat Capability exceeds Resistance Strength





**Figure 7: Vulnerability**

Vulnerability is always relative to the type of force and vector involved: the Vulnerability of an information Asset depends upon the Loss Scenario being analyzed. As an analogy to an information Asset's Vulnerability to some specific Loss Scenario, the tensile strength of a rope is pertinent only if the Threat Agent's force is a weight applied along the length of the rope. Tensile strength does not generally apply to a scenario where the Threat Agent is fire, chemical erosion, etc. Likewise, a computer anti-virus product does not reduce the Vulnerability of a payment system from an internal employee seeking to perpetrate fraud. Open FAIR risk analysts, therefore, evaluate Vulnerability in the context of specific threat types facing the information Asset and Control types protecting the Asset.

Because Vulnerability is a probability, an Asset cannot be more than 100% vulnerable to damage by any specific Threat Agent/threat vector combination. Vulnerability can exist such that harm can occur from more than one Threat Agent through more than one threat vector, but each of those represents a different potential Threat Event. For example, if a person is walking down the street at night in a particularly dangerous part of town, they are vulnerable to multiple potential Threat Events; for example, being run over by a car, being mugged, or being the victim of a drive-by shooting. The probability of occurrence for any one of these Threat Events cannot exceed 100% (certainty), but the aggregate risk of loss is certainly greater due to the multiple Loss Scenarios that could occur.

#### 4.3.2.1 *Threat Capability (TCap)*

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.

Attackers exist on a continuum of skills and resources, including at one end of the continuum attackers with little skill, little experience, and a low level of determination, to the other end with highly skilled, experienced, and determined attackers. The Threat Capability continuum describes attackers as existing at various percentiles, where the 25<sup>th</sup> percentile of Threat Agents are less skilled and able than the 50<sup>th</sup> percentile of Threat Agents who are less skilled and able than the 99<sup>th</sup> percentile of Threat Agents.

Threat Agents within a single Threat Community will not have the same capabilities. Therefore, the probability of the most capable Threat Agent acting against an Asset is something less than

100%. Depending upon the Threat Community under analysis, and other conditions within the scenario, the probability of encountering a highly capable Threat Agent may be remote.

Information security professionals and risk analysts often struggle with the notion of considering Threat Agent capability as a percentile of a Threat Community, resulting in a probability, perhaps only a remote one, that only the most capable threat is attacking that Asset. Many analysts and decision-makers, instead, tend to gravitate toward focusing on the worst case, but focusing solely on the worst case is to think in terms of possibility rather than probability.

Some Threat Agents may be proficient in applying one type of force but incompetent at others. For example, a network engineer may be proficient at applying technological forms of attack but relatively incapable of executing complex accounting fraud.

#### 4.3.2.2 *Resistance Strength (RS)*

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.

Attackers exist on a continuum of skills and resources, and Resistance Strength measures the strength of a Control as compared to that percentile of attackers, specifically measuring the percentile of attackers that the Asset's Control(s) can be expected to resist.

As an analogy to the strength of an information security control, a rope's tensile strength rating provides an indication of how much force it is capable of resisting. The baseline measure (Resistance Strength) for this rating is Pounds per Square Inch (PSI), which is determined by the rope's design and construction. This Resistance Strength rating does not change when the rope is put to use. Regardless of whether there is a 10-pound weight on the end of the 500-PSI rope or a 2,000-pound weight, the Resistance Strength does not change.

Information security controls, however, do not have a baseline scale for force that is as well-defined as PSI. Password strength is a simple example of how to approach this. It is possible to estimate that a password eight characters long, comprised of a mixture of upper and lowercase letters, numbers, and special characters, will resist the cracking attempts of some percentage of the general Threat Agent population. Therefore, password Resistance Strength can be represented as this percentile. (Recall that Resistance Strength is relative to a particular type of force – in this case, cracking.)

Vulnerability is determined by comparing the Resistance Strength against the capability of the specific Threat Community under analysis and assessing the probability that the Threat Capability will exceed the Resistance Strength. For example, password Resistance Strength may be estimated at the 80<sup>th</sup> percentile, yet the Threat Community within a scenario might be estimated to have better than average capabilities, such as in the 90<sup>th</sup> percentile range.

### 4.3.3 **Summary: Loss Event Frequency**

Loss Event Frequency is the probable number of Loss Events within a given time period, expressed as a distribution. Loss Event Frequency is composed of several sub-factors, as shown in Table 1.

**Table 1: Loss Event Frequency Factors**

<b>Loss Event Frequency Factor</b>	<b>Description</b>	<b>Unit of Measure</b>
Loss Event Frequency	Probable number of economic losses within a given time period	Events per unit time (e.g., events per year); or the probability of a single Loss Event in a given timeframe (e.g., 20% chance within the next year)
Threat Event Frequency	Probable number of Threat Agent attempts at creating a loss within a given time period	Events per unit time (e.g., events per year); or the probability of a single Threat Event in a given timeframe (e.g., 20% chance within the next year)
Vulnerability	Probability that a Threat Event becomes a Loss Event; probability that Threat Capability is greater than Resistance Strength (Synonym: Susceptibility)	Probability (between 0-1 or measured as a percentage, between 0 and 100%)
Contact Frequency	Probable number of times a Threat Agent contacts the stakeholder's Asset within a given time period	Events per unit time (e.g., events per year); or the probability of a single Contact Event in a given timeframe (e.g., 20% chance within the next year)
Probability of Action	Probability that a Contact Event becomes a Threat Event	Probability (between 0-1 or measured as a percentage, between 0 and 100%)
Threat Capability	The relative ranking of a Threat Agent's skill, resources, and time within a Threat Community	Percentile (0-100)
Resistance Strength	The ability to resist a Threat Community's range of skills, resources, and time	Percentile (0-100)

## 4.4 Loss Magnitude (LM)

The Open FAIR method defines risk as the probable frequency and probable magnitude of future loss. The previous section introduced the factors that drive the probability of Loss Events occurring. This section describes the other half of the risk equation – the factors that drive Loss Magnitude when events occur.

Loss Magnitude is the probable magnitude of economic loss resulting from a Loss Event (measured in units of currency). Loss Magnitude is expressed as a distribution of losses, not a single value for loss, and is always evaluated from the perspective of the Primary Stakeholder, the party that bears the economic loss from the Loss Event.

Historically, data regarding Loss Magnitude have been scarce. Many organizations still do not measure losses when events occur, and those that do often limit their analyses to the “easy stuff”

(e.g., person-hours, equipment replacement). Furthermore, the lack of a standard taxonomy has made it difficult to normalize data across organizations.

Because Loss Magnitude can be difficult to estimate, analysts frequently exclude analyzing it, assess only possible, speculative worst-case outcomes, or model losses with tools that are deceptively precise. Excluding Loss Magnitude from an analysis means the analyst is not analyzing risk: risk *always* has a loss component. Citing worst-case possibilities alone removes the probability element from the analysis – by definition, risk is a combination of the probability of a loss along with its magnitude. Computational modeling tools that present risk results with a precision that cannot be supported by the precision of the modeled risk factors give decision-makers an inaccurately high understanding of the certainty inherent in the analysis.

In general, the majority of losses associated with information systems are small, but there is still the remote chance of a large loss, usually described by a Loss Magnitude distribution having a “fat tail”, as shown in Figure 8.

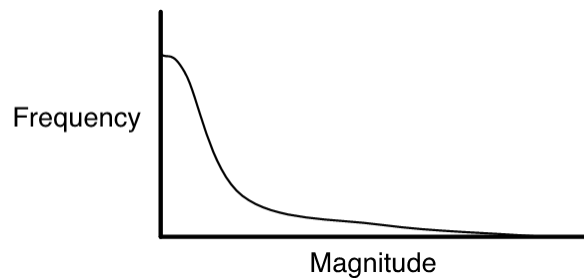


Figure 8: A Typical Loss Magnitude Distribution

#### 4.4.1 Forms of Loss

The potential for loss stems from the value of the affected Asset(s) and/or the liability it introduces to an organization. For example, customer information provides value through its role in generating revenue for a commercial organization or services for a public organization, and that same information could introduce liability to the organization if a legal duty exists to protect it or if customers have an expectation that the information about them will be appropriately protected.

Six forms of loss are defined within this document:

- **Productivity** – direct losses associated with the reduction in an organization’s ability to generate its primary value proposition (e.g., income, goods, services); it may also include costs associated with personnel who are unable to perform their duties but who continue to collect their paycheck (e.g., a call center’s phone lines are down, but personnel continue to be paid); it accounts for the loss of revenue due to operational outages and discontinuation (e.g., revenue lost when a retail website is unavailable due to a system outage); and it includes costs associated with the impaired productivity of personnel (e.g., increased costs from switching from automated to manual methods)
  - Lost revenue is not delayed revenue; for example, when a retail website goes down some proportion of its customers may wait to perform their transactions rather than use a different retailer – the sales and marketing departments in most organizations will have reliable data to inform these estimates

- **Response** – direct expenditures associated with managing a Loss Event (e.g., internal or external person-hours, logistical expenses, legal defense, public relations expenses)
- **Replacement** – direct expenditures associated with replacing an Asset; typically represented as the expense associated with replacing lost or damaged Assets (e.g., rebuilding a facility, purchasing a replacement laptop, replacing a terminated employee, covering the losses experienced by fraud)
- **Fines and Judgments** – direct expenditures associated with legal or regulatory actions levied against an organization, including settlements and bail for any organization members who are arrested
- **Competitive Advantage** – future estimated business losses associated with a diminished competitive position, specifically associated with Assets that provide competitive differentiation (e.g., lower production cost, higher quality, advanced capabilities) between the organization and its competition
  - Within the commercial world, examples would include operational efficiencies, trade secrets, merger and acquisition plans, etc.
  - Outside the commercial world, examples would include military secrets, secret alliances, etc.
- **Reputation** – future estimated business losses associated with an external stakeholder's perception that an organization's value proposition is diminished and/or that the organization represents liability to the stakeholder; this accounts for any reduction in revenue due to lost market share and typically materializes as reduced market share (for commercial organizations), reduced stock price (for publicly traded companies), reduced willingness to cooperate in joint ventures, or an increased cost of capital

#### 4.4.2 Loss Flow

Once a Loss Event begins, there are two stages to the loss from the perspective of Loss Magnitude: the Primary Loss and the Secondary Loss. Loss Flow is the structured decomposition of how losses materialize when a Loss Event occurs. Loss Flow incorporates the following:

- A Threat Agent acts against an Asset (the Threat Event)
- This Threat Event directly affects the Primary Stakeholder in terms of productivity loss, response costs, etc. – this is the Primary Loss Event
- Sometimes this Primary Loss Event also has an effect on Secondary Stakeholders, such as customers, regulators, media, etc., who may react against the Primary Stakeholder
- When Secondary Stakeholders react against a Primary Stakeholder, they act as new Threat Agents against the organization's Assets (such as reputation, legal fees, etc.), which again affects the Primary Stakeholder – this is referred to as the Secondary Loss Event.

A couple of things to recognize:

- Secondary Losses are always predicated upon a Primary Loss

- Although called “Secondary Stakeholders”, they are most accurately viewed as “Secondary Threat Agents” when they begin acting against the Primary Stakeholder’s Assets

For example, if a Payment Processor (Primary Stakeholder) suffers a breach, it must respond and recover from that breach. Costs incurred while recovering from the breach are Primary Losses. However, consumers who have credit fraud committed against them due to the breach also suffer indirect consequential harm. When those consumers (Secondary Stakeholders) demand relief from the Payment Processor, those consumers become new Threat Agents trying to cause harm against the Payment Processor, usually by “attacking” its financial Assets through a lawsuit. In this case, the Payment Processor may expend resources to provide credit monitoring to those affected consumers to mitigate additional Secondary Losses. This is an example of a Primary Loss (response and recovery from the initial breach) followed in time by a Secondary Loss (credit monitoring and exposure to a lawsuit’s fine).

#### 4.4.2.1 *Primary Loss*

The first phase of the Loss Event, referred to as Primary Loss, occurs directly as a result of the Threat Agent’s action upon the Asset. The owner of the affected Assets would be considered the Primary Stakeholder in an analysis (e.g., The Open Group is the Primary Stakeholder in a scenario where its website goes offline as a result of an infrastructure failure). Of the six forms of loss described in the previous section, productivity, response, and replacement are generally the forms of loss experienced as Primary Loss. The other three forms of loss only occur as Primary Loss when the Threat Agent is directly responsible for those losses (e.g., fines and judgments loss when the Threat Agent is filing charges/claims).

#### 4.4.2.2 *Secondary Loss*

The second phase of the Loss Event, referred to as Secondary Loss, occurs as a result of Secondary Stakeholders (e.g., customers, stockholders, regulators) reacting negatively to the Primary Loss. This can be thought of as “fallout” from the Primary Loss. An example would be customers taking their business elsewhere after their personal information had been compromised or due to frustration experienced as a result of frequent service outages.

Secondary Loss has two primary components: Secondary Loss Event Frequency (SLEF) and Secondary Loss Magnitude (SLM).

Secondary Loss Event Frequency allows the analyst to estimate the chance (percentage of time) a scenario is expected to have secondary effects. Even though this variable is called a “frequency”, it is estimated as a percentage because it represents the conditional probability that a Primary Loss results in a Secondary Loss.

Secondary Loss Magnitude represents the losses that are expected to materialize from dealing with Secondary Stakeholder reactions (e.g., fines and judgments, loss of market share).

Of the six forms of loss, response, fines and judgments, competitive advantage, and reputation are most commonly associated with Secondary Loss. It is unusual to experience productivity or replacement loss within Secondary Loss. In the case of the loss of competitive advantage resulting from theft of trade secret information, the “secret” is lost immediately; the impact of the loss is realized over a long time period, and it may or may not occur.

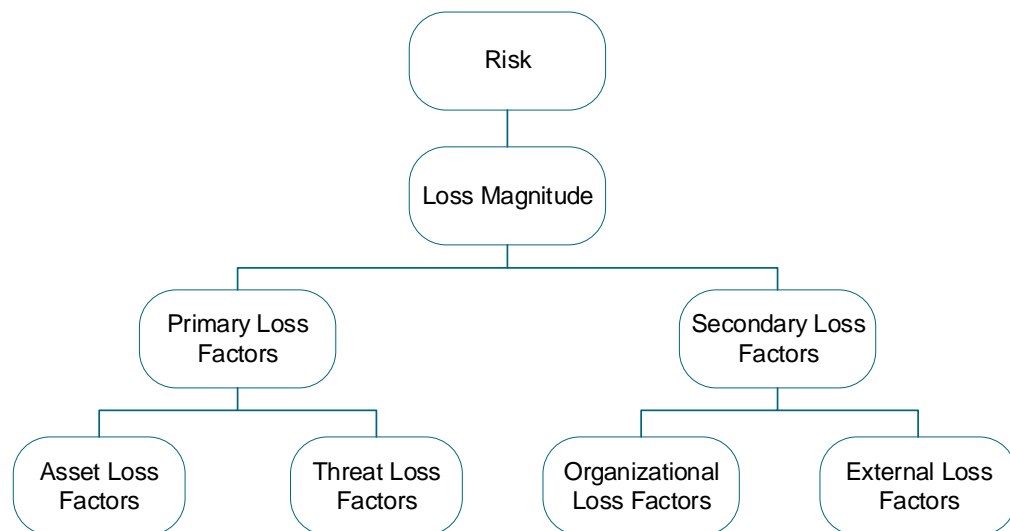
The effect of Secondary Loss on an organization can cascade. As losses pile up from initial Secondary Losses, additional Secondary Stakeholders may react negatively, compounding the

effect until losses are so great that the organization fails completely (e.g., the demise of Arthur Andersen in 2002).

### 4.4.3 Loss Factors

Loss factors are attributes or properties of the asset, threat, organization, or external environment that affect the magnitude of the loss to the Primary Stakeholder of a Loss Event.

Loss factors may contribute to either/both Primary or/and Secondary Loss, so the risk analyst must evaluate the factors within all four of these categories. However, asset and threat loss factors are referred to as Primary Loss Factors, while organizational and external loss factors are referred to as Secondary Loss Factors.



**Figure 9: Loss Factors**

#### 4.4.3.1 Asset Loss Factors

Asset loss factors include value/liability and volume.

The value/liability characteristics of an Asset play a key role in both the nature and magnitude of loss. Value/liability can be further defined as:

- **Criticality** – characteristics of an Asset that have to do with the impact on an organization's productivity; for example, the impact a corrupted database would have on the organization's ability to generate revenue
- **Cost** – the intrinsic value of the Asset; e.g., the cost associated with replacing it if it has been made unavailable (e.g., stolen, destroyed); for example, the cost of replacing a stolen laptop or rebuilding a bombed-out building
- **Sensitivity** – the harm that can occur from unintended disclosure

Sensitivity is further broken down into four sub-categories:

- **Embarrassment/Reputation** – the information provides evidence of incompetent, criminal, or unethical management and refers to reputation damage resulting from the

nature of the information itself, as opposed to reputation damage that may result when a Loss Event takes place

- **Competitive Advantage** – the information provides competitive advantage (e.g., key strategies, trade secrets) and, of the sensitivity categories, this is the only one where the sensitivity represents value; in all other cases, sensitivity represents liability
- **Legal/Regulatory** – the organization is bound by law or contract to protect the information
- **General** – sensitive information that does not fall into any of the above categories but would result in some form of loss if disclosed

Asset volume simply recognizes that more Assets at risk means greater Loss Magnitude if an event occurs (e.g., two children on a rope swing *versus* one child, or one sensitive customer record *versus* a thousand).

#### 4.4.3.2 Threat Loss Factors

Threat loss factors include action, competence, and whether the Threat Agent is internal or external to the organization, and how the Threat Agent then uses the compromised information Asset can affect the loss suffered by the Primary Stakeholder.

Threat Agents can take one or more of the following *actions* against an Asset:

- **Access** – unauthorized access of Asset(s)
- **Misuse** – unauthorized use of Asset(s)
- **Disclose** – illicit disclosure of sensitive information
- **Modify** – unauthorized changes to Asset(s)
- **Deny Access** – prevention or denial of authorized access

Note: Any of these actions may be the assigned mission of a Threat Agent.

Threat Agents take these actions after they have succeeded in committing a confidentiality, integrity, or availability breach against the stakeholder’s information Asset, as shown in Table 2.

**Table 2: Threat Agent Actions Following a Successful Breach**

Observed Information Asset Breach	Threat Agent Exploitation Post-Breach
Confidentiality	<p>Access – the Threat Agent gains unauthorized access but takes no further action beyond “having” the data.</p> <p>Misuse – the Threat Agent makes unauthorized use of the Asset in committing consequential losses to the Primary or Secondary Stakeholders, such as committing identity theft, setting up a pornographic distribution service on a compromised server, etc.</p> <p>Disclose – the Threat Agent illicit disclosure of sensitive information distributes information to other unauthorized parties.</p>



Observed Information Asset Breach	Threat Agent Exploitation Post-Breach
Integrity	Modify – the Threat Agent creates or modifies information that makes that information or information processing inaccurate or otherwise unreliable or untrustworthy. The stakeholder bears consequential losses from using inaccurate (unauthorized) information in its business processes.
Availability	Deny Access – the Threat Agent prevents or denies authorized access to the Asset. This includes deleting information, taking systems offline, and ransomware style events.

By gaining unauthorized access to information Assets, Threat Agents may establish a foothold in that Asset for later malicious use. If undetected, this foothold is not yet a loss to the Primary Stakeholder. When detected, the loss will be a confidentiality, integrity, or availability loss with the consequences that come from that loss. Threat Agents may gain a foothold as part of a long-term strategy to accomplish their assigned mission, such as to defeat or compromise an enemy military's future operation.

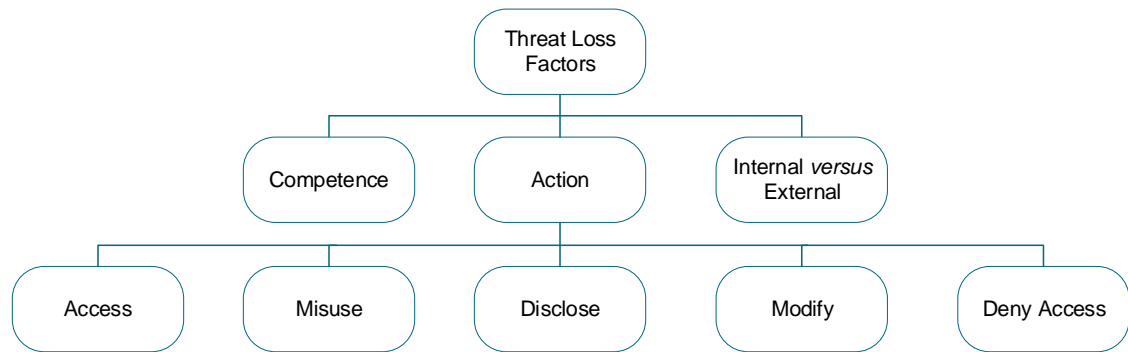
Each of these actions affects Assets differently, which drives the degree and nature of loss. The combination of the Asset, kind of violation, and kind of exploitation of this violation determines the fundamental nature and degree of loss. For example, the potential for productivity loss resulting from a destroyed or stolen Asset depends upon how critical that Asset is to the organization's productivity. If a critical Asset is simply illicitly accessed, there is no direct productivity loss. Similarly, the destruction of a highly sensitive Asset that does not play a critical role in productivity will not directly result in a significant productivity loss. However, that same Asset, if disclosed, can result in significant loss of competitive advantage or reputation, and generate legal costs.

Which action(s) a Threat Agent takes will be driven primarily by that attacker's motive (e.g., financial gain, revenge, recreation) and the nature of the Asset. For example, a Threat Agent bent on financial gain is less likely to destroy a critical server than to steal an easily pawned Asset like a laptop. For this reason, the risk analyst must have a clear definition of the Threat Community and its intended goal to evaluate Loss Magnitude effectively.

Threat competence is a measure of how able the Threat Agent is in exploiting the compromised Asset to accomplish some Threat Agent goal; it is the amount of damage a Threat Agent is capable of inflicting once the information Asset compromise occurs to the Primary or Secondary Stakeholders. For instance, a Threat Agent with low threat competence may not cause a large loss despite having sufficient Threat Capability to overcome the Asset's Controls.

Note: Threat competence differs from Threat Capability: threat competence affects Loss Magnitude while Threat Capability affects Loss Event Frequency.

*Whether a Threat Agent is external or internal to the organization* can play a pivotal role in how much loss occurs. Specifically, Loss Events generated by malicious internal Threat Agents (including employees, contractors, etc.) *typically* have not resulted in significant regulatory or reputation losses because it is recognized that trusted insiders are exceedingly difficult to protect against.



**Figure 10: Threat Loss Factors**

#### 4.4.3.3 Organizational Loss Factors

Organizational loss factors are those specific to the organization or business that suffers the loss and include when the Loss Event occurred, whether the organization took reasonable care in protecting the information Asset breached, and how it was able to detect the Loss Event in the first place.

When a Loss Event occurs, its *timing* can significantly impact Loss Magnitude. For example, the disclosure of earnings before public release or disclosure of a potential acquisition by an organization before the deal is publicly disclosed.

An organization's duty of *reasonable care* to protect the information Asset can affect the legal liability an organization faces from an event. Whether reasonable and appropriate preventative measures are in place (given the threat environment, value of the Asset, and legal and regulatory compliance requirements) can determine the severity of consequential legal and reputational damage.

How effectively an organization *responds* to an event can spell the difference between an event nobody remembers a year later and an event that stands out as an example (good or bad) in the annals of history. There are three components to a response:

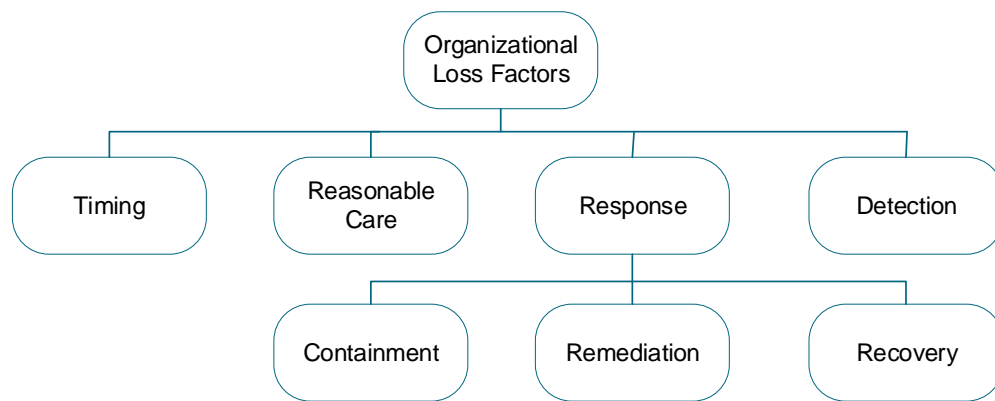
- **Containment** – an organization's ability to limit the breadth and depth of an event (e.g., cordoning-off the network to contain the spread of a worm)
- **Remediation** – an organization's ability to remove the Threat Agent (e.g., eradicating the worm)
- **Recovery** – the ability to bring things back to normal

All three of these response components must exist, and the degree to which any of them is deficient can have a significant impact on Loss Magnitude.

Response capabilities are usually considered solely within the context of criticality; e.g., the ability to return productivity to normal. However, response capabilities can also significantly affect losses resulting from sensitive information disclosure. For example, an organization that experiences a publicly disclosed breach of confidential customer information generally can significantly reduce its losses by being forthright in its admissions and by compensating harmed parties fully. Conversely, an organization that denies and deflects responsibility is much more likely to become a pariah and a media whipping post.

The organization must *detect* the Loss Event before it can respond and mitigate it. Incidents can take place that are undetected for a considerable period of time. However, for such an event to result in a material loss, it must first be detected. For example, the damage from sensitive competitive advantage information that makes its way to a competitor is likely to materialize and be recognized, though perhaps with less-than-timely detection. Only when detected, however, can the organization respond and reduce its losses, such as by taking legal action against a competitor who stole proprietary information.

Note: “Undetected Loss Events”, such as advanced persistent threats or situations described as a Threat Agent gaining a “foothold” (as described in [Section 3.5.3.2](#)) in a system to exploit at a later time are defined as Threat Events before they are detected and, once detected, become Loss Events.



**Figure 11: Organizational Loss Factors**

#### 4.4.3.4 External Loss Factors

External loss factors include external party detection, legal and regulatory, competitors, media, and Secondary Stakeholders (e.g., customers, partners, stockholders, shareholder activists).

These five categories represent entities that can inflict Secondary Loss upon the organization as a consequence of an event. In other words, events will often result in direct forms of loss (e.g., productivity, response, replacement) due to the criticality and inherent value characteristics of Assets. Secondary Losses may also occur based upon the external reaction to a Loss Event (e.g., sensitive information disclosure).

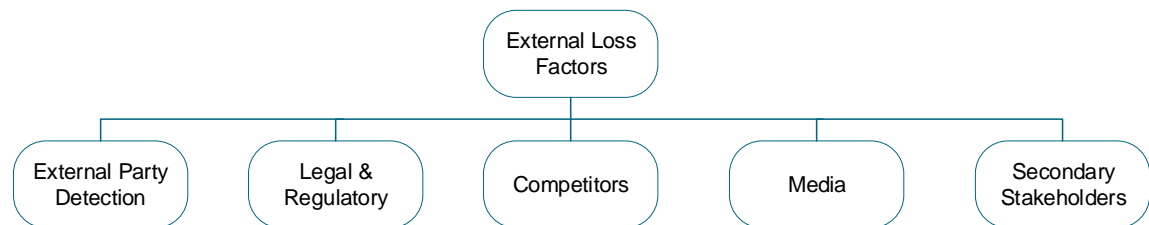
Moreover, all of the factors within these external categories can be described as “reactive to an event”. In other words, for an external factor to affect Loss Magnitude, the external party first must detect the event. For example, if an employee misuses his legitimate access to customer information to commit identity theft, the customer(s), regulators, and lawyers cannot inflict harm upon the organization unless that theft is tied back to the organization. Likewise, if a productivity outage is not detected by customers, partners, etc., then the organization will not be subject to a negative response on the part of those stakeholders.

*External party detection* can be thought of as a binary factor on which all other external factors are predicated. Detection of an event by an external party can happen as a consequence of the severity of the event, through intentional actions by the Threat Agent, through unauthorized disclosure by someone on the inside who is familiar with the event, through intentional disclosure by the organization (either out of a sense of duty, or because it is required by law), or by accident.

The *legal and regulatory landscape* likely affects the Primary Stakeholder’s exposure to fines, judgments, and other sanctions associated with a Primary Loss. Primary Stakeholders can recognize that environment, seek appropriate legal guidance, and act to mitigate their risk associated with legal and regulatory compliance.

Losses associated with the *competitive* landscape typically have to do with the competition’s ability and willingness to take advantage of the Primary Stakeholder’s loss of control of sensitive information.

*Media* reaction can have a significant effect on how stakeholders, lawyers, and even regulators and competitors view the event. If the media chooses to vilify the organization and keep it in the headlines for an extended period, the result can be much more significant. Conversely, if the media paints the organization as a well-intentioned victim that exercised reasonable care but still suffered the event at the hands of a criminal, then legal and reputation damage can be minimized. This is why organizations *must* have effective crisis communication processes in place.



**Figure 12: External Loss Factors**

#### 4.4.4 Summary: Loss Magnitude

Loss Magnitude consists of the Primary Stakeholder’s economic loss, measured in money or currency of a materialized Loss Event. These events consist of a direct impact, called the Primary Loss, and a potential secondary impact, called the Secondary Loss, initiated as a reaction to that Primary Loss by Secondary Stakeholders who become Secondary Threat Agents. Losses manifest themselves in six forms: productivity, response, replacement, fines and judgments, competitive advantage, and reputation.

Losses can be amplified or diminished by loss factors, which are how qualities of the asset, threat, organization, or external environment affect losses once they begin to occur.

**Table 3: Loss Magnitude Factors**

Loss Magnitude Factor	Description	Unit of Measure
Total Loss Magnitude	Sum of Primary and Secondary Loss Magnitude; an economic loss	Money, currency
Primary Loss Magnitude	Direct economic losses associated with a confidentiality, integrity, or availability loss of information Assets	Money, currency

Loss Magnitude Factor	Description	Unit of Measure
Secondary Loss Magnitude	Indirect, conditional losses associated with Secondary Stakeholders affected by the Primary Loss becoming Threat Agents and trying to cause a loss to the Primary Stakeholder	Money, currency
Secondary Loss Event Frequency	Conditional probability that a Primary Loss will result in a Secondary Loss	Probability (between 0-1 or measured as a percentage, between 0 and 100%)
Forms of Loss	Six forms of loss that completely describe possible losses and can occur as a Primary or Secondary Loss: productivity, response, replacement, fines and judgments, competitive advantage, and reputation.	Money, currency
Loss Factors	Four loss factors that affect magnitude of loss: asset, threat, organizational, external	Dimensionless scalars, multipliers

## A Risk Taxonomy in the Context of Risk Analysis

---

Extensive discussion in development of this risk taxonomy included considerations that can be grouped into four categories:

- Concerns regarding complexity of the model
- The availability of data to support statistical analyses
- The iterative nature of risk analyses
- Perspective

Many of these considerations are not so much critical of the Open FAIR framework, but rather are observations and concerns that apply no matter what method is used to analyze risk.

### A.1 Complexity of the Model

There is no question that the Open FAIR framework goes into greater detail than most (if any other) information risk models, and if usage of the framework required analyses at the deepest layers of granularity, then it would indeed be impractical for most risk analyses. Fortunately, most analyses can be performed using data and/or calibrated estimates at higher levels of abstraction within the model; e.g., measuring Threat Event Frequency rather than attempting to measure Contact Frequency and Probability of Action. This flexibility within the framework allows the user to choose the appropriate level of analysis depth based on their available time, data, as well as the complexity and significance of the scenario being analyzed.

Of course, the fact that the framework includes greater detail provides several key advantages:

- The aforementioned flexibility to go deep when necessary
- A greater understanding of contributing factors to risk
- The ability to better troubleshoot/critique analysis performed at higher layers of abstraction

Another consideration to keep in mind is that risk is inherently complicated. If it were not, then there would be no need for well-defined frameworks and no challenges over analyzing risk and communicating about it. Using over-simplified and informal models almost invariably results in unclear and inconsistent assumptions, leading to flawed conclusions, and therefore false recommendations. With that in mind, even the detailed Open FAIR taxonomy is not a perfect or comprehensive treatment of the problem. There are no perfect taxonomies/models of real-world complexity.

With regard to communicating complex risk information to business decision-makers (who often want information like this delivered in simple form), the problem is not inherently with the model, but rather with the user. As is the case with any complex problem, results must be articulated in a way that is useful and digestible to decision-makers. It is also not unusual for

management to ask how the analyst arrived at their results, and having a rigorous framework to refer to in the explanation tends to improve credibility and acceptance of the results.

## **A.2 Availability of Data**

In risk assessments, good data is especially difficult to acquire for infrequent events. In the absence of such data, how do we arrive at valid frequency estimates?

Good data has been and will continue to be a challenge within the risk problem space for some time to come. In part, this stems from the absence of a detailed framework that:

- Defines which metrics are needed
- Provides a model for applying the data so that meaningful results can be obtained

The Open FAIR framework has been proven in practice to help solve those two issues. It does not, of course, help with those instances where data is unavailable because events are rare. In those cases, regardless of the analysis method chosen, the estimates cannot be as well substantiated by data. On the other hand, the absence of data due to the infrequency of events *is* data – of sorts – and can be used to help guide our estimates. As additional information is acquired over time, it is possible to adjust the initial estimates.

## **A.3 Iterative Risk Analyses**

Due to the inherent complexity of risk, risk analyses tend to be iterative in nature. In other words, initial risk analyses tend to be “sighting shots” that become more precise as additional analyses are performed. Furthermore, there comes a point of diminishing returns beyond which additional precision is not warranted given the necessary time and expense of deeper/broader analyses. Of course, this is true of any analysis method, including the Open FAIR model.

## **A.4 Perspective**

An alternative view held by some is that “exposure” should be the focus rather than “risk”. The argument put forward here is that “risk” can be thought of as the inherent worst-case condition, and “exposure” represents the residual risk after Controls were applied.

Setting aside the possibility that those who hold this view misinterpret the definition of risk within the Open FAIR model, both issues are related (sort of a “before” and “after” perspective) and relevant. The Open FAIR framework provides the means to analyze both conditions by allowing the analyst to derive unmitigated risk as well as mitigated risk levels.

## B Practical Use of the Open FAIR Method

---

### B.1 The Risk Language Gap

Over time, the ways to manage risk have evolved to keep up with ways to conduct business. There is a long history here, predating the use of IT in business. As the scope, scale, and value of business operations have evolved, specializations to manage the risk have similarly evolved, but in doing so, each specialization has developed its own view of risk and how to describe its components. This has resulted in a significant language gap between the different specializations, all of whom are stakeholders in managing risk.

This gap is particularly evident between business managers and their IT risk/security specialists/analysts. For example, business managers talk about “impact” of loss, not in terms of how many servers or operational IT systems will cease to provide normal service, but rather what the impact will be of losing these normal services on the business’s capacity to continue to trade normally, measured in terms of \$-value; or will the impact be a failure to satisfy applicable regulatory requirements which could force them to limit or even cease trading and perhaps become liable to heavy legal penalties.

Therefore, a business manager tends to think of a “threat” as something which could result in a loss that the business could not absorb without seriously damaging its trading position. Compare this with our risk taxonomy definitions for “Threat” and “Vulnerability”:

- **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
- **Vulnerability:** the probability that a Threat Event will become a Loss Event

Similar language gaps exist between other stakeholders in management of risk. Politicians and lawyers are particularly influential stakeholders: they are in the powerful position of shaping national and international policy (e.g., OECD, European Commission), which in turn influences national governments to pass laws and regulatory regimes on business practices that become effective one to three years down the line.

### B.2 Key Risk Concepts

This document is an essential step towards enabling all stakeholders in risk management to use key risk management terms – especially Control, Asset, Threat, and Vulnerability – with precise meanings to bridge the language gap between IT specialists, business managers, lawyers, politicians, and other professionals, in all sectors of industry and commerce and the critical infrastructure, whose responsibilities bear on managing risk.



## B.3 Using the Open FAIR Model with Other Risk Assessment Frameworks

This document describes the factors that contribute to risk and how they affect each other, and is primarily concerned with establishing accurate estimates for the probable frequency and probable magnitude of future Loss Events associated with information and information technology. It is not, *per se*, a “cookbook” that describes how to perform an enterprise (or individual) risk assessment. For example, the Open FAIR documentation does not specify where and how an analyst should obtain information to use in the assessment, as much as it explains how to describe the value of that information and how the information contributes to risk. In particular, this document specifies the factors and their relationships that comprise risk but not a single, deterministic model to calculate each factor.

Many information security standards and frameworks specify that information risk assessments *should be done* but provide little to no specifications on *how to do* them. The O-RT and O-RA Standards along with guidance documentation from The Open Group provide a way to quantify risk in those information security standards and frameworks.

Senior management and boards of directors are guided by best practices within their professional domains to treat information risk as an enterprise risk, and the Open FAIR model is one standard that allows that risk to be expressed in economic, business terms, and in the same units of measure as other enterprise risks. This compatibility of the unit of measure of risk between information risk and other business operational risks allows information risk to be compared, contrasted, and aggregated to develop overall enterprise-wide risk assessments. In essence, “risk is risk”, whether it is related to an enterprise’s operation, a bank’s loan portfolio, a trading desk’s value at risk, or information technology: it is the probable frequency of an uncertain loss and the magnitude of that loss expressed as a distribution of economic outcomes.

Practitioners who must perform information technology risk assessments to comply with other industry and regulatory standards, frameworks, and methodologies can use the Open FAIR taxonomy and framework to build consistent and defensible risk statements that are measured in the same economic terms as other risks they have to manage.

## Index

abstraction .....	2, 10	response.....	24
Asset volume .....	22	containment.....	24
competitive landscape .....	26	recovery .....	24
competitors .....	25	remediation .....	24
contact .....	13	risk.....	10
intentional .....	13	risk assessment .....	8
random .....	13	risk factor .....	1
regular .....	13	risk factor variables .....	9
Contact Frequency (CF) .....	13	risk management stack .....	9
data metrics .....	29	risk measurement .....	11
detection .....	25, 26	Secondary Loss .....	20
flexibility .....	28	Secondary Loss Event .....	19
information security risk .....	1	Secondary Loss Event Frequency	
legal and regulatory .....	25	(SLEF) .....	20
loss.....	18	Secondary Loss Factors.....	21
competitive advantage.....	19	Secondary Loss Magnitude (SLM) ..	20
fines/judgments .....	19	secondary stakeholders.....	25
productivity .....	18	sensitivity	
replacement .....	19	competitive advantage .....	22
reputation .....	19	embarrassment/reputation .....	21
response.....	19	general.....	22
loss analysis.....	17	legal/regulatory .....	22
Loss Event Frequency (LEF).....	12	Threat Capability (TCap) .....	15
loss exposure .....	10, 11	threat competence.....	23
Loss Magnitude (LM) .....	17	Threat Event Frequency (TEF) .....	12
media .....	25, 26	threat loss factors .....	22
password strength .....	16	action .....	22
possibility .....	11	competence .....	22
prediction.....	11	internal or external to the	
Primary Loss .....	20	organization.....	22
Primary Loss Event .....	19	timing .....	24
Primary Loss Factors .....	21	unintended disclosure.....	21
probability .....	11, 14	value/liability .....	21
probability factor		cost.....	21
level of effort.....	14	criticality .....	21
risk of detection/capture .....	14	sensitivity .....	21
value .....	14	volume.....	21
Probability of Action (PoA) .....	13	Vulnerability (Vuln).....	14
Resistance Strength (RS) .....	16		