Open Group Standard

Risk Analysis (O-RA)

Copyright © 2013, 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 implementers to use the names, labels, etc. contained within the specification. The intent of publication of the specification is to encourage implementations of the specification.

Technical Standard

Risk Analysis (O-RA)

ISBN: 1-937218-41-6

Document Number: C13G

Published by The Open Group, October 2013.

Please note that this standard was re-issued in May 2014 with a revised copyright notice.

Comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

Preface

The Open Group

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

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

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

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

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

This Document

This document is The Open Group Standard for Risk Analysis (O-RA). It is a companion document to the Risk Taxonomy Standard.

This document provides a set of standards for various aspects of information security risk analysis.

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 Risk Analysis Standard 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 Risk Analysis Standard, and the companion Risk Taxonomy Standard, to be used as a foundation for normalizing the results of risk analyses across varied risk domains.

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

- **The Open Group Risk Taxonomy (O-RT), Version 2.0 Technical Standard** (C13K, October 2013) defines a taxonomy for the factors that drive information security risk – Factor Analysis of Information Risk (FAIR). This standard was first published in January 2009, and has been revised as a result of feedback from practitioners using the standard and continued development of the FAIR taxonomy.
- **The Open Group Technical Guide: Requirements for Risk Assessment Methodologies** (G081, January 2009) identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements. In this way, it explains what features to look for when evaluating the capabilities of any given methodology, and the value those features represent.
- **The Open Group Technical Guide: FAIR – ISO/IEC 27005 Cookbook** (C103, November 2010) describes in detail how to apply the Factor Analysis of Information Risk (FAIR) methodology to ISO/IEC 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.

Trademarks

ArchiMate®, DirecNet®, Jericho Forum®, Making Standards Work®, OpenPegasus®, The Open Group®, TOGAF®, and UNIX® are registered trademarks and Boundaryless Information Flow™, Dependability Through Assuredness™, FACE™, Open Platform 3.0™, and The Open Group Certification Mark™ are trademarks of The Open Group.

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

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 contributions of the following individuals for their valued original work and their continued support in guiding the Security Forum members through our process to develop this Risk Analysis Standard:

- Chris Carlson, Boeing
- Jim Hietala, VP Security, The Open Group
- Jack Jones, CXOWARE
- Michael Legary, Seccuris
- James Middleton, Nationwide Insurance
- Steve Tabacek, CXOWARE
- Chad Weinman, CXOWARE

Informal contributions and commentary were also provided by these risk industry outside experts. We thank them for their input and contributions:

- Jack Freund, TIAA-CREF
- Alex Hutton, Zions Bank
- David Musselwhite, Quicken Loans
- Ben Tomhave, Lockpath

The Open Group also acknowledges the members of the Security Forum who have contributed to the development of this Standard.

Special thanks go to Douglas Hubbard, author of How to Measure Anything. Many of the ideas in the measurement and calibration section of this standard were originally described by him in this important book.

Referenced Documents

The following documents are referenced in this Standard:

- An Introduction to Factor Analysis of Information Risk (FAIR), Risk Management Insight LLC, November 2006; refer to: www.riskmanagementinsight.com.
- FAIR – ISO/IEC 27005 Cookbook, Technical Guide, C103, published by The Open Group, November 2010; refer to: www.opengroup.org/bookstore/catalog/c103.htm.
- How to Measure Anything: Finding the Value of Intangibles in Business, Douglas W. Hubbard, John Wiley & Sons, 2010.
- Requirements for Risk Assessment Methodologies, Technical Guide, G081, published by The Open Group, January 2009; refer to: www.opengroup.org/bookstore/catalog/g081.htm.
- Risk Taxonomy (O-RT), Version 2.0, Open Group Standard, C13K, published by The Open Group, October 2013; refer to: www.opengroup.org/bookstore/catalog/c13k.htm.

1 Introduction

1.1 Objective

The objective of this Risk Analysis (O-RA) Standard is to enable risk analysts to perform effective information security risk analysis using the Factor Analysis of Information Risk (FAIR) framework. When coupled with the Risk Taxonomy (O-RT) Standard, it provides risk analysts with the specific processes necessary to perform effective FAIR-based risk analysis.

This Standard should be used with the companion Risk Taxonomy Standard 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 Risk Analysis Standard is intended to be used with the Risk Taxonomy Standard, which defines the FAIR taxonomy for the factors that drive information security risk. Together, these two standards comprise a body of knowledge in the area of FAIR-based information security risk analysis.

Although the terms “risk” and “risk management” mean different things to different people, this Standard 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”.

Although the concepts and standards within this Standard were not developed with the intention of being applied towards other risk types, experience has demonstrated that they can be effectively applied to other risk types. For example, they have been successfully applied in managing the likelihood and consequence of adverse events associated with project management or finance, in legal risk, and by statistical consultants in cases where probable impact is a concern (e.g., introducing a non-native species into an ecosystem).

1.3 Conformance

At the time of publication, there are no conformance requirements defined in this section for the purposes of this Standard. Readers are advised to check The Open Group web site for any conformance and certification requirements referencing this Standard.

1.4 Normative References

The following standards contain provisions which, through references in this Standard, constitute provisions of the Risk Analysis Standard:

- Risk Taxonomy (O-RT), Version 2.0, Open Group Standard, C13K, published by The Open Group, October 2013; refer to: www.opengroup.org/bookstore/catalog/c13k.htm.

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.

1.5 Terminology

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

Can Describes a permissible optional feature or behavior available to the user or application. The feature or behavior is mandatory for an implementation that conforms to this document. An application can rely on the existence of the feature or behavior.

May Describes a feature or behavior that is optional for an implementation that conforms to this document. An application should not rely on the existence of the feature or behavior. An application that relies on such a feature or behavior cannot be assured to be portable across conforming implementations. To avoid ambiguity, the opposite of “may” is expressed as “need not”, instead of “may not”.

Must Describes a feature or behavior that is mandatory for an application or user. An implementation that conforms to this document shall support this feature or behavior.

Shall Describes a feature or behavior that is mandatory for an implementation that conforms to this document. An application can rely on the existence of the feature or behavior.

Should For an implementation that conforms to this document, describes a feature or behavior that is recommended but not mandatory. An application should not rely on the existence of the feature or behavior. An application that relies on such a feature or behavior cannot be assured to be portable across conforming implementations. For an application, describes a feature or behavior that is recommended programming practice for optimum portability.

Will Same meaning as “shall”; “shall” is the preferred term.

1.6 Future Directions

As a standards body, The Open Group aims to evangelize the use of FAIR within the context of these risk assessment or management frameworks. Our aim is to continue to work to describe how FAIR may be used with other risk assessment frameworks. In doing so, The Open Group becomes not just a group offering yet another risk assessment framework, but a standards body which solves the difficult problem of developing consistent, defensible statements concerning risk.

2 Introduction to FAIR Risk Analysis

2.1 Assessment *versus* Analysis

The information security profession (and the broader enterprise risk management discipline to some degree) often does not clearly and consistently differentiate between "risk assessment" and "risk analysis". There is a difference, however, which is important to understand. Risk assessments tend to encompass a broader context that includes processes and technologies that identify, evaluate, and report on risk-related concerns. Risk analysis can be considered the evaluation component of the broader risk assessment process, which determines the significance of the identified risk concerns.

Virtually all risk assessment processes and tools attempt to risk-rate their findings in some fashion. Historically, these ratings are set using qualitative/ordinal scales and practitioner estimates (e.g., "this issue is high risk" or "this is a 4 on a scale of 1-to-5") without undergoing any meaningful analysis. As a result, the ratings are vulnerable to bias (intended or not), poorly defined models, and undefined assumptions. Risk analysis performed using Factor Analysis of Information Risk (FAIR) – or any other similarly rigorous method – is intended to support more effective analyses so that the resulting risk statements are less vulnerable to these problems and thus are more meaningful and defensible.

2.2 Why is a Tightly-Defined Taxonomy Critical?

Without a logical, tightly-defined taxonomy, risk analysis approaches will be significantly impaired by an inability to measure and/or estimate risk factor variables. This, in turn, means that management will not have the necessary information for making well-informed comparisons and choices, which will lead to inconsistent and often cost-ineffective risk management decisions. The Open Group Risk Taxonomy Standard (based on FAIR) provides the clear definition of risk factors and risk factor relationships necessary to guide professionals in their analysis of risks.

2.3 Risk Analysis Approach

All risk analysis approaches must include the following fundamental process elements:

- 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 using a model that represents a logical, rational, and useful view of what risk is and how it works

The first two elements above can be summarized as “scoping” the analysis. Practitioners must recognize that time spent in scoping is crucial to performing effective analyses. In fact, carefully scoping an analysis virtually always results in an overall saving in time spent on the analysis, due to better clarification of data requirements and less time spent troubleshooting and revising the analysis.

When performing risk analysis it is also important to recognize that risk-related data is never perfect. In other words, there will always be some amount of uncertainty in the data being used. As a result, measurements and estimates should faithfully reflect the quality of data being used. The most common approach to achieving this is to use ranges and/or distributions rather than discrete values as inputs. Calculating results can then be accomplished using Monte Carlo or other stochastic methods.

3 Risk Measurement and Calibration

This chapter defines a very specific challenge in risk analysis, namely how to measure and calibrate risk in a variety of circumstances. Measurement and calibration are fundamental to performing effective risk analysis. These concepts have been informed by the work of Douglas Hubbard, whose book *How To Measure Anything* describes many of the methods of measurement and calibration, including the wheel mechanism for increasing confidence in estimates for data.

3.1 Calibration

Calibration is a method for gauging and improving an individual’s ability to make good estimates. Because measuring risk involves making good estimates, calibration is critical for risk analysts to understand. Performing calibration to make better estimates is a skill that can be learned.

3.1.1 Starting with the Absurd

Calibration starts with making absurd estimates. The purpose of doing this is to enable the risk analyst to recognize starting values for the estimation which are clearly not possible. It is also an attempt to break any bias that an analyst may have. An example of starting with an absurd estimate would be if you were asked to estimate the wingspan of a Boeing 747, and you provided as an absurd estimate 10' on the low side, and 300' on the high side. Someone with experience seeing the airplanes at airports will recognize that these values are absurd estimates, perhaps using as frames of reference the height a of basketball hoop on the low end, and the length of a football field on the high end. Once we understand that these are absurd values for minimum and maximum (min/max) values in a range, we can start to narrow in on values that we'll have more confidence are appropriate as min/max values in a range. So starting with these clearly absurd values, it then becomes more possible to narrow in on a more realistic range of min/max values.

3.1.2 Decomposing the Problem

Measurement and estimation in risk analysis requires the analyst sometimes to decompose broad, high-level risk components into smaller pieces that are easier to deal with. An example of this might be trying to estimate the height of the Willis Tower in Chicago – formerly known as the Sears Tower. By decomposing the problem into “how many floors is the building” and “how much vertical space does each floor occupy”, we can start to make sense of the entire question. In information security risk analysis, a similar broad question might be: “How much risk do we have around lost laptops and Personally Identifiable Information (PII)?”. To decompose this into components that we can more easily deal with (and for which we might have data to support risk analysis), we can ask ourselves questions such as: “How many laptops have we historically lost each year?”, “How much PII is being stored on laptops by employees?”, and “What costs do organizations similar to ours experience when they lose PII?”.

3.1.3 Testing Confidence using the Wheel, Establishing 90% Confidence Overall, and 95% Confidence at Each End

The wheel is a mechanism to help strengthen an analyst's conviction or confidence in an estimated range of values, to move them to a point where the analyst is 90% confident that the actual value is within the min/max range. The wheel mechanism helps risk analysts improve their calibration abilities by forcing them to really evaluate (and revise) their choice for a min/max value in a range.

With an initial absurd range for the value, the next step is to narrow the range to more accurately estimate the actual values so that the analyst is confident that the actual value will fall within the range 90% of the time (a 90% confidence interval).

Hubbard uses the analogy of a wheel to help narrow the range (Hubbard, 2007, p.57ff). The analyst is offered a choice between two scenarios:

1. They will receive $1,000 if the actual value falls within their prediction.
2. Spinning a wheel with 90% of its area painted black and 10% painted red. They will win $1,000 if the wheel stops in the black.

The wheel obviously implements a 90% confidence interval and the desired goal is that the analyst has no preference between the two methods. If the analyst prefers the wheel, then they are not truly confident that their estimate represents a 90% confidence interval for the value and the estimate needs to be revised. The confidence interval can be tightened by asking the analyst to make the same choice regarding whether the estimate will be less than (or greater than) some value 95% of the time.

3.1.4 Challenging Assumptions

Assumptions may be challenged by getting other analysts’ estimates, and by finding data that is useful to the estimation activity. Challenging assumptions is important when estimating because when our assumptions are off, our estimations will be as well.

3.2 Distributions

FAIR risk analysis makes extensive use of distributions when making measurements or estimates. Creating distributions in FAIR requires the analyst to provide four parameters:

- Minimum Likely Value
- Most Likely Value
- Maximum Likely Value
- Confidence Level

The distributions (description of how often particular values appear in the data) created during a FAIR analysis are used to express many of the elements of the Risk Taxonomy, including (among others) distributions for Contact Frequency (CF), Probability of Action (PoA), Threat Capability (TCap), and Resistance Strength (RS). The advantage to using distributions *versus* attempting to derive discrete values is that it is for the most part impossible to get to a discrete value. For example, when estimating attacker TCap, we typically see a range of different attackers, with different skills and experience, so using a range is a more accurate way to represent TCap. The same can be seen to be true for other taxonomy elements such as PoA and RS. Using distributions in risk analysis helps to provide more accurate results.

3.3 Most Likely Values

Within distributions, the value most likely to be observed is the value that appears most often among all values in the entire data set.

3.4 Monte Carlo

Monte Carlo simulations are a method for analyzing data that has significant uncertainty. Monte Carlo simulations perform repeated random sampling to obtain numerical results. The output of Monte Carlo simulations used in risk analysis is shown as probability distributions. The primary advantage of using Monte Carlo simulations in risk analysis is the ability of the method to perform thousands of calculations on random samples, allowing risk analysts to create a more accurate and defensible depiction of probability given the uncertainty of the inputs.

3.5 Accounting for Uncertainty

3.5.1 Range Confidence

Confidence in the end-points of the range is built through training for risk analysts to improve their calibration, and remove their personal estimating biases. The wheel exercise, described in Section 3.1.3, helps to improve calibration and reduce personal bias.

3.5.2 Curve Shaping

Curve shaping refers to the degree of confidence that the analyst has in the most likely value within a distribution. Distributions for which analysts have a very high degree of confidence in the most likely value will be very peaked and narrow, while distributions in which analysts have a low level of confidence in the most likely value will be more flat. An example of a distribution where there is a high degree of confidence in the most likely value might be estimating the range of values for the number of presidential candidates to receive more than 5% of votes. In most modern US elections, there have been exactly two. In terms of how we can increase confidence in the most likely value, we can again use the wheel to move our estimates of most likely values to an improved confidence level for estimates where we don’t have significant data.

3.6 Accuracy *versus* Precision

Accuracy can be defined for risk analysis as “our capability to provide correct information”, while precision is “exact, as in performance, execution, or amount”. Estimates that are falsely precise can mislead decision-makers into thinking that there is more rigor in the risk analysis than there actually is. Using distributions or ranges can bring higher degrees of accuracy to estimates.

An example of an estimate that is precise but inaccurate would be to estimate that the wingspan of a 747 is exactly 107'. An example of an estimate that is accurate but not precise would be to estimate that the wingspan of a 747 is between 1' and 1000'.

The concept of a useful degree of precision refers to creating estimates that have a level of precision that matches the objective of the estimation exercise. To extend the airplane wingspan example, if our range estimate is 10' to 300', and the objective of the estimation exercise is to allow us to build a hangar that will be big enough to house the plane, then the estimate is likely accurate, but it is not usefully precise.

3.7 Subjectivity *versus* Objectivity

Objective risk measurements are those which are not influenced by personal feelings, interpretations, or prejudice; but which are based on facts and are unbiased. Subjective risk measurements are those which are influenced by personal feelings, interpretations, or prejudice.

Data that is more subjective in nature includes data that is informed primarily by one person's opinion. An information security example might be if we asked a random employee at a company how many laptops the company loses in a given year. Their opinion would be a pretty subjective answer, perhaps informed by their own experience, or their knowledge of co-workers who have lost laptops.

Our goal as risk analysts is to drive objectivity into our risk measurements to the greatest extent possible. We have two primary mechanisms for doing this. The first is to gather more data to help inform the risk estimate. The second mechanism is to develop a better understanding of what the estimates are derived from; in other words, the factors that make up or influence the estimates. The precise definitions and relationships provided in the Risk Taxonomy Standard help to inform this understanding.

Data that is objective in nature, to use the example above, would include going to the IT group in charge of managing IT assets, and asking them for the records of lost laptops for the past several years.

It is important to understand that for many risk measurements, subjectivity and objectivity exist on a spectrum, such that a given measurement is not purely objective or subjective. Purely objective data is not achievable because humans are inherently subjective by their nature. So humans have to decide what data to capture, how to collect it, and what filters to apply to the use and presentation of the data, all of which can (and frequently do) introduce bias.

3.8 Deriving Vulnerability (Vuln)

Vulnerability is the probability that an asset will be unable to resist the actions of a threat agent. Deriving vulnerability in a FAIR risk analysis requires the risk analyst to estimate the Threat Capability (TCap) (expressing this as a distribution of potential attackers), and to estimate Control Strength (CS) (expressing this as a distribution of percentages). An important distinction is that the percentages provided in the estimate for CS represent the min/most likely/max values for the % of time that the control will be resistant to attack for a specific community of attackers, as defined when describing the TCap in a specific FAIR analysis. Once we have estimated the ranges for TCap and RS, we use Monte Carlo analyses to compare a random sample from TCap with a random sample from RS. Running thousands of random samples, we are able to determine in what percentage of those samples we are vulnerable.

3.8.1 Threat Capability (TCap) Continuum

In FAIR, Threat Capability (TCap) refers to the level of skills and resources possessed by the potential attacker. 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 TCap continuum describes attackers as existing at various percentiles, where the 25th percentile are not very skilled, the 50th percentile are mid-level skilled, and the 99th percentile are highly skilled.

3.8.2 Defining a Threat Community TCap Distribution

In performing a FAIR risk analysis, the analyst defines a minimum likely capability for the threat, a maximum likely value, and a most likely value. These represent the minimum level of skills that we expect an attacker to have, the maximum level of skills an attacker might have, and the skill level of the most likely attacker. All of these values must be created with a 90% confidence level.

3.9 Ordinal Scales

Using ordinal scales (for example, 0-5) to measure components in a risk analysis, or to categorize overall risk level, brings numerous problems.

These include:

- The meaning of each ordinal value is undefined.
- Ordinal values don't accommodate range values spanning multiple ordinal values. For example, if our ordinal scale starts at 1, defined as range of probability from 1-20%, and 2, defined as 21-40%, how do we deal with a range of probability from 15-35%?
- Ordinal numbers shouldn't (or can't) be multiplied, at least not without creating arbitrary results with little meaning.

3.10 Diminishing Returns

Douglas Hubbard suggests in his book that:

"*The information value curve is usually steepest in the beginning. The first 100 samples reduce uncertainty much more than the second 100.*"

To the FAIR risk analyst, this means that there is a diminishing return associated with gathering more data in a risk analysis.

4 The Risk Analysis Process

This chapter provides insights into how to leverage the taxonomy to perform a risk analysis. The informative example scenario provided is the same as the one within the Risk Taxonomy Standard but will be covered in more depth within this Standard.

The example scenario we will use throughout this section is defined below:

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

Before we get started, think to yourself how you would rate the level of risk within this scenario based upon the assessments you've seen or done in the past.

Important Note: This example uses quantitative ranges assigned to qualitative terms (e.g., "High", "Medium", etc.) as a means of demonstrating how the taxonomy is applied to an analysis. Factor Analysis of Information Risk (FAIR) is more widely recognized in industry for its ability to be leveraged in a more effective quantitative analysis performed using PERT distributions as inputs, and leveraging Monte Carlo as the computational process. Further, many of the risk measurement and calibration topics discussed in Chapter 3 relate to the quantitative application of the taxonomy.

4.1 The Analysis: FAIR Basic Risk Analysis Methodology

The simplified process we will use in this example is comprised of four main stages, as follows:

- Stage 1: Identify Scenario Components (Scope the Analysis)
- Stage 2: Evaluate Loss Event Frequency (LEF)
- Stage 3: Evaluate Loss Magnitude (LM)
- Stage 4: Derive and Articulate Risk

4.1.1 Stage 1: Identify Scenario Components (Scope the Analysis)

4.1.1.1 Assumptions

It is important to realize that in any risk analysis, regardless of method, assumptions will play a role. In order to effectively manage this reality it is important that the analyst clearly documents their key assumptions to ensure all that those who review the analysis understand the basis for the values that were used. One area where documenting all assumptions is vital is within the identification of the components (i.e., scoping) of the analysis.

4.1.1.2 *Identify the Asset at Risk*

The first question we have to answer is: “What asset is at risk?” Another way to think about this is to determine where value or liability exists.

A typical question in a scenario where we are analyzing lost mobile devices is whether the devices themselves are the asset, or whether it’s the information stored on or accessed by the devices. The short answer is “they’re all assets”. In this case, however, it’s almost always the information we’re concerned about because its value is far greater to an organization than the device itself.

In our scenario provided at the start of this section we have multiple assets: the credentials as well as the applications, systems, and information that the credentials provide access to. In this case, however, we’ll focus on the credentials, recognizing that their value is inherited from the assets they are intended to protect.

4.1.1.3 *Identify the Threat Community*

The second question we have to answer is: “Risk associated with what threat?” If we examine the nature of the organization (e.g., the industry it’s in, etc.), and the conditions surrounding the asset (e.g., an HR executive’s office), we can begin to parse the overall threat population into communities that might reasonably apply. How many threat communities we choose to analyze, and how we subdivide them, is up to us. It’s probably not a good use of time to include every conceivable threat community in our analysis. It is recommended to create a short list of the most probable threat communities.

Are we saying that it’s not possible for a nation-state spy to attack this bank through this exposure? No. But by considering the nature of the threat communities relative to the industry, organization, and asset, we can come to reasonable conclusions without falling victim to analysis paralysis.

Within this scenario, it seems reasonable to consider the risk associated with the following threat communities:

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

With experience it becomes easier to determine which communities are worthwhile to include and exclude. For this example, we’ll focus on the cleaning crew.

An additional technique to further define a threat community is to build a “profile” or list of common characteristics associated with a given threat community. While there is no standard list of attributes that should be evaluated for each and every threat community, some common characteristics to consider include:

- Motive
- Objective
- Access Method
- Personal Risk Tolerance
- Desired Visibility
- Sponsorship
- Skill Rating
- Resources

4.1.1.4 *Identify the Loss Event*

In order to develop well-reasoned estimates, it is also important to identify the type of threat event under analysis. Specifically, there are four types of threat scenarios:

- Malicious (where harm is intended); e.g., an attempted theft
- Error (where an act occurred that was not intended); e.g., entering the wrong command at a keyboard
- Failure (where an act resulted in unintended consequences); e.g., the right command was given, but the system failed to perform as intended
- Natural (resulting from acts of nature); e.g., high winds

In many cases, a final consideration regarding the definition of a threat event under analysis is to identify the "threat vector". Essentially, the threat vector represents the path and/or method used by the threat agent. For example, an attacker seeking to gain access to sensitive corporate information may try any of a number of vectors – through technical attacks, leveraging human targets, etc. Identifying the relevant vector can be important because each vector may have a different frequency and different control levels. In some cases, threat communities also have different capabilities for different vectors.

The final scoping question we have to answer is: "What does the loss event look like?" Another way to think about this is to clearly define the event that may occur which would result in a loss to the organization. By answering this question we can ensure that all stakeholders are aware of the primary concern or event we are measuring (i.e., managing assumptions).

The specificity of this description is important. Note that it 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. Could the analysis be more general and include these other scenarios? Yes, but because the frequency and impact of these scenarios may vary significantly, making effective estimates would likely be impractical.

When identifying and defining the loss event on which the analysis will focus, it is useful to consider the threat event type. Since we have profiled the threat community, the threat event type further defines the context in which the threat community is likely to affect the asset. Common threat events include: malicious, error, failure, and natural/environmental.

In our example, we could define the loss event as: *the malicious access 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*.

4.1.1.5 Scenario Parsing

During the scoping of the analysis we can consider whether to combine multiple scenarios into a single analysis or whether we should decompose our analysis down to a single scenario. While there are no "rules" on this topic there are some key considerations to share.

Often we may want to perform a single analysis that encompasses more than one threat community or asset. This is generally acceptable but careful consideration should be given if:

- The threats do not share the same objective.
- The threats do not share the same access methods (internal *versus* external human threats).
- There is more than one asset and each one is distinctly different (e.g., location, controls, value).

If any of the cases above are true, the analyst should consider performing more than a single analysis. It often takes less time and is more efficient to perform multiple "simpler" analyses than to try to make estimates for more complex scenarios.

4.1.1.6 Lesson Learned

Identifying and clearly defining scenario objectives is a critical aspect of any risk analysis. We should ensure that this process is completed for each and every analysis and not bypassed or haphazardly completed for the sake of efficiency. As you will see when we start evaluating the factors related to Loss Event Frequency (LEF) and Loss Magnitude (LM), we will be referring to each of these identified components when making estimations.

4.1.2 Stage 2: Evaluate Loss Event Frequency (LEF)

4.1.2.1 Top-Down Approach

When we look at the Loss Event Frequency (LEF) side of the taxonomy (pictured below) we see a "tree" structure of lower-level factors driving the elements above. This is a correct interpretation of how the taxonomy functions. Unfortunately, as a result of this structure, practitioners often assume they should start deriving LEF by working at the lowest level of abstraction (i.e., Contact Frequency (CF) and Probability of Action (PoA)). It is important to remember that analyses can be performed at higher layers of abstraction. Note that the notion of "diminishing returns" often applies here; i.e., the output from deep analysis is not always a significant improvement over analyses performed at higher levels of abstraction in the taxonomy.

To leverage the top-down approach we should first consider whether we are able to make defensible estimations at the LEF itself. A question we may ask is: “Has this event happened in the last few years. If so, how many times?” If the loss event we are measuring has occurred in the recent past then we may be able to put our estimations directly at the LEF. For example, if we are attempting to estimate how often storms knock out power to our building; we likely have very objective historical information over the past five to ten years showing the frequency of such events. By leveraging this data we can make LEF estimations directly.

Now, if we don’t have data on past loss events, or if factors (such as controls) have changed, we should step down one layer and attempt to work at Threat Event Frequency (TEF) and Vulnerability (Vuln). Another additional consideration around which level of abstraction we should work at is based on the purpose of the analysis. For instance, if we are evaluating several different control options and are looking to identify which option is most effective from a risk reduction perspective, then deriving Vuln by analyzing Resistance Strength (RS) and Threat Capability (TCap) may be most appropriate.

To recap: the appropriate level of abstraction to use in an analysis will usually be determined by:

- The purpose of the analysis. If the analysis will be performed multiple times to assist in determining the effectiveness of a new control, then we should work at a lower level (e.g., RS) where the change can be more objectively and accurately estimated.

- The type and quality of data at hand and/or the amount of time available to the analyst – deeper levels of analysis take longer.

The benefit of working higher in the taxonomy is increased efficiency, and when there is data it often is more objective in nature.

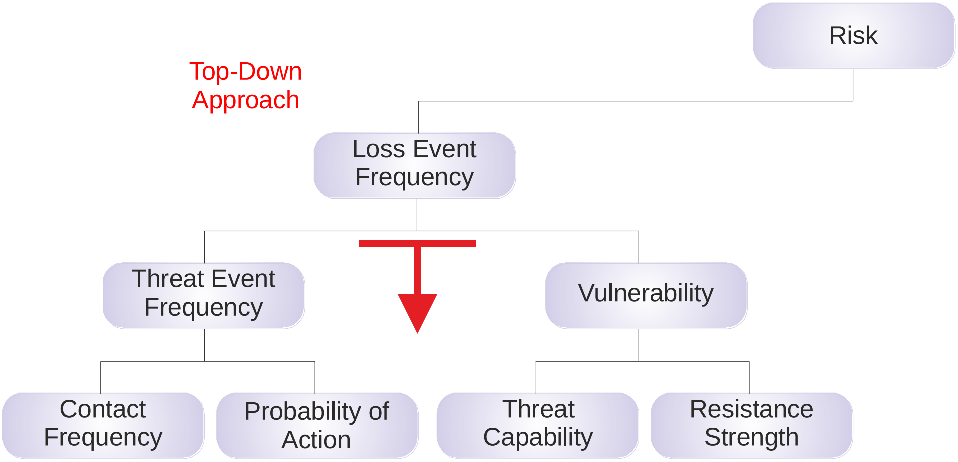


Figure 1: Top-Down Approach

4.1.2.2 *Estimate the Loss Event Frequency (LEF)*

A Loss Event Frequency (LEF) estimate would be based upon how frequently the loss event has or can be estimated to occur within a given timeframe. As mentioned above, estimating the LEF is straightforward if the loss event for the scenario we are measuring has occurred multiple times in the past.

Recognizing that the risk landscape is dynamic and threats as well as organizational controls may change, we should be mindful when using historical event data to estimate LEF directly. For example, if the organization has implemented several new controls as a result of an event in the past, these new controls may impact either the Threat Event Frequency (TEF) or Vulnerability (Vuln) of the organization to the threat. If this is the case, it may be more comfortable to make estimates at lower levels of the taxonomy.

4.1.2.3 Estimate the Threat Event Frequency (TEF)

Some people demand reams of hard data before they are comfortable with estimating attack frequency. Unfortunately, because we don't have much (if any) really useful or credible data for many scenarios, TEF is often ignored altogether. The minute we ignore this component of risk, however, we are no longer talking about risk. So, in the absence of hard data, what's left? One answer is to use a qualitative scale, such as Low, Medium, or High. And, while there's nothing inherently wrong with a qualitative approach in many circumstances, a quantitative approach provides better clarity and is more useful to most decision-makers – *even if it's imprecise*. For example, years of empirical data may not exist to document how frequently cleaning crew employees abuse usernames and passwords on sticky-notes, but a reasonable estimate can be made within a set of ranges.

A TEF estimate would be based upon how frequently contact between this threat community (the cleaning crew) and the credentials occurs *and* the probability that they would act against the credentials. If the cleaning crew comes by once per workday, contact reasonably occurs a couple of hundred times per year. The probability that they would act is driven by three primary factors:

- The value of the asset to them (based upon their motives – financial gain, revenge, etc.)
- How vulnerable the asset appears to be …
- *versus* the risk of being caught and suffering unacceptable consequences

Recognizing 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, then it seems reasonable to estimate a Low TEF (perhaps between 0.1 and 1 times per year).

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)

Is it possible for a cleaning crew to have 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? Absolutely! Does it happen? Undoubtedly. Might such a person be on the crew that cleans this office? Sure – it's possible. Nonetheless, the probable frequency is relatively low.

When making estimates of variables like this, it is important to identify factors that may play a role in supporting or contradicting your estimates. Using our example scenario, perhaps the cleaning crew is escorted through their rounds by a member of the physical security team or the premises are well covered by CCTV. Perhaps they're bonded and undergo thorough background checks. Or perhaps they've been with the company for years. None of these are guarantees, of course, but they are relevant considerations that affect the likelihood of misbehavior.

4.1.2.4 *Estimate the Threat Capability (TCap)*

Threat Capability (TCap) refers to the threat agent's skill (knowledge and experience) and resources (time and materials) that can be brought to bear against the asset. A different scenario might provide a better illustration of this component of the analysis – something like a web application with an SQL injection weakness – but scenarios like that don't lend themselves to an introductory document. In this case, all we're talking about is estimating 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. It's reasonable to rate the cleaning crew TCap as Medium (meaning average skill and resources), as compared to the overall threat population. Keep in mind that TCap is always estimated relative to the scenario. If our scenario was different, and we were evaluating the cleaning crew's capability to execute an SQL injection attack, we'd probably rate them lower (perhaps within the bottom 16% when compared against 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

4.1.2.5 *Estimate Resistance Strength (RS)*

Resistance Strength (RS) has to do with an asset's ability to resist compromise. In our scenario, because the credentials are in plain sight and in plain text, the RS is Very Low. This would mean we are likely protected from only the bottom 2% of an average threat population. If they were written down, but encrypted, the RS would be different – probably much higher (perhaps resistant to all but the top 2% of the threat population).

The question sometimes comes up: "Aren't good hiring practices a control for internal assets?" and "Isn't the lock on the executive's door a control?" Absolutely, they are. But these controls factor into the frequency of contact, as opposed to how effective the controls are at the point of attack. RS is commonly associated with preventative-type controls, a topic further discussed later within this Standard (Chapter 5).

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

4.1.2.6 *Derive Vulnerability (Vuln)*

Deriving Vulnerability (Vuln) is easy once you have established your TCap and RS. Recall from Section 3.8 that Vulnerability is the difference between the force that's likely to be applied, and the asset's ability to resist that force. If and where they intersect determines the level of vulnerability.

If we looked at this within a table, it could be represented as the table below:

Vulnerability (Vuln)

	VH	VH	VH	VH	H	M
	H	VH	VH	H	M	L
Threat Capability (TCap)	**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)

4.1.2.7 *Derive Loss Event Frequency (LEF)*

In our scenario, given a TEF of Low and Vulnerability of Very High, the LEF would likely be Low. Keep in mind that Vulnerability is a percentage, which means that you can never be more than 100% vulnerable. Consequently, the LEF will never be greater than the TEF.

If we looked at this within a table, it could be represented as the table below:

Loss Event Frequency (LEF)

Threat Event Frequency (TEF)	**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)

4.1.3 Stage 3: Evaluate Loss Magnitude (LM)

Using the previous steps, we have determined that the probability of a loss event in our scenario is Low (somewhere between 0.1 and 1 times per year). Now we're faced with analyzing loss if an event does occur.

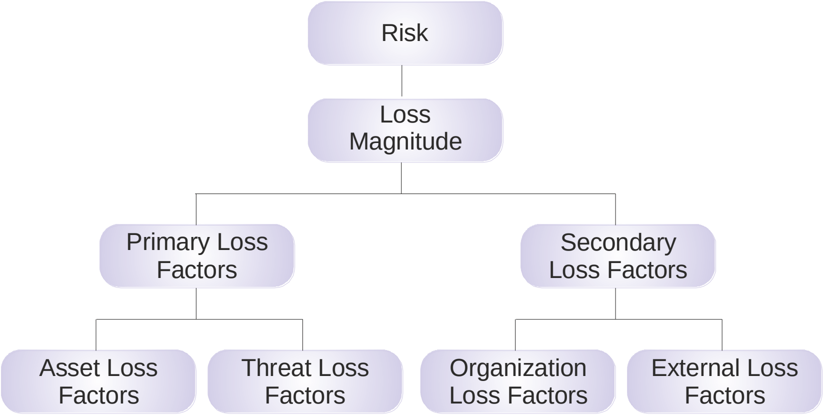


Figure 2: Loss Magnitude (LM)

As mentioned earlier, we can reasonably expect these credentials to provide access to HR organizational information (organization charts, etc.), as well as employee personal and employment information (performance data, health and medical data, address, SSN, salary, etc.). For our scenario, we'll assume that the asset we are most concerned about is personal employee information.

Remember that, in determining Loss Magnitude (LM), FAIR uses an approach of differentiating Primary and Secondary Loss. For more details on each of these forms of loss and clearly distinguishing the differences between them, please refer to the Risk Taxonomy Standard.

Further note that deriving LM using PERT distributions as input and Monte Carlo as a computational engine will provide the most effective and accurate measure of LM.

4.1.3.1 Estimate Primary Loss

Within this scenario, three potential threat actions stand out as having relevant loss potential, as follows:

- **Misuse** – employee records typically have information that can be used to execute identity theft, which introduces potential legal and reputation loss.
- **Disclosure** – employee records often have sensitive personal information related to medical or performance issues, which may introduce legal and reputation exposure.
- **Deny access (destruction)** – employee records are a necessary part of operating any business. Consequently, their destruction can introduce some degree of lost productivity.

We'll focus on Misuse (e.g., identity theft) in this analysis given that it's a common concern for scenarios such as this. In some cases it may be necessary to evaluate the loss associated with more than one threat action in order to decide which one has the most significant loss potential. This is often possible within the same analysis when performed quantitatively.

A key assumption in the LM portion of this analysis is that the volume of compromised employee information would be 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 breeches of customer records, which can number in the millions. Of course, 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 rationale that supports their foundational assumptions. When using the qualitative values such as in this example, it sometimes makes sense to perform multiple analyses (e.g., one for best-case, another for most likely, and a third for worst-case). If the analysis is being performed using PERT distributions and Monte Carlo, instead of the matrices used in this document, all three cases can be covered at once.

Our next step is to estimate the Primary Loss magnitude for Misuse.

Loss Forms					
Productivity	Response	Replacement	Fine/ Judgments	Comp. Adv.	Reputation
L	M	—	—	—	—

The scale below represents one possible set of ranges to characterize LM. The ranges within scales like this will need to reflect the loss capacity and tolerances of the organization.

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

Note that we didn't estimate LM for Replacement, Fines & Judgments, Competitive Advantage, or Reputation. Given the definitions for Primary and Secondary Loss, as well as the individual definitions for each of these loss forms, some of these loss forms may be relevant for Secondary Loss (covered shortly) in this scenario. However, those forms of loss should not materialize directly as a result of the event and thus would not be accounted for in Primary Loss.

Our estimates for Primary Loss in this scenario are 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.
- **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.

Note that the rationale above 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. If the analyst wants to evaluate the worst-case proposition, they can do so. In doing so, however, it is critical that they also reflect the (generally) much lower frequency of such an outcome. As mentioned elsewhere, PERT distributions and Monte Carlo provide greater flexibility and analytic power, particularly with regard to capturing the high and low ends of the possible outcomes.

Another useful tip in determining which forms of Primary Loss (e.g., productivity, response, replacement, etc.) may be applicable is by leading discussions with individuals within the organization that typically respond to or manage negative events. This is especially important for loss events that may have not occurred in the past. These discussions around the types of organizational involvement and loss when a given loss event materializes help to ensure that all forms of loss are evaluated and estimates are accurate. It is rare that the risk analyst is sufficiently informed to understand all applicable primary and secondary forms of loss, let alone their magnitude.

4.1.3.2 Evaluate Secondary Loss

The first step in evaluating Secondary Loss is to identify which, if any, secondary stakeholders would be relevant to the scenario. In other words, identify who, outside of the organization, might react negatively in a manner that would generate additional loss. For a financial institution, the most common secondary stakeholders of interest are customers, regulators, and shareholders.

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 they react will likely be a function of their perception of the existing overall control environment. If you were doing this analysis at a real organization, you would know (or could find out) what the regulatory view of the organization was, which would help you to accurately estimate this source of loss.

Since customer information is not involved in this scenario, we could reasonably assume 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 risk scenarios will not treat employees as secondary stakeholders, this is an exception. The affected employees could potentially leave the organization and/or file lawsuits, so it is reasonable to treat them as secondary stakeholders.

4.1.3.3 Estimate Secondary Loss Event Frequency (SLEF)

Once we have established which secondary stakeholders are relevant, we need to estimate the likelihood that they would be engaged, potentially generating various forms of Secondary Loss.

We can use the scale below to select the probability of secondary stakeholder engagement:

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%

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, we would rate the probability of secondary involvement as Very High.

To derive an actual frequency from that probability estimate, we reference the probability estimate against the primary Loss Event Frequency (LEF) value determined earlier in the analysis:

Secondary Loss Event Frequency (SLEF)

Primary Loss Event Frequency (LEF)						
	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 Probability

4.1.3.4 *Estimate Secondary Loss Magnitude (SLM)*

The next step is to estimate the most likely LM resulting from Misuse for each loss form. This is where assumptions regarding the volume of compromised sensitive information become critical. For this analysis we will assume 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. We could choose to make a different assumption (e.g., a smaller event) if we wanted to but, as with any key assumption in an analysis, we would need to support it with defensible rationale or data.

Loss Forms					
Productivity	Response	Replacement	Fine/ Judgments	Comp. Adv.	Reputation
—	M	—	L	—	—

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

Our rationale for these estimates includes:

- **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/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 moderate (if any at all).

No productivity loss occurred 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 that 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.

Once again it is important to re-iterate that the risk analyst should seek these estimations through discussions within subject-matter experts within the organization. The analyst should strive for having an analysis that is accurate and defensible. By gathering the insight into forms of loss from subject-matter experts, the quality of the overall analysis greatly increases.

4.1.4 Stage 4: Derive and Articulate Risk

Because we separately evaluated Primary and Secondary Loss Event Frequency (LEF) and Loss Magnitude (LM), we have to derive Primary and Secondary Risk, and then derive Overall Risk as a combination of the two.

4.1.4.1 Derive Primary Risk

We have already done the hard part, as risk is simply derived from the LEF and probable LM.

Assuming that the scale below has been "approved" by the leadership of our fictional bank, we can determine that Primary Risk associated with this scenario is Medium based upon a low LEF (between 0.1 and 1 times per year) and a moderate probable LM (between $10K and $100K).

Primary Risk

Primary 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**

Primary Loss Event Frequency (LEF)

4.1.4.2 Derive Secondary Risk

The process for deriving Secondary Risk is identical to Primary Risk, except that we will use the Secondary Loss Event Frequency (Low) and Secondary Loss Magnitude (Moderate) values.

Secondary Risk

Secondary 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 Event Frequency (SLEF)

4.1.4.3 Derive Overall Risk

The last step is to combine Primary and Secondary Risk into an Overall Risk value using the matrix below.

Overall Risk

	VH	VH	VH	VH	VH	VH
	H	H	H	H	H	VH
Secondary Risk	**M**	M	M	M	H	VH
	L	L	L	M	H	VH
	VL	VL	L	M	H	VH
		VL	**L**	**M**	**H**	**VH**

Primary Risk

A couple of important points to note:

- Cells in the matrix that intersect similar levels of risk (e.g., High Primary Risk and High Secondary Risk) could be shown as the next higher level of risk. In other words, the cell that intersects High risk 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 risk tolerance.

- Qualitative statements of risk (e.g., "High", "Medium", etc.) should reflect the loss capacity and subjective risk tolerance of the organization. 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.

Magnitude	Range Low End	Range High End
Severe (SV)	$10,000,000	–
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

In a real analysis, we may choose to evaluate and report on more than one threat community or more than one type of "loss event". However, sometimes by starting to assess the most probable and perceived significant scenario, that single scenario may provide enough information to lead to a well-informed decision. Basically, an analyst shouldn't assume they need to measure every possible scenario in order to support a well-informed decision.

4.2 Additional Risk Analysis Information

4.2.1 Documenting Rationale

When performing an analysis (especially a quantitative-based analysis), the estimates we enter are often only as good as the rationale documented along with them. When performing a risk analysis, we should anticipate that aspects of it might be challenged, especially from stakeholders who have other assumptions or biases. The rationale needs to clearly and concisely define, and must support, any estimates we have entered.

Well documented rationale should state the source of all estimates. The source may be systems (e.g., logs), groups (e.g., incident response), or industry data.

Remember, good sources of data are ones which are more objective in nature than subjective. This means data which has been observed is often more defensible and credible than data which is opinion-based. While any analyst would prefer objective-based estimates, sometimes we just don’t have very good data. When a situation like this arises, it is not the time to try and “hide” it by poorly documenting the rationale. As credible analysts, we should do just the opposite.

4.2.2 Risk Qualifiers

Sometimes, quantitative results don’t communicate everything that may be necessary in order for well-informed decisions to be made. Within the FAIR framework, two qualifiers have been identified that can help decision-makers understand subtle considerations that are not reflected in numeric data.

The Fragile qualifier is used to represent conditions where LEF is low in spite of a high TEF, but only because a single preventative control exists. In other words, the level of risk is fragile based on a single point of failure. For example, if a single control was all that kept malware-related losses low, then that could be said to be a fragile condition.

The Unstable qualifier is used to represent conditions where LEF is low solely because TEF is low. In other words, no preventative controls exist to manage the frequency of loss events. An example might be the risk associated with rogue database administrators. For most organizations, this is a low LEF condition but only because it is an inherently low TEF scenario.

These qualifiers are intended to compensate for the fact that in some scenarios if a decision-maker only looked at the low LEF, they may be lulled into a sense of security that is not warranted.

4.2.3 Capacity and Tolerance for Loss

An organization’s capacity for loss can be interpreted as an objective measure of how much damage it can incur and still remain solvent. For many organizations, this is a function of its capital reserves and other tangible resources, as well as its position in the market. For example, an organization with a stockpile of resources has a greater capacity to absorb disruption in its supply line than one that operates on a razor’s edge regarding resource availability.

An organization’s tolerance for loss can be interpreted as its leadership’s subjective tolerance for loss. Although there often is a strong correlation between objective capacity for loss and subjective loss tolerance, there can be significant differences if executive management is personally loss averse. For example, a financial institution may have substantial reserves and a resilient market presence and yet act as though it is highly averse to loss because executive management experienced a personally traumatizing loss in some past position with a different organization.

Ultimately, it is the combination of capacity for loss and tolerance for loss that determines how an organization perceives and responds to risk.

4.2.4 Translating Quantitative Results into Qualitative Statements

One of the advantages to quantitative risk analysis is that numbers are dispassionate and, by themselves, neutral to bias. Of course, there are instances in which decision-makers don't want to take the time to personally interpret the significance of quantitative results, and just want a simple red, yellow, or green label to look at. Fortunately, it can be relatively simple to convert numeric values to qualitative statements. The caveat is that these translations should be guided by scales that have been approved by management. It is inappropriate for risk analysts to define and use qualitative scales that represent their risk tolerance or their personal interpretation of what they believe the organization's risk tolerance to be. The challenge, of course, is that management may not be readily available to formally define risk scales. In this circumstance, the analyst may define a scale they believe is accurate for the organization and then have the scale reviewed by management for approval.

An example scale is shown below:

Label	**Average Annualized Loss Exposure**
Severe (SV)	> $10,000,000
High (H)	$1,000,000 to $9,999,999
Moderate (M)	$100,000 to $999,999
Low (L)	$10,000 to $99,999
Very Low (VL)	< $10,000

If an analysis resulted in an average annualized loss exposure of $4.5M, that could be interpreted as High Risk based on this scale.

4.2.5 Troubleshooting

When analysts or stakeholders disagree on the results of or a component of an analysis, there are three recommended techniques to managing the disagreements.

The first technique is to revisit the scoping or rationale within an analysis and determine whether an assumption has been made which varies from the other analysts or stakeholders. If a difference is found, this is often easily resolved.

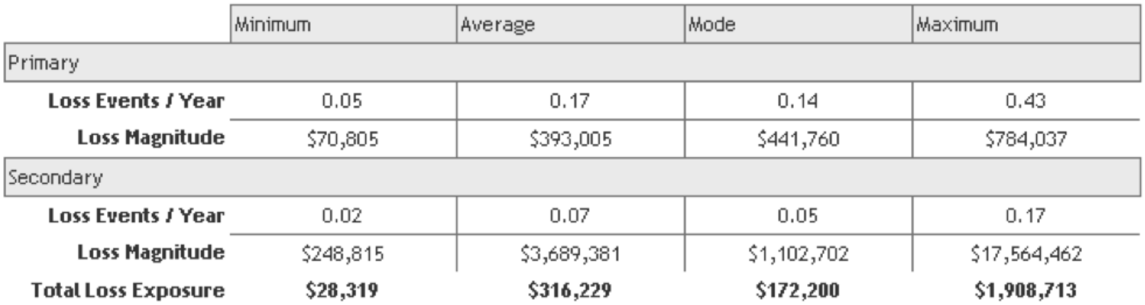
The second technique is to leverage the taxonomy. The taxonomy breaks down the factors that drive risk. For example, if a disagreement exists regarding estimates made at the Loss Event Frequency (LEF), step down to a lower level of abstraction. By stepping one level lower in abstraction both sides may once again find agreement and the higher estimate will now be derived.

The third recommended technique is to perform two or more analyses to encompass the disagreement. As an example, if one analyst believes the Threat Event Frequency (TEF) is at least once a year while a second analyst believes the TEF is less frequent, you can perform two analyses using both figures and observe whether there is a significant deviation in the overall results.

Often you will find that the majority of disagreements will be resolved after approaching the problem using the first two techniques.

4.2.6 Interpreting Results

The results of a fully quantitative FAIR risk assessment are often generated in tabular format. The table presents the summary statistics of the resultant distributions computed using Monte Carlo. An example of this output is presented below:



	Minimum	Average	Mode	Maximum
Primary				
Loss Events / Year	0.05	0.17	0.14	0.43
Loss Magnitude	$70,805	$393,005	$441,760	$784,037
Secondary				
Loss Events / Year	0.02	0.07	0.05	0.17
Loss Magnitude	$248,815	$3,689,381	$1,102,702	$17,564,462
Total Loss Exposure	**$28,319**	**$316,229**	**$172,200**	**$1,908,713**

This table shows the minimum, average, mode, and maximum risk values for both the primary and secondary loss and frequency factors. Interpreting this table would be done as follows:

Primary Loss Events/Year

The primary losses would occur as little as once in 20 years (0.05) and as much as 43 times in 100 years (0.43). The average frequency is as much as 17 times in 100 years (0.17), but the most likely (mode) value is 7 times in 50 years (0.14).

Primary Loss Magnitude

The primary losses, per event, would be as little as $70,805 (minimum) and as much as $784,037 (maximum). The average losses are $393,005, but the most likely losses (mode) are $441,760.

The secondary loss events/year and loss magnitude are interpreted in the same fashion as the primary factors.

The Total Loss Exposure is the total computed risk that is experienced on an annual basis (if a risk is not shown to be occurring at least once per year). This means that the amount of a single loss event is spread over the years leading up to it. Risk scenarios with loss events occurring once or multiple times per year show the sum of the annual loss events.

Practical advice for communicating FAIR results is to focus on most likely and maximum values, and generously round off the results to whole numbers. For instance, the above table could be interpreted as about $175,000 of annualized loss occurring about once every 7 years (it helps to convert the decimals back into fractions to express the frequency values).

Note that it can also be useful in many instances to communicate both the annualized loss exposure (e.g., $172k average) and the single event loss magnitude (e.g., $1.1M average) to help executives get a clear picture of the risk.

5 Basic Control Considerations in FAIR Risk Analysis

This chapter provides guidance on how to evaluate the effect of controls within the context of the Risk Taxonomy. It is important to keep in mind that all controls are intended to affect either or both the frequency and magnitude of loss, thus a workable definition of control is *any person, policy, process, or technology that has the potential to reduce the frequency and/or magnitude of loss*. Understanding where a control's effect may be realized within the taxonomy is critical in order to accurately account for a control within an analysis.

5.1 Control Categories

At a basic level, there are four ways in which controls can affect risk:

3. **Avoidance Controls** affect the frequency and/or likelihood of encountering threats.
4. **Deterrent Controls** affect the likelihood of a threat acting in a manner that can result in harm.
5. **Vulnerability Controls** affect the probability that a threat's action will result in loss.
6. **Responsive Controls** affect the amount of loss that result from a threat's action.

The question may arise about why detective controls aren't explicitly accounted for. The reasoning is that detective controls can play a role in each of the categories listed above and thus isn't a distinct control category itself. For example, system logging and monitoring can in some circumstances be a deterrent by increasing a potential threat's perception of the likelihood of being caught. At the same time, logging and monitoring can inform an organization that an event is underway, allowing it to intervene before loss materializes. Even if intervention isn't timely enough to prevent loss from occurring, early detection can allow an organization to respond quickly enough to minimize the magnitude of loss.

Figure 3 identifies where these control categories play a role within the taxonomy.

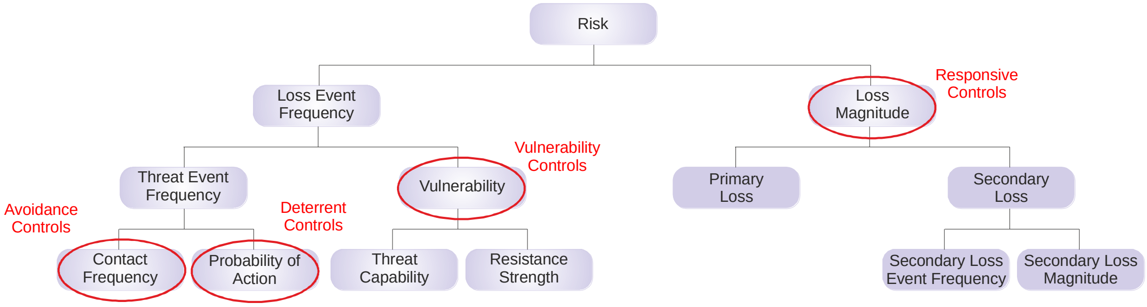


Figure 3: Control Categories

5.2 Avoidance Controls

As stated above, avoidance controls affect the frequency and/or likelihood that a threat will come into contact with an asset. Logically then, if Contact Frequency (CF) is reduced, this reduction will also translate into a lower Threat Event Frequency (TEF), Loss Event Frequency (LEF), and exposure to risk. Examples of information security-related avoidance controls include:

- Firewall filters
- Physical barriers
- The relocation of assets
- The reduction of threat populations (e.g., reducing the number of personnel who are given legitimate access to assets)

As with any control, the effect may not be absolute. For example, firewalls usually are configured to permit certain types of traffic, which means that threat events may still occur against assets behind the firewall. Nonetheless, firewalls also almost invariably reduce the frequency of threat events by shielding against certain types of traffic.

When considering the effect of avoidance controls in an analysis, simply measure or estimate the reduction in CF specific to the threat community under consideration.

5.3 Deterrent Controls

Deterrent controls reduce the probability that a threat agent will act against the asset in a manner that may result in loss. As with avoidance controls, this effect flows up the taxonomy to affect Threat Event Frequency (TEF), Loss Event Frequency (LEF), and exposure to risk. Examples of common information security-related deterrent controls include:

- Policies
- Logging and monitoring
- Enforcement practices
- Asset "hardening" (e.g., many threat actors are opportunistic in nature and will gravitate toward easier targets, rather than targets that are perceived to be difficult)
- Physical obstacles (e.g., external lights on building, barb-wire fencing, etc.)

Measuring the effect of deterrent controls is often challenging. Nonetheless, reasonable estimates can be made (using calibrated methods discussed elsewhere in this document) to reflect their value.

5.4 Vulnerability Controls

Vulnerability controls reduce the probability that a threat's action will result in loss. In a scenario where the context is a malicious action, vulnerability controls generally focus on increasing the difficulty a threat actor faces in their attempts to gain access, disrupt, etc. In a scenario where the context is non-malicious (e.g., human error), vulnerability controls often focus on reducing complexity and/or difficulty faced by personnel to reduce the probability that their actions will result in harm.

Note: Vulnerability controls are sometimes referred to as "resistive controls", but this term tends to exclusively connote controls against malicious acts.

Examples of vulnerability controls in an information security context would include:

- Authentication
- Access privileges
- Patching
- Some configuration settings

Note that response time can affect vulnerability. For example, if personnel monitoring a CCTV system identified that someone was attempting to pick the lock on a door, and the personnel were able to intervene before the door was successfully breached, then that would be an example of reduced vulnerability due to detection and response capabilities.

Measurements and estimates for vulnerability controls may be applied to the Resistance Strength (RS) variable or at the Vulnerability (Vuln) variable, depending on what level of abstraction the analysis is being performed at.

5.5 Response Controls

In the context of this discussion, response controls refer to those controls that occur after a loss event has been detected and that are focused on reducing the magnitude of loss that results. Examples of response controls in an information security context include:

- Back-up and restore media and processes
- Forensics capabilities
- Incident response processes
- Credit monitoring for persons whose private information has been compromised

Measurements and estimates regarding the effect of response controls are applied in the Loss Magnitude (LM) branch of the taxonomy, and are reflected as lower monetary LMs.

In closing, it is important to understand what relation different types of controls have to the Risk Taxonomy. During the estimation of different taxonomy factors in an analysis, it is important to evaluate all applicable controls and their overall effectiveness. Data on this is often available by reviewing the following:

- Audits (Technical and Regulatory) – Audits that evaluate the effectiveness of controls can provide useful information about the current state and possibly an indication of the continued state of controls.
- Penetration Tests/Security Scans – These exercises can provide useful knowledge of where controls are present and how effective they may be in preventing a threat action from materializing into a loss. Some penetration tests also provide good insight into the overall responsiveness of the organization (with regard to identifying threat actions).

A Business Case

A.1 Risk Management Decision-Making

Risk management is fundamentally about making decisions – decisions about which risk issues are most critical (prioritization), which risk issues are not worth worrying about (risk acceptance), and how much to spend on the risk issues that need to be dealt with (budgeting). In order to be consistently effective in making these decisions, we need to be able to compare the issues themselves, as well as the options and solutions that are available. In order to compare, we need to measure, and measurement is predicated upon a solid definition of the things to be measured. Figure 4 shows these chained dependencies.

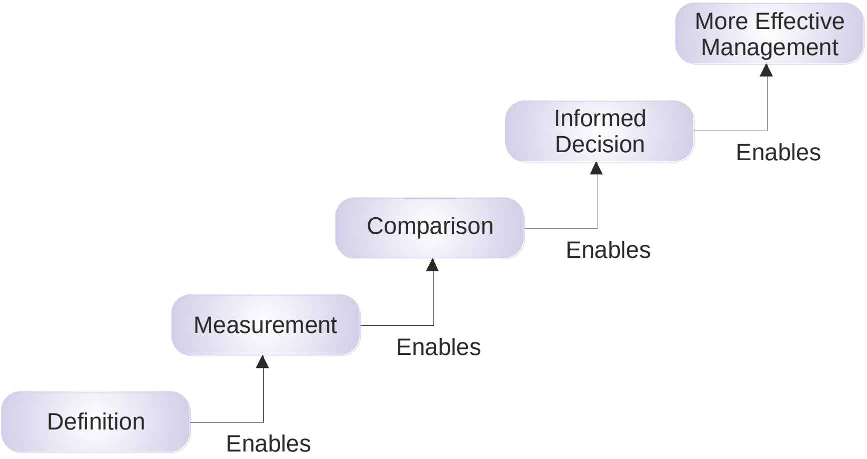


Figure 4: Chained Dependencies

To date, the information security profession has been hamstrung by several challenges, not the least of which is inconsistent nomenclature. For example, in some references, software flaws/faults that could be exploited will be called a "threat", while in other references these same software faults will be referred to as a "risk", and yet other references will refer to them as "vulnerabilities". Besides the confusion that can result, this inconsistency makes it difficult if not impossible to normalize data and develop good metrics.

A related challenge stems from mathematical equations for risk that are either incomplete or illogical. For example, one commonly cited equation for risk states that:

*Risk = (Threat * Vulnerability) / Controls*

Amongst other problems, this equation doesn't tell us whether *Threat* means the level of force being applied or the frequency with which threat events occur. Furthermore, impact (magnitude of loss) is left out of the equation altogether. As we will touch on shortly, organization management cares very deeply about the question of Loss Magnitude (LM), and so any risk equation that ignores impact is going to be meaningless to the very people who need to use risk analyses to make risk decisions.

These issues have been a major contributor to why the information security profession has consistently been challenged to find and maintain "a seat at the table" with the other organizational functions (e.g., finance, marketing, etc.). Furthermore, while few people are likely to become excited with the prospect of yet another set of definitions amongst the many that already exist, the capabilities that result from a well-designed foundational taxonomy are significant.

Likewise, in order for our profession to evolve significantly, it is imperative that we operate with a common, logical, and effective understanding of our fundamental problem space. The Risk Taxonomy Standard seeks to fill the current void and set the stage for the security profession's maturation and growth.

Note: Any attempt to describe the natural world is destined to be incomplete and imprecise to some degree due to the simple fact that human understanding of the world is, and always will be, limited. Furthermore, the act of breaking down and categorizing a complex problem requires that black and white lines be drawn where, in reality, the world tends to be shades of gray. Nonetheless, this is exactly what human-critical analysis methods and science have done for millennia, resulting in a vastly improved ability to understand the world around us, evolve, and accomplish objectives previously believed to be unattainable.

This Standard is a current effort at providing the foundational understanding that is necessary for similar evolution and accomplishment in managing information risk. Without this foundation, our profession will continue to rely too heavily on practitioner intuition which, although critically important, is often strongly affected by bias, myth, and commercial or personal agenda.

Glossary

Action

An act taken against an asset by a threat agent. Requires first that contact occurs between the asset and threat agent.

Asset

Anything that may be affected in a manner whereby its value is diminished or the act introduces liability to the owner. Examples include systems, data, people, facilities, cash, etc.

Broad Spectrum Risk Analysis

Any analysis that accounts for the risk from multiple threat communities against a single asset.

Contact

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) and/or Loss Magnitude (LM).

Control Strength (CS)

The strength of a control as compared to a standard measure of force.

FAIR

Factor Analysis of Information Risk

Loss Event

Occurs when a threat agent's action (threat event) is successful in negatively affecting an asset.

Loss Event Frequency (LEF)

The probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.

Loss Magnitude (LM)

The probable magnitude of loss resulting from a loss event.

Multi-level Risk Analysis

Any analysis that accounts for the risk from a single threat community against a layered set of assets (e.g., defense in depth).

Primary Stakeholder

The person or organization that owns the asset at risk. For example, The Open Group would be the primary stakeholder in risk scenarios related to its assets.

Probability of Action (PoA)

The probability that a threat agent will act against an asset once contact occurs.

Probable Loss Magnitude (PLM)

The probable magnitude of loss resulting from a loss event.

Resistance Strength (RS)

The strength of a control as compared to a standard measure of force.

Risk

The probable frequency and probable magnitude of future loss.

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, etc.) that is capable of acting against an asset in a manner that can result in harm.

Threat Capability (TCap)

The probable level of force 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 an asset will be unable to resist the actions of a threat agent.

Index