*Open Group Standard*

# Risk Taxonomy (O-RT), Version 2.0

Technical Standard

**Risk Taxonomy (O-RT), Version 2.0**

ISBN: 1-937218-42-3

Document Number: C13K

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

1 Introduction ........ 11

1.1 Objective ........ 11

1.2 Overview ........ 11

1.3 Conformance ........ 13

1.4 Normative References ........ 13

1.5 Terminology ........ 13

1.6 Future Directions ........ 14

2 Risk Management Model ........ 15

2.1 Risk Assessment Approach ........ 15

2.2 Why is a Tightly-Defined Taxonomy Critical? ........ 15

3 Technical Requirements ........ 17

3.1 Risk Taxonomy Overview ........ 17

3.2 Risk ........ 17

3.3 Loss Event Frequency (LEF) ........ 18

3.4 Threat Event Frequency (TEF) ........ 18

3.4.1 Contact Frequency (CF) ........ 19

3.4.2 Probability of Action (PoA) ........ 20

3.4.3 Vulnerability (Vuln) ........ 20

3.4.4 Threat Capability (TCap) ........ 21

3.4.5 Resistance Strength (RS) ........ 21

3.5 Loss Magnitude (LM) ........ 22

3.5.1 Forms of Loss ........ 23

3.5.2 Loss Flow ........ 24

3.5.3 Loss Factors ........ 25

4 Example Application (Informative) ........ 31

4.1 The Scenario ........ 31

4.2 The Analysis: FAIR Basic Risk Assessment Methodology ........ 31

4.2.1 Stage 1: Scope the Analysis ........ 32

4.2.2 Stage 2: Evaluate Loss Event Frequency (LEF) ........ 33

4.2.3 Stage 3: Evaluate Loss Magnitude (LM) ........ 36

4.2.4 Stage 4: Derive and Articulate Risk ........ 41

A Business Case ........ 44

A.1 Risk Management Decision-Making ........ 44

A.2 What Makes this the Standard of Choice? ........ 45

A.3 Who Should Use It? ........ 46

A.4 Related Dependencies ........ 47

B Risk Taxonomy Considerations ........ 48

B.1 Complexity of the Model ........ 48

B.2 Availability of Data ........ 49

B.3 Iterative Risk Analyses ........ 49

B.4 Perspective ........ 49

C Practical Use of FAIR ........ 50

C.1 The Risk Language Gap ........ 50

C.2 Key Risk Concepts ........ 51

C.3 Using FAIR with Other Risk Assessment Frameworks ........ 51

C.4 The Ability of a FAIR-Based Approach to Complement Other Standards ........ 51

C.5 An Example: Using FAIR with OCTAVE ........ 52

# 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 Taxonomy (O-RT), Version 2.0. It is an updated version of the Risk Taxonomy Standard (Doc. No. C081) that was published in January 2009.

This document provides a standard definition and taxonomy for information security risk, as well as information regarding how to use the taxonomy.

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 Taxonomy 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 Taxonomy Standard to be used as a foundation for normalizing the results of risk analyses across varied risk domains.

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

- **The Open Group Risk Analysis (O-RA) Technical Standard** (C13G, October 2013) provides a set of standards for various aspects of information security risk analysis.
- **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.

## Differences from the Original Version of the Standard

This document includes changes to the Risk Taxonomy Standard that have evolved since the original document was published. These changes came about as a result of feedback from practitioners using the Standard, as well as from continued research performed by CXOWARE.

Most of the changes are minor, representing refinements in terminology. For example, Control Strength (CS) is now referred to as Resistance Strength (RS). This change was made to more clearly emphasize that controls accounted for in that portion of the taxonomy must be resistive in nature (e.g., passwords). Other, non-resistive controls (e.g., logging, recovery processes) would be accounted for in other parts of the taxonomy.

More substantive changes were made to how loss magnitude is evaluated, which significantly improve the quality of loss estimates.

# 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 contribution of Alex Hutton and Jack Jones, Risk Management Insight, as well as CXOWARE, for their valued original work and their continued support in guiding the Security Forum members through our process to develop this Risk Taxonomy Standard.

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

# Referenced Documents

The following documents are referenced in this Standard:

- A Taxonomy of Computer Program Security Flaws, with Examples, Naval Research Laboratory, September 1994; refer to: http://chacs.nrl.navy.mil/publications.

- 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.

- Methods for the Identification of Emerging and Future Risks, European Network and Information Security Agency (ENISA), November 2007; refer to www.enisa.europa.eu/doc/pdf/deliverables/EFR_Methods_Identification_200804.pdf.

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), US-CERT; refer to www.cert.org/octave.

- 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 Analysis (O-RA), Open Group Standard, C13G, published by The Open Group, October 2013; refer to: www.opengroup.org/bookstore/catalog/c13g.htm.

# 1 Introduction

## 1.1 Objective

The objective of this 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 Standard 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 Standard 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 Standard 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 Standard does not address how to assess or analyze risk.[1] This Standard also does not cover those elements of risk management that pertain to strategic and tactical risk decisions and execution.

This Risk Taxonomy Standard 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 (CF), the analyst could move up a layer of abstraction and instead measure Threat Event Frequency (TEF). 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 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".

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 do 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 we use to describe it, we can't be effective in delivering meaningful, comparable risk assessment results. This Risk Taxonomy Standard 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] The Open Group has published a separate standard for performing FAIR-based risk analysis: the Risk Analysis Standard.

## 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 Taxonomy Standard:

- Risk Analysis (O-RA), Open Group Standard, C13G, published by The Open Group, October 2013; refer to: www.opengroup.org/bookstore/catalog/c13g.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

None.

# 2 Risk Management Model

## 2.1 Risk Assessment Approach

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

## 2.2 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 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.

This concept can be illustrated in what is referred to as a "risk management stack" showing the relationship between these elements.

Effective Management

↑

Well-informed Decisions

↑

Effective Comparisons

↑

Meaningful Measurements

↑

Accurate Risk Model

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.

# 3 Technical Requirements

## 3.1 Risk Taxonomy Overview

The complete Risk Taxonomy is comprised of two main branches: Loss Event Frequency (LEF) and Loss Magnitude (LM). Within those two branches are the factors that drive the occurrence and magnitude of losses. Figure 1 lays out the higher-level abstractions within the framework.

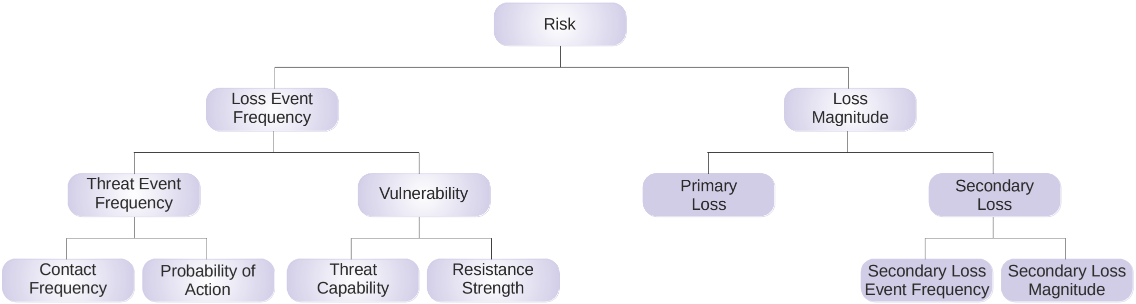

**Figure 1: High-Level Risk Taxonomy Abstractions**

Note that this diagram 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, but it is important to recognize that, theoretically, the layers of abstraction may continue indefinitely, much like the layers of abstraction that exist in our understanding of physical matter (e.g., molecules, atoms, particles, etc.). The deeper layers of abstraction can be useful in our understanding but generally aren't necessary in order to perform effective analyses.

Another point worth recognizing is that the factors within the LEF side of the taxonomy have relatively clean and clear cause-and-effect relationships with one another, which simplifies calculation. Factors within the LM side of the taxonomy, however, have much more complicated relationships that defy simple calculation. As a result, LM measurements and estimates generally are aggregated by loss type (e.g., $xxx of productivity loss, plus $yyy of legal fines and judgments, etc.).

## 3.2 Risk

Risk estimates the probable frequency and magnitude of future loss (also known as "loss exposure"). Thus, this Risk Taxonomy Standard focuses solely on pure risk (only resulting in loss) as opposed to speculative risk (which might generate either a loss or a profit).

With this as a starting point, the first two obvious components of risk are loss frequency and loss magnitude. In this Standard, these are referred to as Loss Event Frequency (LEF) and Loss Magnitude (LM), respectively.

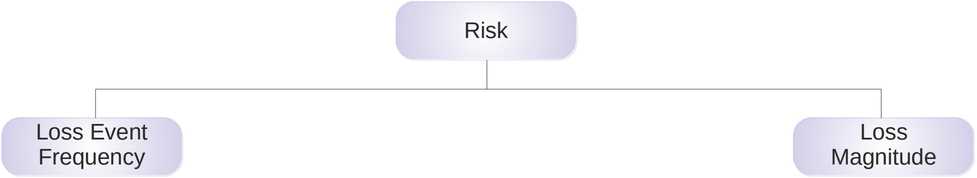

**Figure 2: Risk**

We will decompose the factors that drive LEF first, and then examine the factors that drive probable LM.

## 3.3 Loss Event Frequency (LEF)

Loss Event Frequency (LEF) is the probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.

In order for a loss event to occur, a threat agent has to act upon an asset, such that loss results. This leads us to our next two factors: Threat Event Frequency (TEF) and Vulnerability (Vuln).

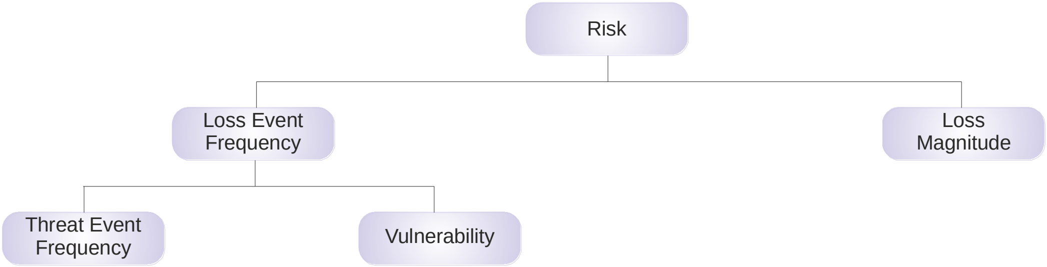

**Figure 3: Loss Event Frequency (LEF)**

Probability always is based on a timeframe (event X is 10% likely to occur over the next Y) because, given no time-framing, almost any event is possible.

## 3.4 Threat Event Frequency (TEF)

Threat Event Frequency (TEF) is the probable frequency, within a given timeframe, that a threat agent will act against an asset.

You will probably see the similarity between this definition and the definition for LEF above. The only difference is that the definition for TEF doesn’t include whether threat agent actions are successful. In other words, threat agents may act against assets, but be unsuccessful in affecting 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 include 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 cord became unplugged (or, depending on the scenario under analysis, if the person were injured).

This definition also provides us with the two factors that drive TEF: Contact Frequency (CF) and Probability of Action (PoA). Note that PoA is predicated upon contact. Figure 4 adds these two factors to our taxonomy.

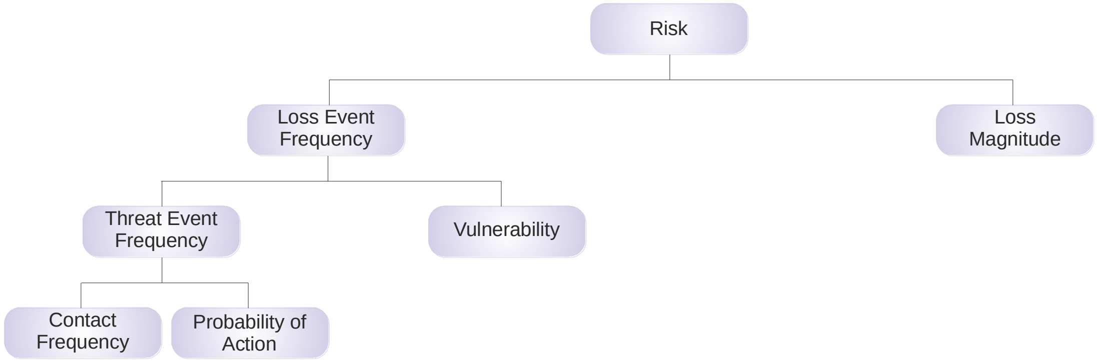

**Figure 4: Threat Event Frequency (TEF)**

### 3.4.1 Contact Frequency (CF)

Contact Frequency (CF) is the probable frequency, within a given timeframe, that a threat agent will come into contact with an asset.

Contact can be physical or "logical" (e.g., over the network). Regardless of contact mode, three types of contact can take place, as follows:

- **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 the cleaning crew regularly comes by at 5:15, 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.

### 3.4.2 Probability of Action (PoA)

Probability of Action (PoA) 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 we're talking about "thinking" threat agents such as humans and other animals, and artificially intelligent threat agents like malicious programs (which are extensions of their human creators).

The probability that an intentional act will take place is driven by three primary factors, as follows:

- **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.

### 3.4.3 Vulnerability (Vuln)

Having covered the high-level factors that drive whether threat events take place, we now turn our attention to the factors that drive whether the asset is able to resist threat agent actions.

Vulnerability (Vuln) is the probability that a threat event will become a loss event.

Vulnerability exists when there is a difference between the force being applied by the threat agent, and an object's ability to resist that force. This simple analysis provides us with the two primary factors that drive vulnerability: Threat Capability (TCap) and Resistance Strength (RS). Figure 5 adds these factors to our taxonomy.

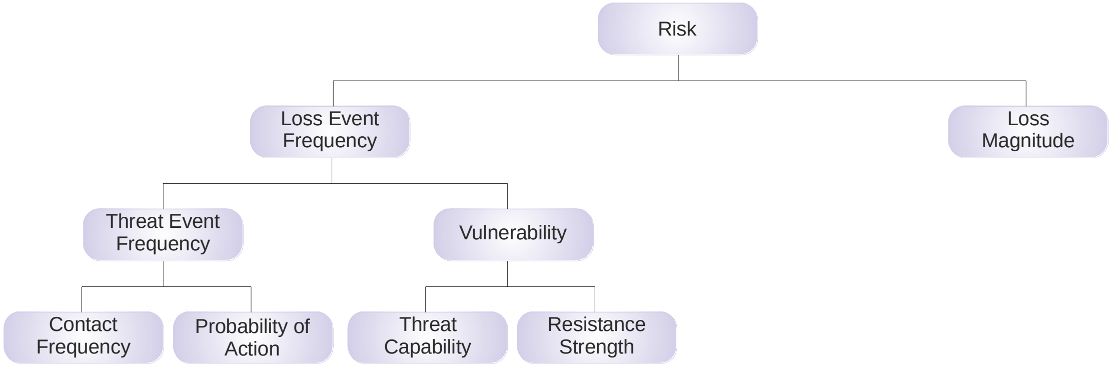

**Figure 5: Vulnerability**

Vulnerability is always relative to the type of force and vector involved. In other words, the tensile strength of a rope is pertinent only if the threat agent force is a weight applied along the length of the rope. Tensile strength doesn’t generally apply to a scenario where the threat agent is fire, chemical erosion, etc. Likewise, a computer anti-virus product doesn’t provide much in the way of protection from the internal employee seeking to perpetrate fraud. The key, then, is to evaluate vulnerability in the context of specific threat types and control types.

One final point regarding vulnerability: there’s no such thing as being more than 100% vulnerable to damage by any specific threat agent/attack vector combination. Vulnerability can exist such that harm can occur from more than one threat agent through more than one attack vector, but each of those represents a different potential threat event. For example, if I’m walking down the street at night in a particularly dangerous part of town, I’m 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 scenarios cannot exceed 100% (certainty) but the aggregate risk of loss is certainly greater due to the multiple threat scenarios that could occur.

### 3.4.4 Threat Capability (TCap)

Threat Capability (TCap) is the probable level of force that a threat agent is capable of applying against an asset.

Not all threat agents are created equal. In fact, threat agents within a single threat community are not all going to have the same capabilities. What this should tell us is that the probability of the most capable threat agent acting against an asset is something less than 100%. In fact, 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.

As information security professionals, we often struggle with the notion of considering threat agent capability as a probability. We tend, instead, to gravitate toward focusing on the worst case. But if we look closely at the issue, it is clear that focusing solely on worst case is to think in terms of possibility rather than probability.

Another important consideration is that some threat agents may be very proficient in applying one type of force, and incompetent at others. For example, a network engineer may be proficient at applying technological forms of attack, but may be relatively incapable of executing complex accounting fraud.

### 3.4.5 Resistance Strength (RS)

Resistance Strength (RS) is the strength of a control as compared to a baseline measure of force.

A rope’s tensile strength rating provides an indication of how much force it is capable of resisting. The baseline measure (RS) for this rating is pounds per square inch (PSI), which is determined by the rope’s design and construction. This RS rating doesn’t change when the rope is put to use. Regardless of whether you have a 10-pound weight on the end of the 500-PSI rope, or a 2000-pound weight, the RS doesn’t change.

Unfortunately, the information risk realm doesn’t have a baseline scale for force that is as well defined as PSI. Consider, however, password strength as a simple example of how we can approach this. We can 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 RS can be represented as this percentile. (Recall that RS is relative to a particular type of force – in this case, cracking.) Vulnerability is determined by comparing RS against the capability of the specific threat community under analysis. For example, password RS may be estimated at the 80th percentile, yet the threat community within a scenario might be estimated to have better than average capabilities – let's say in the 90th percentile range.

## 3.5 Loss Magnitude (LM)

Loss Magnitude (LM) is the probable magnitude of loss resulting from a loss event.

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.

Unfortunately, Loss Magnitude (LM) has tended to be one of the toughest nuts to crack in analyzing risk. As a result, loss has often been excluded from analyses, only the worst-case outcomes were cited, or calculations tried to be over-precise. Excluding LM from an analysis means that we are not analyzing risk (by definition, risk *always* has a loss component). Citing worst-case possibilities alone removes the probability element from our analysis (by definition, risk is a probability issue). Trying to be precise is generally a waste of time because of the inherent complexity within loss, and because decision-makers generally aren't expecting high degrees of precision. Management's experience with other forms of risk (investment, market, etc.) has taught them that actual losses can't be predicted with any precision.

Making matters even more difficult in the information risk environment is the fact that there has historically been limited data regarding LM. This is improving, but many organizations still don't perform loss analysis when events occur, and those that do track loss often limit their analyses to the "easy stuff" (e.g., person-hours, equipment replacement, etc.). Furthermore, without a standard taxonomy, it's very difficult to normalize the data across organizations.

Out of a population of information security incidents, you will generally have a loss distribution that looks something like Figure 6.

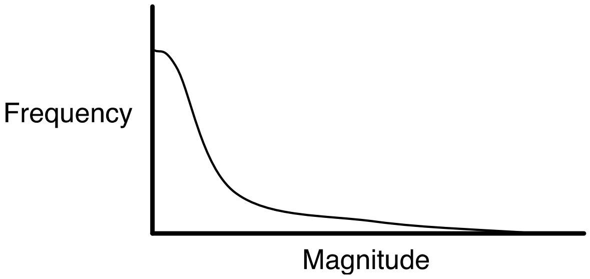

**Figure 6: Loss Magnitude (LM) [Source: The Open Group]**

In other words, there are far more events that result in loss at the low end of the magnitude spectrum than there are at the high end of the spectrum. For example, individual virus incidents, unauthorized use of systems to serve up MP3 files, even password cracking and loss of Personally Identifiable Information (PII)), rarely result in significant loss. The question we have to ask ourselves is: “Why?” What factors are responsible for this? Clearly some of these events have significant potential for harm, but if we compared the *actual* loss from two similar events – one in which minimal loss occurred, and another where substantial loss occurred – what factors determined the difference? In order for us to make well-reasoned, accurate estimates of loss, we have to understand how loss materializes.

### 3.5.1 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. That same information can also 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 Standard, as follows:

- **Productivity** – generally represents the reduction in an organization’s ability to generate its primary value proposition (e.g., income, goods, services, etc.). Note that this is the category where loss of revenue due to operational outages and discontinuation would be accounted for (e.g., revenue lost when a retail web site is unavailable due to a system outage). Productivity loss may also include sunk 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). Note that it can be important to distinguish lost revenue from delayed revenue. For example, when a retail web site goes down some proportion of its customers may wait to perform their transactions rather than use a different retailer. This, of course, is highly dependent on the nature of the market and competition. The sales and marketing departments in most organizations will have reliable data to inform these estimates.

- **Response** – expenses associated with managing a loss event (e.g., internal or external person-hours, logistical expenses, legal defense, public relations expenses, etc.).

- **Replacement** – the intrinsic value of an asset. Typically represented as the capital 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, etc.).

- **Fines and Judgments** – legal or regulatory actions levied against an organization. Note that this includes bail for any organization members who are arrested. Note that the costs associated with legal defense are captured in Response costs.

- **Competitive Advantage** – losses associated with diminished competitive position. Within this framework, competitive advantage loss is specifically associated with assets that provide competitive differentiation between the organization and its competition. Within the commercial world, examples would include trade secrets, merger and acquisition plans, etc. Outside the commercial world, examples would include military secrets, secret alliances, etc.

- **Reputation** – 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. From a practical perspective, reputation damage typically materializes as reduced market share (for commercial organizations), reduced stock price (for publically traded companies), reduced willingness to cooperate in joint ventures, or increased cost of capital. Note that this is where a reduction in revenue due to lost market share would be accounted for.

Keep in mind that loss is evaluated from a single perspective – typically that of the organization under analysis. For example, although customers might be harmed if their personal information is stolen, our risk analysis would evaluate the losses experienced by the organization rather than the losses experienced by the customers.

## 3.5.2 Loss Flow

The concept of loss flow is new to this issue of the Standard, and significantly improves the ability to evaluate LM accurately.

We refer to loss flow as a structured decomposition of how losses materialize when an event occurs. Loss flow incorporates the following:

- A threat agent acts against an asset.
- This event affects the primary stakeholder in terms of productivity loss, response costs, etc.. This is considered the primary component of the loss event.
- Sometimes this initial event also has an effect on secondary stakeholders, such as customers, regulators, media, etc.
- The reactions of the secondary stakeholders may, in turn, act as new threat agents against the organization's assets (such as reputation, legal fees, etc.) which, of course, affects the primary stakeholder. This is referred to as the secondary component of the loss event.

A few things to recognize:

- Secondary losses are always predicated upon a primary loss.
- We may call them "secondary stakeholders" but they are most accurately viewed as "secondary threats" when they begin acting against our assets.

### *3.5.2.1 Primary Loss*

From a loss flow perspective there are two phases in which loss materializes from an event. The first phase, 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 web site 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., Competitive Advantage loss occurring when the threat agent is a competitor, Fines and Judgments loss when the threat agent is filing charges/claims, etc.).

#### 3.5.2.2 *Secondary Loss*

The second phase, Secondary Loss, occurs as a result of secondary stakeholders (e.g., customers, stockholders, regulators, etc.) reacting negatively to the primary event. Think of it as “fallout” from the primary event. 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. Note that 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 percentage of time a scenario is expected to have secondary effects. Note that even though this variable is called a “frequency”, it actually is estimated as a percentage to reflect that it represents the percentage of primary events that have secondary effects.

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, etc.).

Of the six forms of loss, Response, Competitive Advantage, Fines & Judgments, and Reputation are most commonly associated with Secondary Loss. It is unusual to experience Productivity or Replacement loss within Secondary Loss.

Two important considerations of Secondary Loss are that:

- It is always predicated on a primary event.
- It does not materialize from every primary event.

Another important aspect of Secondary Loss is that its effect 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 Andersen Consulting in 2002).

### 3.5.3 Loss Factors

All loss factors fall within one of the following four categories:

- Asset
- Threat
- Organization
- External

For reasons that will become clear, 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*.

In order for us to make reasoned judgments about the form and magnitude of loss within any given scenario, we have to evaluate the factors within all four of these categories. Within this Standard, we will limit our discussion to some of the most common and most important loss factors.

#### 3.5.3.1 *Asset Loss Factors*

There are two asset loss factors that we are concerned with: value/liability and volume.

As we will see when we cover measurement, the value/liability characteristics of an asset play a key role in both the nature and magnitude of loss. We can further define value/liability as:

- **Criticality** – characteristics of an asset that have to do with the impact to 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; i.e., the cost associated with replacing it if it has been made unavailable (e.g., stolen, destroyed, etc.). Examples include 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. Note that this 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, etc.). 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 to protect the information.
  - **General** – sensitive information that doesn’t 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 equals greater LM if an event occurs; e.g., two children on a rope swing *versus* one child, or one sensitive customer record *versus* a thousand.

#### 3.5.3.2 *Threat Loss Factors*

Within this document, we’ll limit our threat considerations to three threat loss factors: action, competence, and whether the threat agent is internal or external to the organization.

Threat agents can take one or more of the following actions against an asset:

- **Access** – simple unauthorized access.
- **Misuse** – unauthorized use of assets (e.g., identity theft, setting up a pornographic distribution service on a compromised server, etc.).
- **Disclose** – the threat agent illicitly discloses sensitive information.
- **Modify** – unauthorized changes to an asset.
- **Deny Access** – includes destruction, theft of a non-data asset, etc.

- **Accomplish Assigned Mission** – for example, establish a foothold in the asset for later malicious use.

It is important to recognize that each of these actions affects different assets differently, which drives the degree and nature 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 doesn't play a critical role in productivity won't directly result in a significant productivity loss. Yet that same asset, if disclosed, can result in significant loss of competitive advantage or reputation, and generate legal costs. The point is that it's the combination of the asset, kind of violation, and kind of exploitation of this violation that determines the fundamental nature and degree of loss.

Which action(s) a threat agent takes will be driven primarily by that agent's motive (e.g., financial gain, revenge, recreation, etc.) and the nature of the asset. For example, a threat agent bent on financial gain is less likely to destroy a critical server than they are to steal an easily pawned asset like a laptop. For this reason, it is critical to have a clear definition of your threat community in order to effectively evaluate LM.

Threat competence is similar to the Threat Capability (TCap) factor that contributes to Vulnerability (Vuln). The difference is subtle, but important. Threat competence has to do with the amount of damage a threat agent is capable of inflicting once the compromise occurs, while TCap to violate has to do with the threat agent's ability to put itself in a position to inflict harm. An example may help to clarify this point. A terrorist threat agent has capabilities they would employ in an attempt to access nuclear secrets. These capabilities play a role in the likelihood that they'll be successful in gaining access. Their ability to inflict harm once they've acquired the secrets (e.g., build a bomb) is, however, dependent upon a different set of competencies. In this Standard, the characteristics that enable the terrorist to compromise defenses and be in a position to acquire the secrets are called *threat capabilities*. The characteristics that enable them to inflict harm (e.g., create a bomb) are referred to as *threat competencies*. We will not dwell on threat competence in this document. Nonetheless, it's useful to recognize that this factor exists in order to have a more complete understanding of risk.

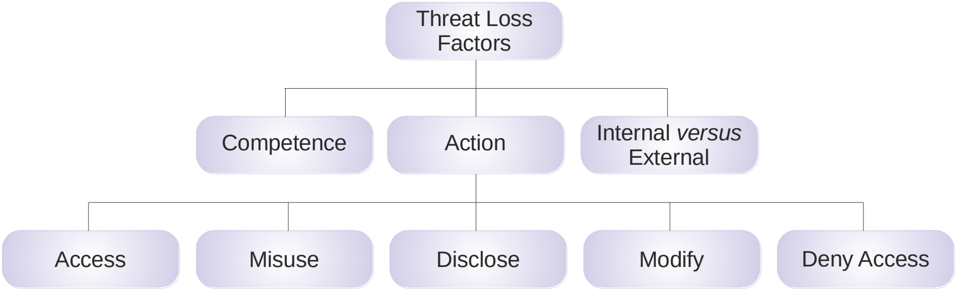

**Figure 7: Threat Loss Factors**

The consideration of 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.

#### 3.5.3.3 *Organization Loss Factors*

There are many organizational loss factors. Within this document, we will limit our discussion to four – timing, due diligence, response, and detection.

The *timing* of an event can have a tremendous impact on loss. For example, an event occurring in the midst of a big advertising campaign may create significantly greater loss than a similar event at some other time of year.

*Due diligence* can play a significant role in the degree of liability an organization faces from an event. If reasonable preventative measures were not in place (given the threat environment and value of the asset), then legal and reputation damage can be far more severe. The challenge is that "reasonable preventative measures" are not universally defined or agreed. Often, "industry standards" or theoretical "best practices" are looked to as guidelines for due diligence. Unfortunately, these guidelines typically don't consider the threat environment or LM. Consequently, industry standards and best practices may be insufficient (i.e., not truly representative of due diligence) or overly conservative (i.e., prohibitively expensive given the real risk).

How effectively an organization *responds* to an event can spell the difference between an event nobody remembers a year later, and one 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; for example, 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.

We tend to think of response capabilities solely within the context of criticality; i.e., the ability to return productivity to normal. It is critical to recognize, however, that 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 fully compensating harmed parties. Conversely, an organization that denies and deflects responsibility is much more likely to become a pariah and a media whipping post.

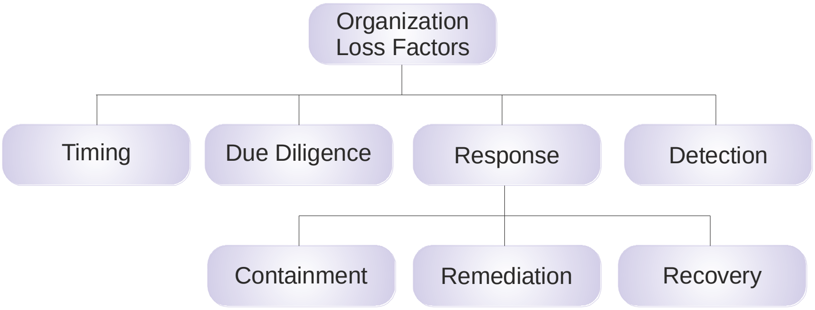

**Figure 8: Organization Loss Factors**

You can't respond to something you haven't detected; i.e., response is predicated on detection. In training sessions, the question often comes up: "What about those events we may not know about – theft of confidential organization information by corporate spies, breaches of sensitive customer information, etc.?"

Clearly, incidents take place that don't immediately show up on the radar. However, it's also reasonable to believe that such events – if they result in material loss – will always be detected eventually. For example, the damage from sensitive competitive advantage information that makes its way to a competitor is likely to materialize and be recognized. Was the detection timely? Perhaps not. However, once detected, the organization may still have an opportunity to respond and reduce its losses. For example, legal action against a competitor who stole proprietary information might be appropriate.

#### 3.5.3.4 *External Loss Factors*

External loss factors generally fall into one of the following five categories – Detection, Legal and Regulatory, Competitors, Media, and Other Stakeholders (e.g., customers, partners, stockholders, etc.).

A couple of important things to recognize about external loss factors include:

- These five categories represent entities that can inflict a secondary form of harm 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, etc.).
- All of the factors within these external categories can be described as "reactive to an event". In other words, in order for an external factor to affect LM, the event has to be detected by an external entity. For example, if an employee executes identity theft by misusing their legitimate access to customer information, the customer(s), regulators, and lawyers can't inflict harm upon the organization unless the identity theft is tied back to the organization. Likewise, if a productivity outage occurs but isn't detected by customers, partners, etc., then the organization will not be subject to a negative response on the part of those stakeholders.

This last point leads us to our first external loss factor – *detection*. Based upon the premise above, we can think of detection as a binary factor on which all other external factors are predicated. External detection of an event 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, intentional disclosure by the organization (either out of sense of duty, or because it is required by law), or by accident.

The legal and regulatory landscape is primarily made up of three parts – regulations (local, state, federal, and international), contract law, and case law. Although this component of the external landscape is evolving rapidly, it is safe to say that fines and sanctions can be significant for organizations within regulated industries. In theory, however, fines and judgments are driven in part by how much harm actually occurs from an event and the level of due diligence exercised to prevent it from occurring in the first place. In other words, if an event occurs that represents a regulatory or legal breach, fines and judgments should reflect how much harm actually occurs to the affected stakeholders as well as how proactive the organization was in preventing the loss.

Losses associated with the competitive landscape typically have to do with the competition's ability and willingness to take advantage of the situation.

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 on 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 who exercised due diligence 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.

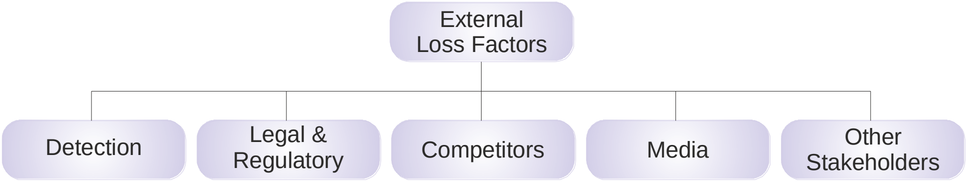

**Figure 9: External Loss Factors**

# 4 Example Application (Informative)

This chapter provides an example of how the Risk Taxonomy may be used to perform a risk analysis. The analysis steps and charts shown are borrowed from the Introduction to Factor Analysis of Information Risk (FAIR). A more detailed walkthrough of this scenario is provided within the companion Risk Analysis Standard.

**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. FAIR is more widely recognized for its ability to be leveraged in a more effective quantitative analysis performed using PERT distributions as inputs, and leveraging a Monte Carlo function as the computational engine.

## 4.1 The Scenario

A Human Resources (HR) executive within a large regional 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.

## 4.2 The Analysis: FAIR Basic Risk Assessment Methodology

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

- Stage 1: Scope the Analysis:

  — Identify the asset at risk

  — Identify the threat community under consideration

  — Define the loss event

- Stage 2: Evaluate Loss Event Frequency (LEF):

  — Estimate the Threat Event Frequency (TEF)

  — Estimate the Threat Capability (TCap)

  — Estimate Resistance Strength (RS)

  — Derive Vulnerability (Vuln)

  — Derive Loss Event Frequency (LEF)

- Stage 3: Evaluate Loss Magnitude (LM):

  — Estimate Primary Loss

— Evaluate Secondary Loss

— Estimate Secondary Loss Event Frequency (SLEF)

— Estimate Secondary Loss Magnitude (SLM)

- Stage 4: Derive and Articulate Risk:

— Derive Primary Risk

— Derive Secondary Risk

— Derive Overall Risk

The stages above, and the example below, describe an analysis performed at a specific level of abstraction in the taxonomy. Specifically, it shows deriving Vulnerability from Threat Capability and Resistance Strength, and then deriving Loss Event Frequency from Threat Event Frequency and Vulnerability.

It is important to remember that analyses can be performed at higher layers of abstraction (e.g., estimating LEF directly) or lower levels of abstraction (e.g., deriving TEF from estimates made at Contact Frequency and Probability of Action). For more information on choosing an appropriate layer of abstraction, please refer to the Risk Analysis Standard.

### 4.2.1 Stage 1: Scope the Analysis

Experience has demonstrated repeatedly that scoping an analysis thoroughly and clearly is the most important thing an analyst can do to shorten the overall time required and improve the quality of the analysis. Skimping on the scoping stage is often a recipe for frustration.

#### *4.2.1.1 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 this scenario is whether the credentials are the asset, or whether it’s the applications, systems, and information that the credentials provide access to. The short answer is “they’re all assets”. In this case, however, we’ll focus on the sensitive personal information accessible via the log-on credentials because that is expected to represent the greatest potential impact.

#### *4.2.1.2 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.

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, and whether it makes sense to combine communities. For this example, we’ll focus on the cleaning crew.

#### 4.2.1.3 Define the Loss Event

Having identified the asset at risk and the relevant threat community, the next step is to clearly define the loss event itself. 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.*

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.

### 4.2.2 Stage 2: Evaluate Loss Event Frequency (LEF)

#### 4.2.2.1 Estimate the Threat Event Frequency (TEF)

Some people demand reams of hard data before they are comfortable providing quantitative estimates. Unfortunately, because we sometimes don’t have useful or credible data for scenarios, the Threat Event Frequency (TEF) is often ignored altogether. When we ignore the frequency 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, I may not have years of empirical data documenting how frequently cleaning crew employees abuse usernames and passwords on sticky-notes, but I can make a reasonable estimate using ranges, particularly if I have been trained in how to make estimates effectively.

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.

Recognizing that cleaning crews are generally comprised of honest people, that an HR executive’s credentials typically would not be considered 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 using the table below.

| Rating | Description |
|---|---|
| Very High (VH) | > 100 times per year |
| High (H) | Between 10 and 100 times per year |
| Moderate (M) | Between 1 and 10 times per year |
| 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 member to have motive, sufficient computing experience to recognize and leverage the potential value of these credentials, and 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 frequency is expected to be relatively low given the variables in play.

#### 4.2.2.2 *Estimate the Threat Capability (TCap)*

Threat Capability (TCap) refers to the threat agent's skill (knowledge & experience) and resources (time and materials) that can be brought to bear. 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, computer skills) 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, relative to the overall threat population, given that basic computer skills are widespread and even the cleaning crew is likely to have some computer experience. Keep in mind that TCap is always estimated relative to the scenario being analyzed. If our scenario were related to SQL injection attack, we would probably rate the cleaning crew as having a lower TCap.

| 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 |

Note that in some scenarios it may be possible to affect relative TCap skill levels by using uncommon technologies or practices. For example, threat agents that may be highly adept in working with Microsoft® technologies may be relatively clueless when faced with an older mainframe computer.

The Resource component of TCap boils down to two elements: time and materials. In some scenarios it may be possible to affect relative TCap by either shortening the time available to the threat agent (e.g., by having highly effective detection and response capabilities) or by minimizing the materials that are available to them (e.g., removing unnecessary tools and utilities from systems).

#### 4.2.2.3 *Estimate Resistance Strength (RS)*

Resistance Strength (RS) has to do with an asset's ability to resist being negatively affected by a threat community. In our scenario, given the combination of credentials being in plain sight and in plain text, the RS is Low. An argument could be made for Very Low, except for the fact that even after logging on the attacker would likely need to navigate one or more applications to find the employee information. This highlights the fact that, in addition to explicit controls, the inherent difficulty in performing an attack will affect the likelihood of its success.

| **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 |

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, because they limit the volume of people who come into contact with the sticky-note.

#### 4.2.2.4 *Derive Vulnerability (Vuln)*

Deriving Vulnerability (Vuln) is easy once you have established your TCap and RS. Using the matrix below, simply find the TCap along the left side of the matrix, and the RS along the bottom, where they intersect determines the Vulnerability. For our example, as shown below, a Medium TCap combined with a Low RS results in High Vulnerability.

**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)**

4.2.2.5 *Derive Loss Event Frequency (LEF)*

Similar to Vulnerability, Loss Event Frequency (LEF) is derived by intersecting the TEF and Vulnerability within a matrix.

**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)**

In our scenario, given a TEF of Low and Vulnerability of High, the LEF is 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.

## 4.2.3 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 the magnitude of loss if an event does occur.

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.

Note that the steps for evaluating LM vary from those outlined in the original Standard, mostly due to the new approach for differentiating Primary from Secondary Loss. The changes also represent the fact that best-case, worst-case, and most likely outcomes are easily derived using PERT distributions as input and Monte Carlo as a computational engine.

4.2.3.1 *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.

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/<br>Judgments | Comp.<br>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.

#### *4.2.3.2 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.

#### *4.2.3.3 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)** | **VL** | **L** | **M** | **H** | **VH** |
|---|---|---|---|---|---|
| **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 |

**Secondary Loss Probability**

#### *4.2.3.4 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.

## 4.2.4 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.

### *4.2.4.1 Derive Primary Risk*

We've 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)**

### *4.2.4.2 Derive Secondary Risk*

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

**Secondary Risk**

| Secondary Loss Magnitude (LM) | | VL | L | M | H | VH |
|---|---|---|---|---|---|---|
| | 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 |

**Secondary Loss Event Frequency (SLEF)**

#### *4.2.4.3 Derive Overall Risk*

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

**Overall Risk**

| Secondary Risk | | VL | L | M | H | VH |
|---|---|---|---|---|---|---|
| | VH | VH | VH | VH | VH | VH |
| | H | H | H | H | H | VH |
| | M | M | M | M | H | VH |
| | L | L | L | M | H | VH |
| | VL | 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 evaluation of a problem like executive credentials on a sticky-note, it’s likely that we would analyze and report on more than one scenario (e.g., another threat community), and then aggregate the results to have a more complete picture of the true loss exposure.

# 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 10 shows these chained dependencies.

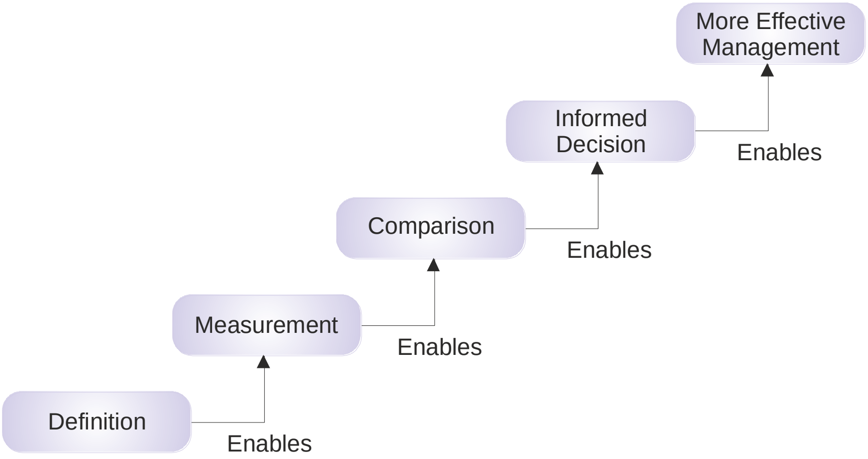

**Figure 10: Chained Dependencies**

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. This 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.

## A.2 What Makes this the Standard of Choice?

Although definitions and taxonomies already exist within the information security landscape, none provide a clear and logical representation of the fundamental problem our profession is tasked with managing – the frequency and magnitude of loss. For example:

- Existing taxonomies tend to focus on a sub-component of the problem. Two current examples of work limited to particular areas of concern are the Common Weakness Enumeration (CWE) and the Common Attack Pattern Enumeration and Categorization (CAPEC).[2] However, while these two efforts are noteworthy, valuable, and consistent, most efforts are not consistent. In the absence of a common foundation it becomes difficult or impossible to tie together or interlink sub-taxonomies, which limits their utility to only the most narrow applications.

- Taxonomies are inconsistent in their use of common terms (e.g., "risk" in one taxonomy may translate to "vulnerability" in another). This makes normalization of data difficult if not impossible, and leads to confusion and ineffective communication, which can further erode credibility.

[2] Information about CWE is available at http://cwe.mitre.org, and information about CAPEC is available at http://capec.mitre.org.

- Documents that claim to describe "taxonomies" in fact provide definitions without clear or, in some cases, any descriptions of the relationships between elements. Absent these relationships, it becomes impossible to perform meaningful calculations even when good data is available.

The risk taxonomy described within this Standard provides several clear advantages over existing definitions and taxonomies, including:

- There is a clear focus on the problem that management cares about – the frequency and magnitude of loss.
- Risk factor definitions are conceptually consistent with other (non-security) risk concepts with which organization management is already familiar.
- It enables quantitative analysis of risk through the use of empirical data (where it exists) and/or subject-matter expert estimates.
- It promotes consistent analyses between different analysts and analysis methods.
- It provides a framework for describing how risk conclusions were arrived at.
- It effectively codifies the understanding of risk that many highly experienced professionals intuitively operate from but haven't had a reference for.
- It provides a reference and foundation for the evolution of specific sub-taxonomies.
- The multiple layers of abstraction within the model enable analysts to choose how deep/comprehensive they want to be in their analyses. This feature allows analysts to model risk in a cost-effective manner.

## A.3 Who Should Use It?

This Standard should be used by anyone seeking to:

- Understand how risk works and/or the factors that drive risk
- Consistently perform high quality risk analyses
- Develop or apply security metrics
- Evaluate, debate, or discuss the basis for risk conclusions
- Develop or apply risk analysis and assessment methodologies

A few examples of how the taxonomy can provide value are:

- Security organizations sometimes find that management rejects their risk conclusions and recommendations, in part because it's difficult to articulate the intuition and experience that led to those conclusions. The ability to explain how conclusions were arrived at using a logical and rigorous method can have a very significant impact on credibility in the eyes of management.

- Organizations often find that the quality and consistency of analyses performed by their security analysts vary widely. The Risk Taxonomy Standard can be used to improve this by bringing everyone onto the same page with regard to terminology, definitions, and approach. This is especially helpful when bringing on staff who are newer to the profession, as it shortens the time it takes to make them effective.
- Metrics development and application are also improved by using the taxonomy to identify which data points are needed in order to support analyses, as well as where to get that data and how to use it. For example, data regarding threat contact frequency, the type of actions taken, which controls worked or failed to work, types and magnitude of loss, etc., can be extracted from incidents of all kinds (e.g., virus events, user errors, breaches, etc.) and used to support analyses.
- Organizations often engage external consultants to provide an impartial view of the organization's risk posture. The taxonomy can be used very effectively to evaluate the consultants' risk conclusions and recommendations, ensuring that findings aren't inflated (or underrated). This ability to more consistently and effectively analyze risk is a critical factor in enabling more cost-effective risk management.

## A.4 Related Dependencies

In order to make effective use of this Standard, risk assessment and analysis methodologies must provide data and/or estimates for each of the factors within the taxonomy. For example, if an assessment methodology leaves out or ignores Threat Event Frequency (TEF), then conclusions resulting from the methodology will not align with the taxonomy nor will they faithfully represent risk.

Note that where empirical data doesn't exist for one or more of the risk factors, it is acceptable to use subject-matter expert estimates. For practical purposes, quantitative estimates should not be precise. Instead, estimates should be provided as ranges (e.g., "a TEF of 1 to 10 times per year") or as distributions (e.g., "minimum 1 time per year, most likely 7 times per year, with a maximum of 10 times per year") with some form of confidence rating that represents the level of certainty surrounding the estimates.

If qualitative estimates are used as inputs (e.g., "High", "Medium", "Low"), the estimates should ideally be mapped to a predefined set of quantitative ranges (e.g., "Medium = 1 to 10"). This enables the relationships between factors within the taxonomy to be represented mathematically, which enables more effective risk calculation. It also provides a means for comparison between analyses performed by different analysts (normalization), as well as a means of explaining how conclusions were arrived at.

If pure qualitative values are used (i.e., values that don't reference a quantitative range or distribution), then the taxonomy may be used as a structural reference rather than a framework for calculation.

Note that the decision to use qualitative or quantitative values should be driven by the needs and desires of those who will receive or base their decisions on the analysis results. A secondary factor that may drive this choice is whether the analyst is comfortable using quantitative estimates.

# B Risk Taxonomy Considerations

Extensive discussion in development of this Risk Taxonomy included considerations that can be grouped into four categories, as follows:

- 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 FAIR framework, but rather are observations and concerns that apply no matter what method is used to analyze risk.

## B.1 Complexity of the Model

There is no question that the proposed framework goes into greater detail than most (if any other) 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 estimates at higher levels of abstraction within the model; e.g., measuring Threat Event Frequency (TEF) rather than attempting to measure Contact Frequency (CF) and Probability of Action (PoA). 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 we would not need well-defined frameworks and we would not have challenges over analyzing it 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, we recognize that even FAIR's detailed taxonomy isn't a perfect or comprehensive treatment of the problem. There are no perfect taxonomies/models of real-world complexity. It's just that we consider FAIR to be significantly more complete than we are used to, and the best-analyzed and well-defined there is today.

With regard to communicating complex risk information to business decision-makers (who often want information like this delivered in simple form), the problem isn't inherently with the model but rather with the user. As is the case with any complex problem, we need to be able to articulate results in a way that is useful and digestible to decision-makers. It is also not unusual for management to ask how the results were arrived at. Experience has shown that having a rigorous framework to refer to in the explanation tends to improve credibility and acceptance of the results.

## B.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 our 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 FAIR framework has been proven in practice to help solve those two issues. It doesn't, of course, help us with those instances where data isn't available because events are rare. In those cases, regardless of what analysis method is chosen, the estimates aren't going to 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.

## B.3 Iterative Risk Analyses

Due to the inherent complexity of risk, risk analyses tend to be iterative in nature. In other words, it is absolutely true that initial risk analyses tend to be "sighting shots" that often 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.

It is worthy of note that this observation is true of any analysis method, including the FAIR model.

## B.4 Perspective

An alternative view held by some is that "exposure" should be the focus of our attention rather than "risk". The argument put forward here is that they consider "risk" to be 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 FAIR model, both issues are related (sort of a "before" and "after" perspective) and relevant. Fortunately, the FAIR framework provides the means to analyze both conditions by allowing the analyst to derive unmitigated risk as well as mitigated risk levels.

# C Practical Use of FAIR

## C.1 The Risk Language Gap

Over time, the ways we manage risk have evolved to keep up with ways we conduct business. There is a very long history here, pre-dating the use of IT in business. As the scope, scale, and value of business operations have evolved, our 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 will be the impact 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.

So, a business manager tends to think of a “threat” as something which could result in a loss which the business cannot absorb without seriously damaging its trading position. Compare this with our Risk Taxonomy definitions for “threat” and “vulnerability” below:

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.

This Risk Taxonomy Standard 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 so we can 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.

## C.2 Key Risk Concepts

It is critical to understand the difference between possibility and probability in order to analyze risk. You can think of possibility as being binary – something is possible or it isn't. Probability, however, is a continuum that addresses the area between certainty and impossibility. And because risk is invariably a matter of future events, there is always some amount of uncertainty. This is important because executives cannot choose or prioritize effectively based upon statements of possibility. Effective risk decision-making can only occur when information about probabilities is provided.

Another important and related distinction is that 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 doesn't help people understand the probabilistic nature of analysis. Keep in mind that, as a decision-maker, even though you can't tell me which roll of the dice will come up, knowing that the probability is 1-in-36 is incredibly valuable information.

## C.3 Using FAIR with Other Risk Assessment Frameworks

As The Open Group seeks to further its risk management framework based on Factor Analysis of Information Risk (FAIR), it is important to understand what the strengths of a FAIR approach are, and how they complement the work of other standards bodies. This section explains the outputs of a FAIR analysis and how these outputs are valuable in augmenting other risk assessment frameworks.

A valuable starting point here is the work published by the European Network and Information Security Agency (ENISA) in its November 2007 paper: *Methods for the Identification of Emerging and Future Risks*. This ENISA document described how 18 various risk assessment frameworks addressed the criteria that the agency thought were important in assessing risk, and graded them on a numerical scale. In reviewing the ENISA criteria, the rating they assigned to each one, and the other risk assessment frameworks they reviewed, it became obvious that FAIR is not in direct competition with the other risk assessment frameworks, but actually is complementary to many of them. Whereas most frameworks focus on identifying issues that contribute to risk, FAIR provides the means to effectively evaluate the significance of those issues.

Since the original publication of the Risk Taxonomy Standard in January 2009, The Open Group has also published an additional guidance document describing how to use FAIR with ISO/IEC 27005 (see the referenced FAIR – ISO/IEC 27005 Cookbook).

## C.4 The Ability of a FAIR-Based Approach to Complement Other Standards

FAIR, as a taxonomy of the factors that contribute to risk and how they affect each other, is primarily concerned with establishing accurate probabilities for the frequency and magnitude of loss events. It is not, *per se*, a "cookbook" that describes how to perform an enterprise (or individual) risk assessment. For example, FAIR documentation isn't so much concerned about the where and how you should get information for use in the assessment, as much as explaining how to describe the value of that information and how it contributes to creating risk.

So many risk assessment methodologies don't focus or concern themselves with how to establish consistent, defensible belief statements about risk – they simply give you steps they believe an organization should perform in order to have information for use in the creation of risk statements. As such, FAIR can be utilized within the context of many of these standards without significant modifications to FAIR or the other methodology.

## C.5 An Example: Using FAIR with OCTAVE

One good example might be using FAIR to augment an OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) assessment. OCTAVE is a risk assessment methodology developed and sold by US-CERT (refer to www.cert.org/octave). In Version 2 of the OCTAVE criteria, the document authors mention at least three times that: "*Using probability ... is optional*". Section 3.2 of OCTAVE then directs assessors to establish their own criteria and context for developing values (high, medium, low) for "impact" and "likelihood". Unfortunately, OCTAVE gives no structured means to determine why likelihood might be "high" or why impact might be "low". OCTAVE simply states:

*"It is important to establish criteria (for the qualitative expressions) that are meaningful to the organization."*

Practitioners who want a means to develop "meaningful" risk statements using FAIR would simply use the FAIR taxonomy and framework to build consistent and defensible risk statements. This could be accomplished by augmenting Section 3 of the OCTAVE criteria with the relevant parts of the FAIR basic risk assessment methodology (see Chapter 8) which describes how FAIR's basic risk assessment methodology comprises ten steps in four stages. In this example, the risk criteria in Section 3.2 of the OCTAVE criteria would be strengthened by using the appropriate steps in the FAIR basic risk assessment methodology, and the statement of risk required by Section 3.3 of the OCTAVE criteria would similarly be able to use the appropriate step in the FAIR methodology.

# Glossary

### Action

An act taken against an asset by a threat agent. This 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 baseline 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 a threat event will become a loss event.

# Index

abstraction ....................................2, 7
analysis methodology.....................37
asset loss factors.............................16
asset volume ...................................16
CAPEC...........................................35
case law..........................................20
CF.....................................................9
competitive landscape ....................20
competitors.....................................19
contact
  intentional .....................................9
  random ..........................................9
  regular ...........................................9
contract law ....................................20
CWE...............................................35
data metrics.....................................40
deny access.....................................27
destruction......................................27
detection ..................................19, 20
disclosure........................................27
due diligence............................18, 20
  best practices...............................18
  industry standards .......................18
estimate
  distribution..................................37
  range............................................37
external loss factors........................19
FAIR........................................21, 39
fines and judgments........................20
flexibility........................................39
information security risk ..................1
LEF..............................................7, 8
legal and regulatory........................19
legal and regulatory landscape .......20
LM............................................7, 12
loss
  competitive advantage.................13
  fines/judgments...........................13
  forms of.......................................13
  productivity.................................13
  replacement.................................13
  reputation ....................................14
  response.......................................13
loss analysis...................................12
loss event.......................................23
loss exposure ....................................7
loss factors.....................................15
  asset ............................................15
  external .......................................15
  organization ................................15
  threat ...........................................15
loss flow ........................................14
media.......................................19, 20
misuse............................................26
Monte Carlo ................21, 26, 27, 28
organization loss factors.................18
Overall Risk ...................................32
password strength...........................12
PERT............................21, 26, 27, 28
PII...................................................13
PoA.............................................9, 10
possibility.......................................42
prediction .......................................42
Primary Loss ............................14, 26
Primary Risk ..................................31
probability ...............................10, 42
probability factor
  level of effort ..............................10
  risk of detection/capture .............10
  value............................................10
qualitative estimate.........................37
quantitative estimate.......................37
regulations......................................20
response..........................................18
  containment.................................18
  recovery ......................................19
  remediation .................................18
risk....................................................7
risk acceptance ...............................34
risk assessment..........................5, 37
risk budgeting.................................34
risk factor ........................................1
risk factor variables..........................5
risk management stack .....................5
risk measurement ...........................34
risk nomenclature...........................34

risk prioritization............................34
RS...................................................11
Secondary Loss.........................15, 28
Secondary Risk...............................31
sensitivity
  competitive advantage.................16
  embarrassment/reputation...........16
  general.........................................16
  legal/regulatory ...........................16
SLEF..............................................15
SLM...............................................15
stakeholders....................................19
taxonomy
  example.......................................21
TCap...............................................11
TEF..................................................8
threat
  access .........................................17
  accomplish assigned mission ......17
  deny access..................................17
  disclosure ...................................17
  misuse ........................................17
  modification................................17
threat capabilities ...........................17
threat community ...........................22
threat competence...........................17
threat competencies........................18
threat loss factors ...........................17
  action .........................................17
  competence ................................17
  internal or external to the
    organization ............................17
timing ............................................18
unintended disclosure.....................16
value/liability ................................16
  cost.............................................16
  criticality....................................16
  sensitivity...................................16
volume...........................................16
Vuln...............................................10