The Open Group Guide

Open FAIR™ Risk Analysis Process Guide
Version 1.1

The Open Group Guide

Open FAIR™ Risk Analysis Process Guide, Version 1.1

ISBN: 1-947754-06-5

Document Number: G180

Published by The Open Group, January 2018.
Updated September 2022 to align with the Open FAIR™ Body of Knowledge, Version 2.0.

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 1

2 Define the Purpose of Risk Analysis 2
- 2.1 Initial Greenfield Risk Analysis of the *Status Quo* 4
- 2.2 Transfer (Insurance) Risk Analysis 4
- 2.3 Support Other Risk Regimes 5
- 2.4 Remediation Project 5
- 2.5 Prioritization of Alternative Projects 6
- 2.6 Conclusion 6

3 Initiate the Risk Analysis Project 7
- 3.1 Identify the Primary Stakeholder 9
- 3.2 Identify the Asset or Asset Type 9
- 3.3 Identify the Threat Agent or Threat Community 9
- 3.4 Identify the Threat Event 10
- 3.5 Identify Available Resources and Information Sources 10
- 3.6 Identify Time and Budget Constraints 10
- 3.7 Create a Preliminary Risk Question 10
- 3.8 Exit the Initiation Phase 11

4 Scope and Plan the Risk Analysis 12
- 4.1 Scope the Risk Analysis 12
  - 4.1.1 Answer Clarifying Questions 13
  - 4.1.2 Describe the Loss Scenario 17
- 4.2 Plan the Risk Analysis 19
- 4.3 Exit the Scoping and Planning Phases 20

5 Execute the Risk Analysis 21
- 5.1 Model the Status Quo 21
- 5.2 Analyze the Present State of Risk (or Status Quo) 22
- 5.3 Model a Proposed Alternative 22
- 5.4 Estimate the Risk of the Proposed Future State 23
- 5.5 Evaluate the Alternative 23
- 5.6 Prepare to Inform the Decision-Maker 23

6 Inform the Decision-Maker 24
- 6.1 Who? 25
- 6.2 What? 25
- 6.3 When? 25
- 6.4 Where? 26
- 6.5 Why? 26
- 6.6 How? 26
- 6.7 Presenting Findings 26

7 Conclusion 27

Preface

The Open Group

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

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

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

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

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

This Document

This document is The Open Group Open FAIR™ Risk Analysis Process Guide, Version 1.1. It has been developed and approved by The Open Group.

This document offers some best practices for performing an Open FAIR analysis: it aims to help risk analysts understand how to apply the Open FAIR risk analysis methodology. It is meant for analysts who are familiar with the Open FAIR Body of Knowledge but have not yet completed an analysis using it, which means the analyst has read both The Open Group Standard for Risk Analysis (O-RA) and The Open Group Standard for Risk Taxonomy (O-RT). Moreover, the Guide assumes the analyst has done some form of qualitative analysis.

This document complements the Open FAIR™ Risk Analysis Example Guide, which provides examples of completed Open FAIR risk analyses. As a result, this document focuses solely on describing the process for completing an Open FAIR risk analysis, only providing examples as useful for explanation or illustration.

Trademarks

Acknowledgements

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

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

- Chris Carlson, C T Carlson LLC
- Mike Jerbic, Trusted Systems Consulting Group
- Eva Kuiper (formerly of) DXC Technology
- John Linford, The Open Group Director, Security Forum & OTTF
- Dan Riley, Kyndryl
- John “Jay” Spaulding, (former) The Open Group Director, Security Forum & OTTF

Referenced Documents

The following documents are referenced in this Guide.

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

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

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

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

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

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

[G167 2016] The Open FAIR™ – NIST Cybersecurity Framework Cookbook, The Open Group Guide (G167), published by The Open Group, October 2016; refer to: www.opengroup.org/library/g167

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

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

1 Introduction

In the information security industry, when asked to perform a risk analysis, many risk analysts merely apply their own personal methodology and models to arrive at conclusions that are often not comparable: “high risk” for one analyst will mean something entirely different to another.

When analyses do not follow a consistent process, the same input data may lead to varying and diverging results. Moreover, discussing differences in results becomes a long and tedious process, as analysts must attempt to explain and defend their findings. Often, even when analysts have access to a more refined model, such as the Open FAIR™ taxonomy, it is not used to clarify exactly what they are analyzing, which can lead to frustration and inaccurate results.

The body of this document offers guidance on many areas, including identifying the type of risk analysis requested by a decision-maker, a structured way of initiating, planning, organizing, and executing an analysis project, with guidance on how to present results to management. This document structures every risk analysis as a project, with phases that must be completed in order and steps to complete in each phase; however, this does not mean every analysis will require a full project team or leadership by a project manager. Structure and organized thinking are what are important to an analyst or team completing a successful analysis. This document also provides many questions for risk analysts to answer before doing any analysis.

2 Define the Purpose of Risk Analysis

Before beginning any analysis, the risk analyst must understand the decision-maker's purpose for requesting it. That purpose will define the category or main structure of the analysis. Typically, there are five main purposes that sponsors have for requesting a risk analysis:

- Initial risk analysis of the current state or *status quo* (known as a Greenfield analysis[1])
- Transfer (insurance) risk analysis
- Support other risk regimes
- Remediation project
- Prioritization of alternative projects

Regardless of purpose, all risk analyses will go through the initiation, scoping, planning, execution, and informing phases of the analysis. The purpose of the risk analysis will ultimately dictate which steps are taken within the execution phase: Greenfield analyses, analyses used to evaluate risk to transfer or insure, and analyses in support of other regimes will not need to complete all the steps within it, while analyses for remediation projects or alternative prioritization will complete all the steps. The steps within these phases are described in the following sections of this document and are depicted in Figure 1.

[1] A "Greenfield analysis" refers to an initial analysis for which there is no prior work; refer to: https://en.wikipedia.org/wiki/Greenfield_project.

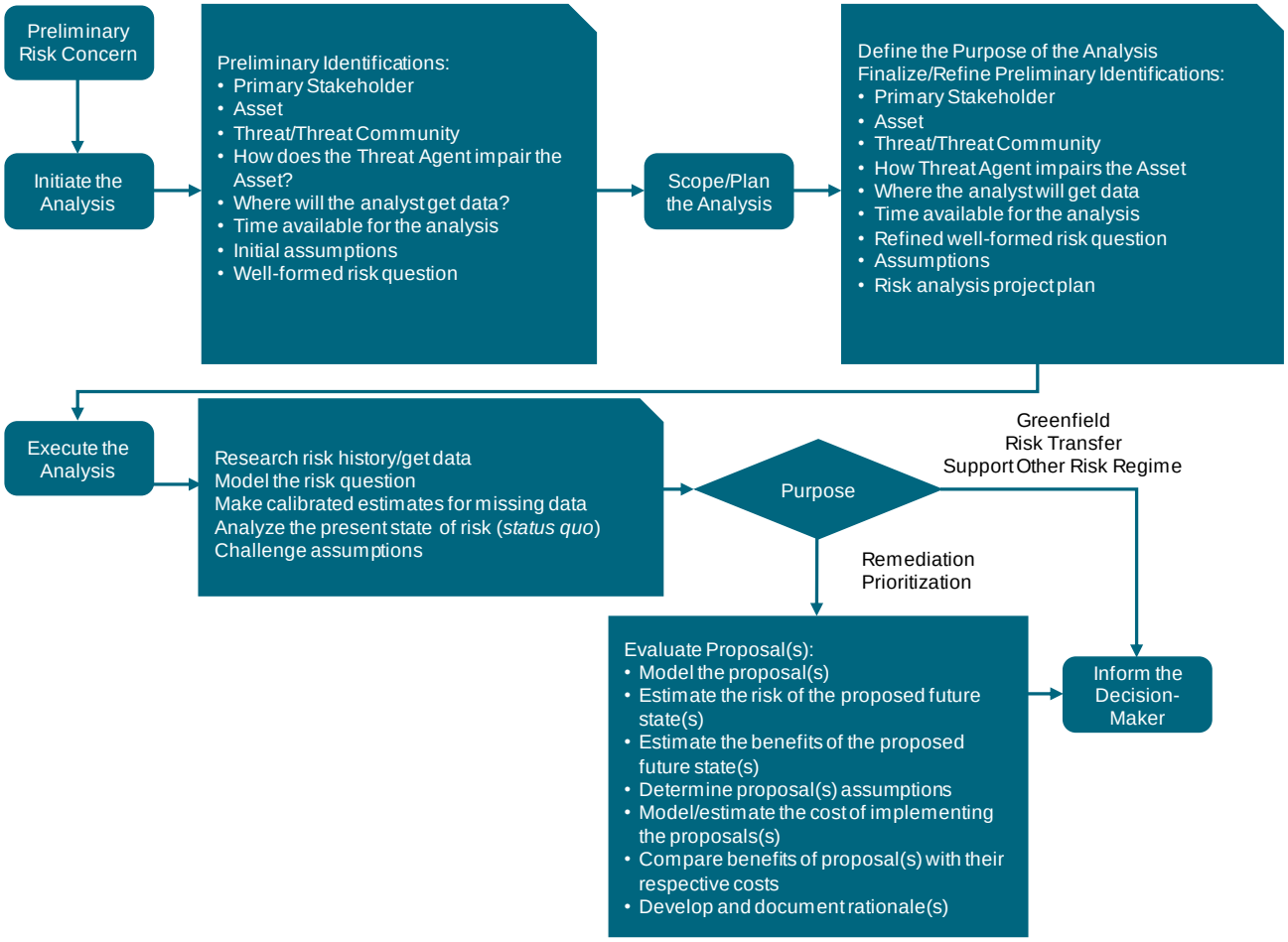

Figure 1: Open FAIR Analysis Process Flow Chart

While the steps taken may vary, all these categories of risk analysis share an identical goal: to assist with effective decision-making, which is why the final phase for every risk analysis purpose is informing the decision-maker.

The Open FAIR framework follows a bottom-up approach. That is, it focuses on ensuring that risk analyses are completed using an accurate model; using an accurate model helps ensure that measurements are indeed meaningful and, therefore, can be used to make effective comparisons. These comparisons lead to informed decisions and ultimately allow decision-makers to make effective decisions. Figure 2 shows how these all relate.

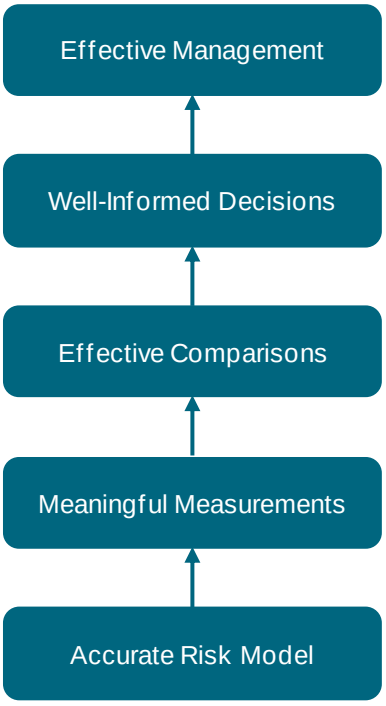

Figure 2: The Open FAIR Risk Management Stack

2.1 Initial Greenfield Risk Analysis of the *Status Quo*

When an organization is performing an initial risk analysis to determine the current risk state, it will utilize an initial Greenfield analysis. As a result, this category of analysis is inherently a top-down approach: the Primary Stakeholders are concerned about specific things and want a statement of risk on the topic as well as a clearly specified Loss Scenario. This current state analysis may be used to continue an analysis, may add to another analysis, or may be used simply to keep management informed.

As mentioned briefly earlier, a Greenfield risk analysis will only need to complete some of the steps in the execution phase. These analyses are completed to understand the current state of risk rather than to remedy a concern. As a result, they do not consider alternatives to the *status quo*.

2.2 Transfer (Insurance) Risk Analysis

Another category of risk analysis is used to determine if transferring the risk to an insurance company is worthwhile. Just as with the initial Greenfield analysis, a transfer risk analysis does not complete all the steps within the execution phase because it will be looking to determine how much risk (if any) can be transferred to an insurance company. The Open FAIR process is particularly useful for this.

The results of a Monte Carlo simulation performed as part of an Open FAIR analysis estimate the probability and magnitude of annual loss – in other words, a probability distribution of annual loss, also called the annual loss exposure. The stakeholder should expect that the average of the distribution represents an expected annual cost. The stakeholder, however, is exposed to

the total distribution of losses, not just the average. Actual losses will vary between the estimated minimum and maximum of the simulated annual loss distribution.

Most stakeholders, however, prefer certainty of their costs to uncertainty. They prefer to pay the average cost – or something near that – each year instead of a cost that varies. In other words, stakeholders prefer low variance to high variance, certainty to uncertainty. When risk-averse stakeholders insure their risk, they transfer the cost variance, not the average cost, to the insurance company in exchange for a premium. The Open FAIR expression of the probability distribution of annual loss exposure informs stakeholders of not just the average of annual loss, but the variability they can expect and can potentially insure against.

2.3 Support Other Risk Regimes

Sometimes, other risk regimes, such as security or compliance standards, may call for a risk analysis to be performed. However, they do not specify how to analyze this risk, making the analysis itself vague and open-ended. To overcome this, the analyst may choose to use the Open FAIR framework to satisfy the risk analysis requirement. For instance, ISO/IEC 27001 [ISO/IEC 27001] specifies that those following the standard should perform a risk analysis, but it does not specify how. An Open FAIR risk analysis meets this requirement and fills the void.[2] Another example of a standard that requires a risk analysis is the NIST framework. Again, the Open FAIR framework can be used to meet this requirement.[3] Moreover, the Open Trusted Technology Provider™ Standard (O-TTPS) [C185-1 2018, C185-2 2018] requires that organizations manage supply chain risk;[4] again, by providing a consistent way of defining, discussing, and measuring risk, the Open FAIR framework can assist with the identification, assessment, prioritization, and mitigation of these risks.

Finally, the Open FAIR framework can also be used to comply with regulations when those regulations ask for a risk-based approach. The Open FAIR framework meets that description and fulfills the requirement well.

Unless otherwise specified within the other risk regime, an Open FAIR risk analysis for this purpose will complete the same steps within the execution phase as a Greenfield or transfer risk analysis.

2.4 Remediation Project

A remediation project is one that aims to mitigate or prevent loss arising from risk. As a result, a risk analysis for a remediation project must go through all the execution phase steps. The first steps act only to establish a *status quo* of current risk. The remaining steps act to evaluate potential solutions, called proposals, to the problem, determining how those proposals would affect the risk, and identifying their benefits and costs. As a result, decision-makers can then determine whether the evaluated mitigation techniques are worth their costs of implementation or whether it is more worthwhile to attempt a different strategy, which can include doing nothing. More guidance on these steps is described in Chapter 5.

[2] Refer to the Open FAIR – ISO/IEC 27005 Cookbook [C103 2010].
[3] Refer to the Open FAIR™ – NIST Cybersecurity Framework Cookbook [G167 2016].
[4] Refer to the Supply Chain Security Risk Management (SC_RSM) requirements within the O-TTPS, Part 1 (§4.2.1.1) and Part 2 (§4.11).

2.5 Prioritization of Alternative Projects

When many sources of risk or many ways to mitigate risk exist, decision-makers may have difficulty deciding how to optimally deploy their limited resources. However, the Open FAIR framework provides a common metric for all the various Loss Scenarios and mitigation options. Therefore, a decision-maker can compare results from multiple Open FAIR risk analyses to determine which proposals are worth pursuing or are most worthwhile to the decision-maker.

Management will likely focus on those proposals with higher net benefits or that are more cost-effective; as a result, the analyst would need to evaluate how other changes would affect net benefits or cost effectiveness and must, therefore, complete all the execution phase steps. The analyst can then create a portfolio of potential solution proposals to a Loss Scenario for management to use when deciding how to address it.

If management has more than one Loss Scenario but only wants to mitigate the greatest risk, the analyst can create a portfolio of Loss Scenarios for decision-makers to consider. Because the risk for every scenario is expressed in the same units and through the same terminology, the decision-maker can consider a set of costs and benefits for each analysis and use these to determine the most important Loss Scenario for focus.

2.6 Conclusion

This chapter highlighted the five most common reasons why management sponsors risk analysis projects. Ultimately, how management will use the analysis will dictate the category of risk analysis and the steps of the project, but every Open FAIR analysis follows a similar set of initial planning and scoping steps. Chapter 3 describes how to initiate a risk analysis project. It discusses important questions to consider and information necessary for any analyst to start to understand the Loss Scenario and project scope. Chapter 4 addresses the topics of scoping and planning a risk analysis. Chapter 5 describes how to execute a risk analysis and walks through the steps required to model and conduct a risk analysis using the Open FAIR framework and methodology. Chapter 6 highlights information crucial to provide when informing the decision-maker. Examples of analyses are published separately in the Open FAIR™ Risk Analysis Example Guide [G21A 2021].

3 Initiate the Risk Analysis Project

In general, a risk analysis project starts when a decision-maker decides they are concerned about the risk of some action or activity.

From this point, the decision-maker conveys this concern (either directly or indirectly) to the risk analyst, who must then work to understand this concern and adequately address it. This means the risk analyst must follow a series of steps or stages, as described below.

The stages presented in this document differ somewhat from those presented in The Open Group Standard for Risk Analysis (O-RA) [C20A 2021], since the focus here is on providing guidance primarily for beginning the analysis, while the O-RA Standard focuses most on completing the analysis. The mapping between documents is shown in Table 1.

Table 1: Cross-Mapping of Risk Analysis Stages

Stage	Open FAIR Risk Analysis Process Guide (this document)	The Open Group Standard for Risk Analysis (O-RA)
Stage 0	Chapter 3: Initiate the Risk Analysis Project	
Stage 1	Chapter 4: Scope and Plan the Risk Analysis	§5.1: Identify the Loss Scenario (Scope the Analysis)
Stage 2	Section 5.1: Model the Status Quo Section 5.2: Analyze the Present State of Risk (or Status Quo)	§5.2: Evaluate the Loss Event Frequency
Stage 3	Section 5.1: Model the Status Quo Section 5.2: Analyze the Present State of Risk (or Status Quo)	§5.3: Evaluate the Loss Magnitude
Stage 4	Section 5.2: Analyze the Present State of Risk (or Status Quo) Section 5.4: Estimate the Risk of the Proposed Future State Section 5.5: Evaluate the Alternative Section 5.6: Prepare to Inform the Decision-Maker Chapter 6: Inform the Decision-Maker	§5.4: Derive and Articulate Risk

Stage	Open FAIR Risk Analysis Process Guide (this document)	The Open Group Standard for Risk Analysis (O-RA)
Stage 5	Section 5.3: Model a Proposed Alternative Section 5.4: Estimate the Risk of the Proposed Future State Section 5.5: Evaluate the Alternative Section 5.6: Prepare to Inform the Decision-Maker Chapter 6: Inform the Decision-Maker	§5.5: Model the Effect of Controls

The risk concern originally presented to the risk analyst is usually vague and is rarely presented in the Open FAIR format of Loss Event Frequency and Loss Magnitude. For instance, a generic concern of a decision-maker could be as simple as "I saw several firms in my industry suffered a ransomware attack; I am worried about that happening to this firm". Clearly, the risk analyst would still have much to determine before being able to describe the Loss Scenario using the Open FAIR framework.

The risk analyst, then, must first determine the purpose of the requested risk analysis. The purpose of the analysis will determine what information is necessary and will dictate which steps will need to be taken later in the analysis, as discussed in Chapter 2.

Once the purpose is identified, the risk analyst must work to ensure the concerns of the decision-maker can be translated into an actionable format consistent with the Open FAIR terminology. This means the risk analyst must identify some information from the presented concerns that can be used to form a preliminary risk question, which is an output of the initiation phase of a risk analysis, along with a project objective statement. This question uses the information provided by the decision-maker to present their concerns consistent with the Open FAIR terminology and structure.

A well-defined risk question will ask about the probable frequency and probable magnitude of future loss. For instance, a generic risk question will ask: "What is the probable frequency and probable magnitude of future loss associated with …… (management's concern)?". An Open FAIR risk analysis uses the probable frequency of future loss (Loss Event Frequency) and the probable magnitude of future loss (Loss Magnitude) to form an estimate of risk. Therefore, the risk question that the analyst answers with their analysis must be as specific as possible. This document discusses refining a risk question in Chapter 4.

Before being able to answer a risk question, the risk analyst must first create a preliminary risk question to be refined later. The risk analyst must also document any assumptions made about the concerns of the decision-maker and the purpose of the analysis because they will be crucial when confirming that the preliminary risk question addresses the concerns of the decision-maker at the end of the initiation phase and while forming the project objective statement.

A risk analysis can only be as strong as the risk question it answers, and forming a preliminary risk question is the first step of an iterative process undertaken by the risk analyst to form as specific a risk question as possible given the information available at this early project stage. Figure 3 shows the steps of the initiation phase. It also shows what information the risk analyst must have as primary parameters, the questions useful for narrowing down the Loss Scenario, and the information needed to form the project objective statement as well as the preliminary risk question.

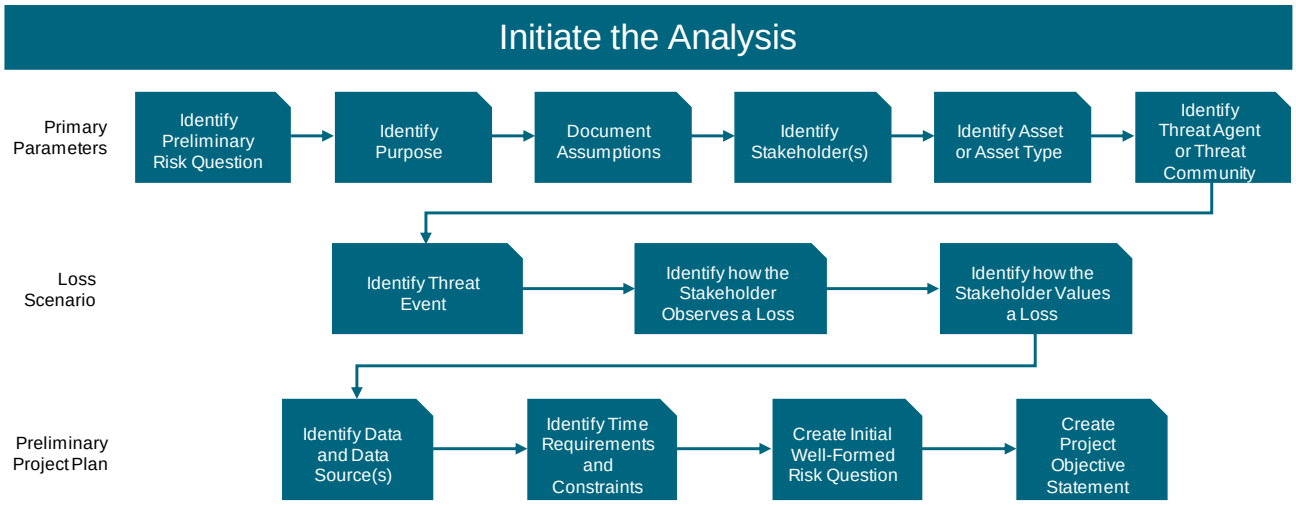

Figure 3: Initiation Phase Steps

3.1 Identify the Primary Stakeholder

For the analyst, identifying the Primary Stakeholder will often be rather straightforward: it is likely the organization sponsoring and defining the parameters of the risk analysis. However, it can also include individual people and groups of people. Simply put, the Primary Stakeholder is the person or organization that owns the Asset at risk, so the risk analyst does a risk analysis on behalf of the Primary Stakeholder. To develop a preliminary risk question, the Primary Stakeholder may not need to be overly specific, but as the analysis progresses, this may change.

3.2 Identify the Asset or Asset Type

An Asset is anything of value; this includes systems, data, people, facilities, cash, etc. To begin, the analyst should have some idea of what the Asset is – this will come from the decision-marker's concerns. In reality, this will likely be vague and require further scoping to identify a specific Asset for an Open FAIR analysis. However, as the analyst understands the stakeholder's concern and the Loss Scenario better, this Asset can become more specific. Refining the Asset will also help the analyst define the threat(s) to that Asset as well as losses from actions against it.

3.3 Identify the Threat Agent or Threat Community

A Threat Agent is anything or anyone that can act against the Asset. The Threat Agent or Threat Community may be human, animal (such as rats or termites), or naturally occurring events (such as earthquakes, floods, or tornados). Human Threat Communities may take deliberate, malicious action or simply make human errors, so the Threat Agent or Threat Community also includes people who may or may not realize they could impair or compromise the Asset.

As the Loss Scenario becomes more specific through scoping, the analyst may identify more than one Threat Agent or Threat Community. For instance, a human Threat Agent may be an insider or an outsider. Outsiders may be hackers, criminals, or even hostile foreign governments. In some cases, the Threat Agent or Threat Community will be more specific than others, which

will require initiating a separate analysis for each newly defined Threat Agent or Threat Community.

3.4 Identify the Threat Event

Threat Agents can act in a wide variety of ways to impair or compromise the Asset; this action is referred to as the Threat Event. By identifying the Threat Agent's actions, the analyst can begin to understand the Loss Scenario(s). For instance, a hurricane might throw a car through the walls of a building or flood an office; a burglar might steal a laptop with banking statements on it from an unlocked car. These examples focus on the specific method that the Threat Agent will use to impair the Asset.

After identifying how the Threat Agent or Threat Community might act against the Asset, the analyst can begin to think of ways to prevent this action or respond to it. However, for the preliminary risk question, the specific method of impairment might not yet be identified, so the analyst must either make assumptions about the Threat Agent and its methods or get clarifying information from the decision-maker or a Subject Matter Expert (SME).

3.5 Identify Available Resources and Information Sources

These resources will be invaluable to the analyst for refining the preliminary risk question. They may include employees working for the organization that requested the analysis, research conducted by various institutes, first-hand accounts of people involved in the scenario, SMEs, etc. Gathering this information can be challenging, especially if the risk analyst is unfamiliar with the process. However, the analyst will use this information to narrow down the preliminary risk question and eventually to form a more specific risk question.

3.6 Identify Time and Budget Constraints

The time and budget available to conduct the analysis will determine a lot about what the risk analyst can do. Specifically, the risk analyst must consider how much detail can possibly be included while still addressing the concerns of the decision-maker and finishing the risk analysis project within the time limit. Depending on the concerns of the decision-maker, the analyst could find that multiple analyses are necessary to address the concerns, so these constraints must be established at the beginning of the project.

By drafting a preliminary project plan before creating a preliminary risk question, the analyst can begin to restrict the scope of the project from ballooning and becoming unmanageable before it even begins. At this stage, the preliminary project plan need be little more than the time and budget available to the risk analyst for the project. The plan will change as the analyst's understanding of the decision-maker's concerns and, therefore, the risk question changes.

3.7 Create a Preliminary Risk Question

The preliminary risk question should include as much information as possible about the Asset, Threat Agent, and Loss Scenario. It is the analyst's first attempt at putting the concerns of the decision-maker into as much of the Open FAIR structure as possible by asking the risk question in terms of the probable frequency and magnitude of future loss associated with the target Asset;

following this structure is crucial for the remainder of the Open FAIR risk analysis. As stated earlier, a well-formatted risk question will ask: "What is the probable frequency and probable magnitude of future loss associated with …… (management's concerns)?".

Perhaps the most common fault is asking a risk question that is too broad. The preliminary risk question acts as a first step in preventing this fault. A preliminary risk question might be: "What is the probable frequency and probable magnitude of future loss associated with loss of functionality in a datacenter?"[5] This is far too broad to be an actual risk question – it does not include an Asset other than the datacenter and has next-to-no information on the Loss Scenario or Threat Agent – but the risk analyst can iteratively revise it to strengthen it.

The risk analyst must remember that developing a risk question is an iterative process. Starting with a risk question that includes some description of frequency or magnitude will help ensure the risk analysis has the correct rigor. The preliminary risk question will undergo multiple modifications and revisions as the risk analyst learns new information about the Loss Scenario and the concerns of the decision-maker.

3.8 Exit the Initiation Phase

The preliminary project plan and the preliminary risk question are the outputs of the initiation phase. At this point, the risk analyst should roughly understand how the provided information fits the Open FAIR format as well as what additional information is necessary to conduct the analysis. Ideally, the analyst will have already identified the Primary Stakeholder, the Asset, and the Threat Community. The risk analyst should have used this information to create a preliminary risk question that follows the Open FAIR format and presents the concern about future loss in terms of probable frequency and probable magnitude. Again, the risk analysis can only be as strong as the risk question it answers. The analyst should also have a general idea of how the project might be spaced out in the available time. This information should be included in the project objective statement. The risk analyst will use this project statement when confirming the purpose and preliminary risk question with the decision-maker.

From this point, the analyst must confirm that the preliminary risk question and project statement accurately represent the concerns of the decision-maker. The preliminary project statement should include the purpose of the analysis as well as any assumptions the analyst has made. Confirming this information with the decision-maker is crucial before refining the preliminary risk question further through scoping. If the preliminary risk question does not represent the decision-maker's concerns, additional refinement is necessary before scoping and planning the risk analysis.

[5] This example preliminary risk question is refined in Chapter 4.

4 Scope and Plan the Risk Analysis

After forming the preliminary risk question, making preliminary assumptions, making preliminary determinations on the Threat Agent, Asset at risk, and Loss Scenario, and confirming that they accurately represent the concerns of the decision-maker, the risk analyst can begin to scope and plan the risk analysis. During this phase, the risk analyst will refine the preliminary risk question and other primary parameters as new information about the Loss Scenario is learned.

Communication with the decision-maker is vital throughout this phase of the analysis because new information could reveal that the concerns initially described by the decision-maker are unfounded and that other Loss Scenarios present greater probability of future loss. If this occurs, the risk analyst must confirm that the decision-maker concurs with the change of focus. Figure 4 depicts the steps within the scoping and planning phases of the risk analysis as well as what information during these phases will be useful for describing the Loss Scenario and creating a project plan.

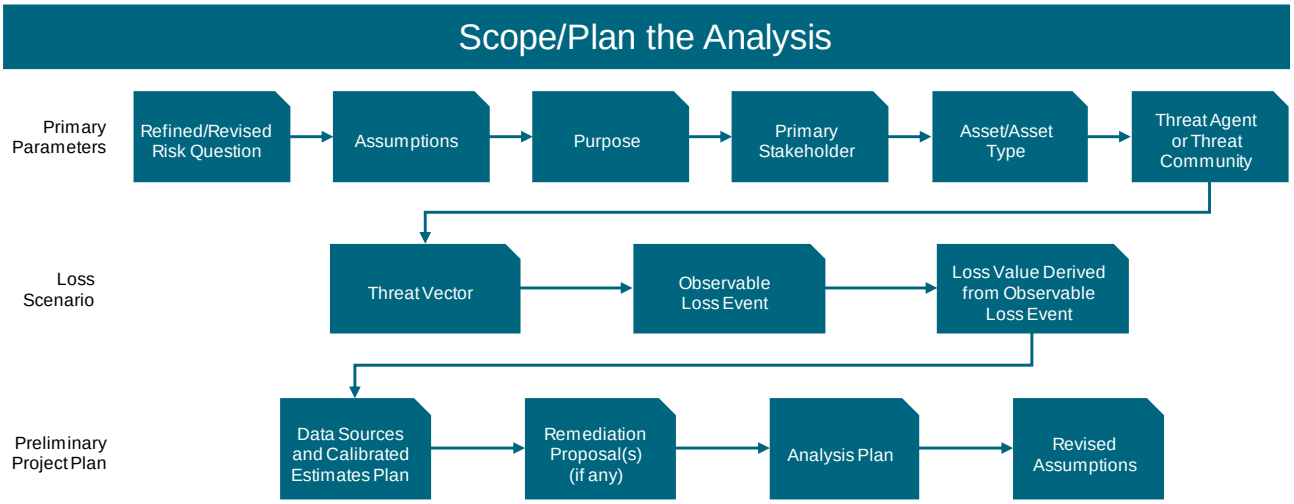

Figure 4: Scoping and Planning Phase Steps

This chapter provides multiple questions that the risk analyst should work to answer as well as guidance on planning the analysis using project management strategies. Although some of the questions might seem repetitive, the risk analyst should remember that working to clarify assumptions made in the initiation phase is necessary because the decision-maker either did not provide or did not consider necessary information.

4.1 Scope the Risk Analysis

After the initiation phase, the risk analyst should have a general idea of the target Asset and Threat Agent(s) and/or Threat Community; therefore, during the scoping process, the analyst must work to define as clearly as possible the target Asset and identify the Threat Agent(s) and/or Threat Community. Depending on the Threat Community, though, many different attack

types may exist, so the analyst must also identify how the Threat Agent could impact the Asset; i.e., the threat vector(s) of interest. This impact could come from a wide array of possibilities, ranging from the deliberate theft of credit card numbers to water damage to a building from a storm.

As the risk analyst scopes the risk analysis, they may find that more than one analysis is required to address sufficiently the concerns of the decision-maker or that an alternative threat is of greater concern. As a result, throughout the scoping process, the risk analyst must stay in consistent communication with the decision-maker, ensuring that any change focus is approved, even for a small change, because all changes will affect the risk question and, therefore, the entire risk analysis.

Before beginning the scoping phase, the risk analyst must have confirmed with the stakeholder that the preliminary risk question addresses the decision-maker's concerns and that the assumptions included in the project statement are reasonable. During the scoping process, these assumptions may change as the risk analyst finds new information.

While scoping the risk analysis, the analyst will also need to consider the relationships among four factors: threats, loss, controls, and Assets. By considering how these interact, the analyst can ensure that the risk question will be specific enough to address the concerns of the decision-maker and that each Open FAIR analysis conducted is deliberately done to aid understanding.

4.1.1 Answer Clarifying Questions

By answering the following clarifying questions precisely and accurately, the analyst can refine a broad preliminary question into something actionable. These questions are similar to what the analyst considered to form the preliminary risk question, so some of the answers could be identical, depending on how much information the decision-maker provided in the preliminary risk concern.

The main objective in answering these questions – perhaps for the second time – is commitment to these answers that form the foundation for the scope of the analysis. Clear, unambiguous answers to these questions will allow the analyst to create a specific risk question for each Open FAIR analysis that will be performed, assuming more than one is necessary.

4.1.1.1 Who is the Primary Stakeholder?

The Primary Stakeholder from the preliminary risk question may or may not be specific enough for the individual Open FAIR analyses. For some analyses, using the organization requesting the analysis as the Primary Stakeholder is likely specific enough. However, the Primary Stakeholder could also be a specific part of a business or a department within an organization. Identifying the exact Primary Stakeholder will ensure the remainder of the analysis only includes information relevant to the concerns of the decision-maker.

4.1.1.2 What is the Asset or Asset Type?

The analyst should have already identified a Preliminary Asset; i.e., the thing that needs to be protected and for which losses need to be calculated. To begin, the analyst should have some idea of what the Asset is – this will come from the decision-marker's concerns. However, as the analyst understands the Loss Scenario(s) better, this Asset can become more specific. For instance, the datacenter specified in the example preliminary risk question in Section 3.7 could refer to any number of different Assets depending on the interests of different Threat Agents or Threat Communities, but customer information stored in the datacenter will likely have specific

Threat Agents. If there is more than one Asset, the analyst might consider conducting more than one Open FAIR analysis, especially if each Asset has a different Threat Agent acting upon it in a different way.

The analyst should also identify aspects of the Asset that will contribute to the Asset's ability to resist the actions of a Threat Agent. It may seem to be a semantic distinction, but information regarding the nature of the Asset and the organization's ability to manage and maintain the Asset contribute to understanding the controls around it, which will be discussed later in this section. The analyst should consider the organization in terms of its business objectives, strategies, and policies as well as legal, regulatory, and contractual requirements, the overall approach to risk management, the expectations of shareholders, geographical locations, and any constraints affecting the organization. All of these will influence the organization's ability to make decisions about risk.

Because the Asset is a fundamental part of loss, the analyst should also understand the business process(es) to which the Asset contributes, the cost to replace the Asset, the architecture of the Asset (hardware, software, nature of services accessible, etc.), and the resources necessary to respond to an incident (geographic location in relation to the Incident Response Team, for example).

From the example preliminary risk question, the Asset of concern is a datacenter. However, this can become more specific. The question specifies loss of functionality as the main concern, but this could result from issues involving power supplied to the datacenter, the ability of the datacenter to connect to a network, etc. Therefore, the Asset will relate directly to the ability of the datacenter to remain functional.

4.1.1.3 Who or What is the Threat Agent or Threat Community?

The Threat Agent is anything or anyone that can act against the Asset. A Threat Community is a group of people or things with similar interests, motives, or methods for impairing the Asset. The Threat Agent or Threat Community will act directly against the Asset, and "rational", human Threat Agents will act against these Assets to accomplish an objective that is valuable to the Threat Agent at an acceptable cost to the Threat Agent.

Depending on the concerns described by the decision-maker, the analyst may have already identified a specific Threat Agent when the risk analysis was requested. If they did not, the analyst can consider the target Asset to understand who or what might impair it and why.

The analyst may find it useful to pre-suppose the applicable Threat Community. In doing so, the analyst should consider information about the Asset's value to the threat, as well as the relative frequency and nature of threat contact with the Asset. The threat analysis can be approached by breaking the threats down by category (e.g., human/natural/malware) and then by characteristics. This descriptive process for collecting and viewing all the threats in relationship to each other can provide a means for identifying the most probable threat for consideration. Table 2 depicts some examples of various threats possible.

Table 2: Threat Examples

Human		Malware	Event/Circumstance Beyond Control
Internal	**External**		
Privileged	Technical Professional	Any Self-Propagating	Natural Disasters
Non-Privileged	Technical Amateur		Animals
	Non-Technical Professional		Flooding
	Non-Technical Amateur		

Although the Open FAIR framework does not specifically address threat actions,[6] the analyst should consider Threat Agent motives to determine the action that the Threat Agent is most likely to take. Because an Open FAIR analysis relies on numbers and quantitative data to create probabilistic ranges, the analyst should look for information on two specific threat metrics: the expected frequency of Threat Events (Threat Event Frequency), and the ability of the Threat Agent or Threat Community to apply force against the Asset and subsequent controls (Threat Capability).

In developing data for these threat metrics, the threat classification and probable threat actions should drive the analyst's quest for evidence and subsequent measurements. Once the metrics for the threat are gathered, the next step in risk analysis would be to review the controls, for the ability to resist controls is relative to Threat Capability, which the Open FAIR framework defines as the level of force a Threat Agent will most likely apply against an Asset.

The example preliminary risk question about the datacenter provides no information on the Threat Agent or Threat Community. For the sake of simplicity, assume the risk analyst has examined the various factors that might act to impede the functionality of the datacenter and found that this datacenter is located in a part of the country frequently impacted by tornadoes. Due to the severe problems tornadoes can impose, the datacenter likely already has excellent information on Threat Event Frequency and Threat Capability, even if it does not use those terms to describe the information.

4.1.1.4 What is the Threat Event?

The answer to this question describes the (eventual, if the Threat Agent is successful) Loss Event(s) and part of the Loss Scenario(s). This question seeks to understand how the Threat Agent will act upon the Asset to impair or otherwise compromise, considering the specific method that the Threat Agent will use, also known as the threat vector.

The threat vector chosen by the Threat Agent will ultimately depend upon the controls used by the organization. Controls in the Open FAIR framework are those things that will contribute to the ability to resist the actions of a Threat Agent or Threat Community. The Open FAIR framework specifies four categories of controls: avoidance, deterrent, Vulnerability, and responsive.

[6] The O-RA Standard does provide high-level categories of actions (access, misuse, disclose, modify, and deny access), but it does not provide specifics for any category.

Resistance Strength, which is impacted by Vulnerability-related controls, is an estimation of the ability to resist the force applied by some percentile of the general Threat Agent population. In the Open FAIR framework, the ability to resist is judged relative to the threat population; therefore, the analyst must understand the Threat Agent or Threat Community before being able to make statements about control strength. Analysts should research and maintain a list of control effectiveness ratings for various controls that are useful in establishing control strength estimates.

Using information gathered during scoping, the analyst would likely find that tornadoes could cause physical damage to the datacenter, damage power lines near the center, or otherwise impair the ability to connect to the network and transfer/receive data. Assuming power outages are the most common result of a nearby tornado, the datacenter would likely have some controls in place to prevent as much functionality loss as possible, such as using back-up generators when power lines are damaged.

4.1.1.5 How does the Asset's Owner Know that the Asset has been Impaired or Compromised?

To phrase this question differently, how does the Primary Stakeholder observe a loss, and what information do stakeholders observe? Again, the answer to this question describes part of the Loss Scenario(s). This question seems as though it may be straightforward; however, this is not always the case. There are clear ways to identify the loss of some Assets (e.g., a stolen car) while identifying the loss of others will be less obvious (e.g., a stolen credit card number). The risk analyst should have a methodology for documenting how the stakeholder observes losses that is followed consistently.

4.1.1.6 How does the Asset Owner Value the Loss as Observed Above?

The Primary Stakeholder will value different Assets and Loss Scenarios differently. For instance, the Primary Stakeholder could only care about replacement costs or may worry about additional costs from a loss.

Regardless, the Open FAIR framework uses monetary values for all losses to ensure the analysis can be completed using common and comparable units, meaning that numerous analyses can be compared and that costs can be discussed and contrasted without difficulty, thereby allowing the analyst to address the concerns of the decision-maker more easily. Therefore, the analyst must convert observable information on the loss to monetary units by modeling how a loss occurs. The model can vary, but the analyst should specify the model used and be able to clearly describe the rationale for using it.

4.1.1.7 Where will you Find Information on the Loss?

This question deals with one of the more challenging aspects of the risk analysis. Not every loss has easily identifiable information. Because the Open FAIR risk tree (see Figure 7) embraces a top-down approach, the analyst might not need large quantities of data from lower levels of the risk tree if the higher levels have enough information on frequency and magnitude of prior loss to inform future estimates.

Sometimes, though, data is not readily available. This is not necessarily a problem: by focusing on quantitative measures and avoiding asking questions that rely on personal feelings, an analyst can obtain information that is more useful. For instance, a risk analyst might ask: "How many times per year does the organization have work laptops stolen from personal vehicles?" to identify the Loss Event Frequency. However, asking: "How strong is the security system already

in place?" will not yield a precise result. Therefore, the risk analyst must consider what can be analyzed while asking questions to find information on the loss.

Continuing the tornado example, useful questions might include: "How many times per year do tornadoes touch down inside of the power grid to which the datacenter is connected?" and "How many times per year does the datacenter lose power as a result of a tornado?". The analyst could direct these questions either to the datacenter of the analysis and/or to similar datacenters to help inform the estimates.

4.1.2 Describe the Loss Scenario

After answering the previous questions, the risk analyst should have a rough idea of the Loss Scenario, which is the "story of loss" as defined from the Primary Stakeholder's perspective and describes how a loss occurs. It should include information on the Threat Agent, the threat vector, and how the Primary Stakeholder values the Asset, observes the loss, and values the loss. The Open FAIR analysis will only apply to the specific Loss Scenario that the risk analyst creates; therefore, the risk analyst must confirm with the decision-maker that it describes the concerns precisely and accurately. At this point, the risk analyst should work to use the answers to those questions to specifically describe the Loss Scenario.

While describing the Loss Scenario, the risk analyst should identify what the Threat Agent does to impair the Asset. The Open FAIR framework breaks down loss into Primary Loss and Secondary Loss categories: Primary Losses occur as a direct result of the Threat Agent's actions, while Secondary Losses occur as a result of a Secondary Stakeholder (a third party) reacting negatively to a Primary Loss and then becoming Threat Agents to Primary Stakeholders through their reactions.

The Loss Scenario is the story of that loss that forms a sentence:

A Threat Agent breaches or impairs an Asset that causes an observable Loss Event that has direct economic consequences (Primary Loss) and may have economic consequences initiated by reactions from others (Secondary Loss).

Table 3 describes the six forms of loss identified in the Open FAIR framework. Of these, productivity, response, and replacement losses are most commonly experienced as Primary Losses; response, competitive advantage, fines/judgments, and reputation losses are most commonly experienced as secondary costs. However, any of the six forms can be experienced as a primary or Secondary Loss.

Table 3: Open FAIR Six Forms of Loss

Forms of Loss	
Productivity	Direct losses associated with the reduction in an organization's ability to generate its primary value proposition (e.g., income, goods, services); it may also include costs associated with personnel who are unable to perform their duties but who continue to collect their paycheck (e.g., a call center's phone lines are down, but personnel continue to be paid); it accounts for the loss of revenue due to operational outages and discontinuation (e.g., revenue lost when a retail website is unavailable due to a system outage); and it includes costs associated with the impaired productivity of personnel (e.g., increased costs from switching from automated to manual methods).

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

In an Open FAIR risk analysis, the probability of a Primary Loss Event and the losses attributed to that event drive the probability of a Secondary Loss Event. An organization has the opportunity to implement controls that will resist threats from identifiable sources of these Secondary Losses. Therefore, in utilizing an Open FAIR approach, loss estimation involves identifying Primary Losses from direct operational impacts, identifying the third-party Threat Agent source of secondary operational impacts, and performing subsequent analyses (as warranted) to determine the likelihood and impact of Secondary Losses from secondary operational impacts.

The Loss Scenario as well as the Primary Loss Event and Secondary Loss Event is presented in Figure 6.

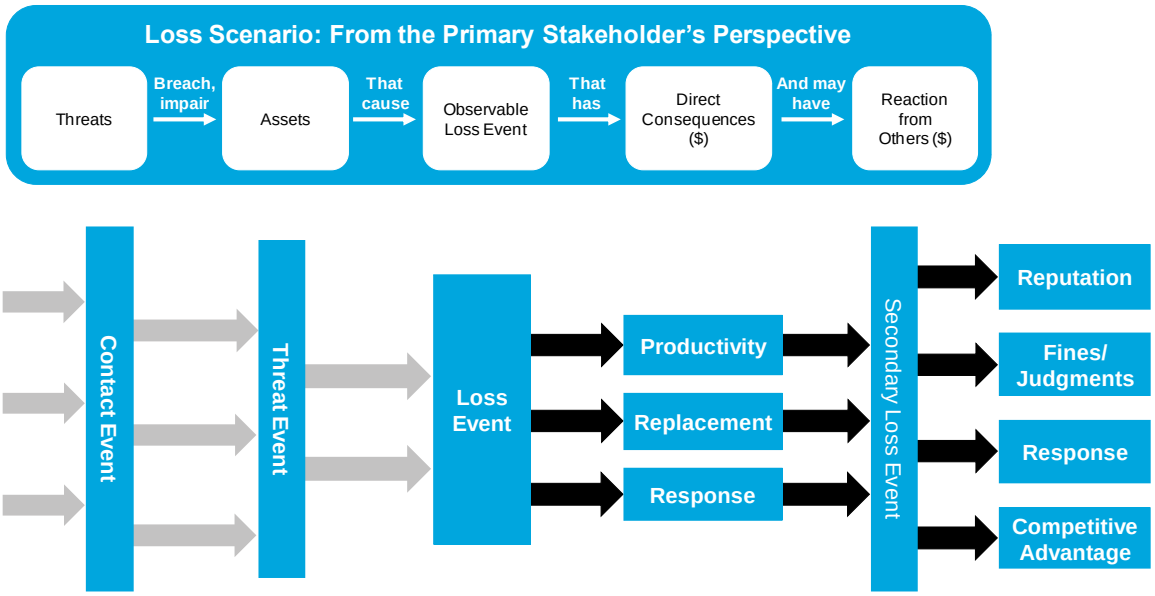

Figure 5: Open FAIR Loss Event

Continuing the hypothetical Loss Scenario, a tornado causing a power outage that prevents devices from communicating would likely face all three of the Primary Losses: the organization will no longer be able to transmit/receive data to/from its clients, employees will need to restore power somehow, and any power supply-related property that the tornado damaged will need to be replaced.

4.2 Plan the Risk Analysis

An Open FAIR risk analysis fits the definition of a project well, and this document treats it accordingly. Therefore, the analyst should be familiar with using project management strategies or should consider seeking an experienced project manager to assist in planning and later executing the analysis.

The risk analyst must do this only after precisely answering the questions above. These questions should have allowed the analyst to further narrow the scope of the risk analysis. After answering these questions, the risk analyst can understand what additional work is necessary to complete the risk analysis project. This means the risk analyst should understand where the necessary data will be found to complete calibrated estimates – any analysis requires finding data from any number of sources or people. Using project management strategies allows the risk analyst to better understand how the risk analysis project will progress.

Because the risk analyst should already have a preliminary project plan from the initiation phase, there will already be a rough understanding of the tasks to be completed; however, this may be little more than an understanding of the time and budget constraints. Therefore, at this point, the risk analyst should identify specific tasks and account for any additional Open FAIR analyses that need to be completed; these tasks will rely upon the purpose of the analysis.

4.3 Exit the Scoping and Planning Phases

More often than not, the initial risk question will have become much narrower during the scoping process.[7] Therefore, the outputs of the scoping phase of the risk analysis are the Threat Agent and/or Threat Community, the Loss Scenario, and the refined risk question. The risk analyst will work to answer this now more specific question. For instance, the risk question asked earlier may now become: "What is the probable frequency and probable magnitude of future loss associated with a tornado causing power loss to a datacenter and preventing communication between devices?". This is now a much stronger risk question: it identifies the Asset, the Threat Agent, and the threat vector. The Loss Scenario then, as the single-sentence story of the loss, would be: "A tornado causes power loss to a datacenter that prevents devices from communicating."

If the decision-maker prefers a shorter version of the risk question, the risk analyst can replace "the probable frequency and the probable magnitude" with "risk", so the question reads: "What is the risk associated with a tornado causing power loss to a datacenter and preventing communication between devices?". However, the risk analyst must remember that the phrase has merely been substituted.

The actionable project plan, which is an output of the planning phase, describes how the risk analyst will complete the project within the time and budget allotted. This project plan will describe research and tasks that need to be completed. It will also include dates for the various deliverables necessary. Now armed with the project plan, a stronger risk question, and a better understanding of the scope of the project, the risk analyst can begin to execute the risk analysis.

[7] Unless the decision-maker presents the concerns in the Open FAIR format and includes all relevant information, the risk question will need to have become more specific for the risk analyst to find something that can be analyzed. If the preliminary risk question was vague, the risk analyst should have worked to refine the initial assumptions through communication with the decision-maker.

5 Execute the Risk Analysis

Having completed the initiation, scoping, and planning phases, the risk analyst should have a thorough understanding of the Loss Scenario as well as a plan on how data will be found about the Loss Scenario; this data will come from historical sources.[8] With this information, the risk analyst can now begin to execute the risk analysis and make calibrated estimates. This phase of the Open FAIR risk analysis is composed of multiple steps. The necessary steps will vary depending on the purpose of the risk analysis, but regardless of purpose, every analysis will analyze the present state of risk (the *status quo*). Figure 6 depicts what steps are required for the different risk analysis purposes, which was already described in Chapter 2.

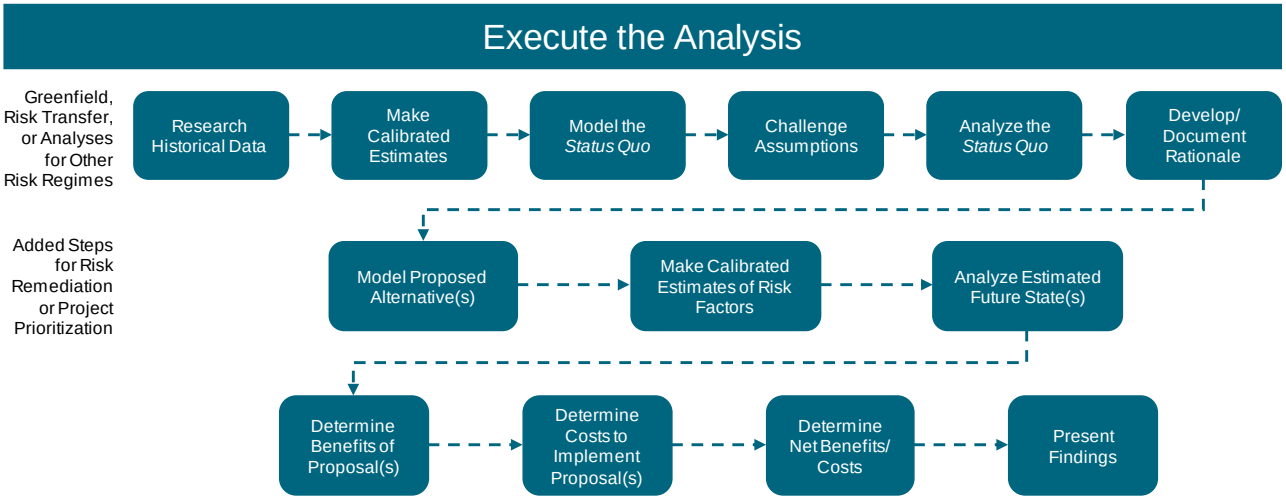

Figure 6: Steps for Risk Analysis Purposes

5.1 Model the Status Quo

The risk analyst can now begin to model the risk question. By this point, the analyst should have already decided on the Asset and the threat as well as worked to find some information and data on the Loss Scenario. This step of the execution phase involves the risk analyst determining how far into the Open FAIR risk tree to go to answer the risk question (see Figure 7).

The analyst needs to have flexibility in modeling the risk question. For instance, some scenarios may need to extend deep into the Loss Event Frequency side or Loss Magnitude side while others will only need to touch upon upper levels; if the analyst knows about Threat Event Frequency and Vulnerability, they might not need to search for information on Contact Frequency. However, if they were hoping to make an eventual change to Contact Frequency by implementing a new control to deter a Threat Agent as part of a remediation project, the analyst would need information on initial Contact Frequency and the Probability of Action to (eventually) show how the new control would affect it.

[8] Sometimes, the loss is unprecedented, so there is no data. Using calibrated estimates can provide data to use in an analysis in the absence of historical data.

Depending on the information found, the risk analyst may need to modify the assumptions made and revised earlier on. Regardless of whether changes to the assumptions are necessary, the risk analyst should document the rationale for why and how the analysis will be completed. This rationale will ultimately determine whether the conclusions in the analysis make sense when the risk analyst informs the decision-maker at the end of the analysis project.

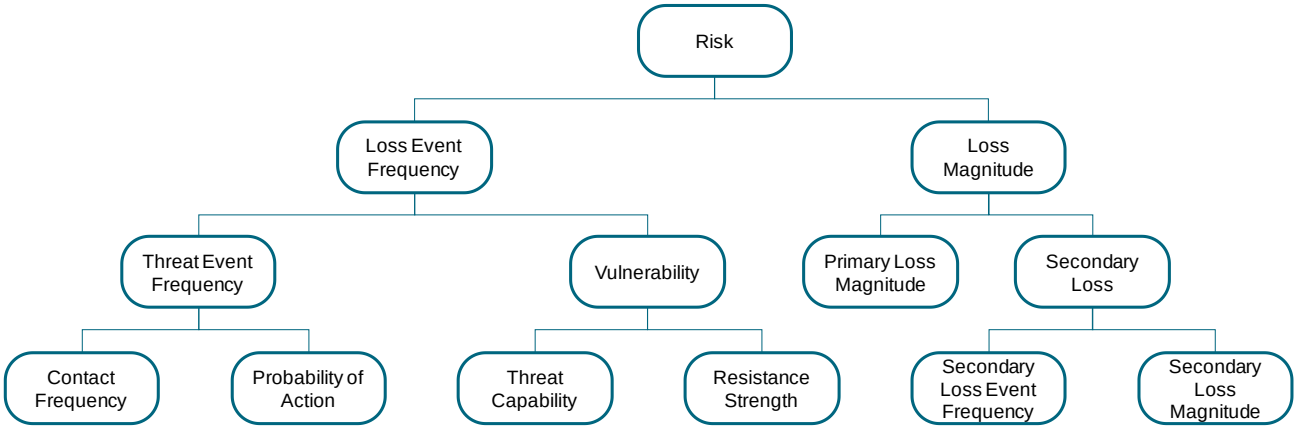

Figure 7: The Open FAIR Risk Tree

5.2 Analyze the Present State of Risk (or Status Quo)

To analyze the present state of risk, the analyst will rely upon the answers to many of the questions from above as well as additional data. This process will involve collecting data from relevant individuals, systems, etc. As mentioned earlier, the data might not be readily available, but having modeled the question, the analyst can make reasonable estimates by focusing on quantitative measures and avoiding asking questions about personal feelings. Although this data might not be perfect, through calibration and by using simulation methods such as Monte Carlo, the analyst can make the (potentially) initially absurd estimates more precise while remaining accurate.

The present state of risk is useful for determining additional action or simply for understanding the current situation. To assist the decision-maker in understanding the analysis of the *status quo*, the risk analyst should also document the rationale for the analysis at this point.

5.3 Model a Proposed Alternative

Some risk analyses will get to this step. If they do, at this point, the analyst should suggest or begin to model the already suggested alternative to the *status quo*. This alternative will depend on what was kept in mind while modeling the risk question. The analyst should be able to explain how changes to the model will be estimated as well as the reasoned arguments to explain these changes.

Therefore, the analyst would need to focus on changes to specific risk factors to show how overall risk might be affected. Changes could apply to a single control or to multiple controls. For instance, strengthening the requirements for passwords would increase Resistance Strength, which would reduce Vulnerability. Therefore, the analyst would need data on Resistance Strength both before and after the change to evaluate its effects.

5.4 Estimate the Risk of the Proposed Future State

After proposing the alternative and deciding how the model will be altered because of the new estimates, the analyst can run the model again. Because the analyst will have already identified which aspects will be changing, running the new model should include calibrated estimates for risk factors that include the proposed changes to provide an estimate of the state of risk if the proposed project is implemented. This state of risk should be directly comparable to the state of risk in the *status quo* because the analyst will have simply altered values as a result of the Open FAIR reliance upon quantitative estimates.

5.5 Evaluate the Alternative

The benefit from a change is the risk reduction expressed as a net present value as measured by the estimated (reduced) risk in the future state as compared to the present state; in other words, a project's benefits are the reduction in risk as estimated over the useful life of the proposed project. These benefits will come from the risk analyses that the analyst has run using estimates from the *status quo* and from the proposed change. The benefits will be used to help determine if the change is worthwhile.

The costs depend upon the changes that are proposed. However, they will be crucial for determining whether the proposed change is worthwhile or if the analyst should attempt to find a different remediation method that is more cost-effective. Fortunately, businesses are rather good at estimating the costs and schedule for a project. To ensure effective comparisons can be made, though, the costs must also be expressed as a net present value over the life of the project.

By describing the costs of the change as well as the benefits, the risk analyst can ensure the decision-maker understands the cost-effectiveness of the change as well as its net benefits. The net benefits ultimately provide a straightforward way for the decision-maker to understand if an alternative is worth pursuing. However, the decision-maker will need to know the rationale of the changes to the *status quo* to understand the net benefits, so the risk analyst must also document the rationale for the analysis and evaluation of the alternative.

5.6 Prepare to Inform the Decision-Maker

The next phase of a risk analysis is to inform the decision-maker of the results of the risk analysis. This will entail presenting analytical findings and a statement on the overall risk. Informing the decision-maker will also involve describing the rationale and assumptions used throughout the risk analysis, so the risk analyst must be sure that these are well documented. The purpose of the risk analysis will ultimately dictate what information the risk analyst must include and how that information is presented, but there will be common information among all the purposes, which were described in Chapter 2.

6 Inform the Decision-Maker

The final phase of every risk analysis is to inform the decision-maker. Regardless of the risk analysis purpose, the analyst should include the risk question and Loss Scenario as well as the rationale behind the analysis, the approach used to analyze the scenario, the data used to justify the analysis, and the confidence level in the results based upon the reliability of the available data.

How the risk analyst chooses to present this will depend not only upon the purpose of the risk analysis but also on personal and organizational preferences. With that said, though, the risk analyst should work to include as much information about the six interrogatives as is relevant for making an informed decision, as shown in Figure 8. With this information, the decision-maker can determine what (if anything) should be done about the current risk.

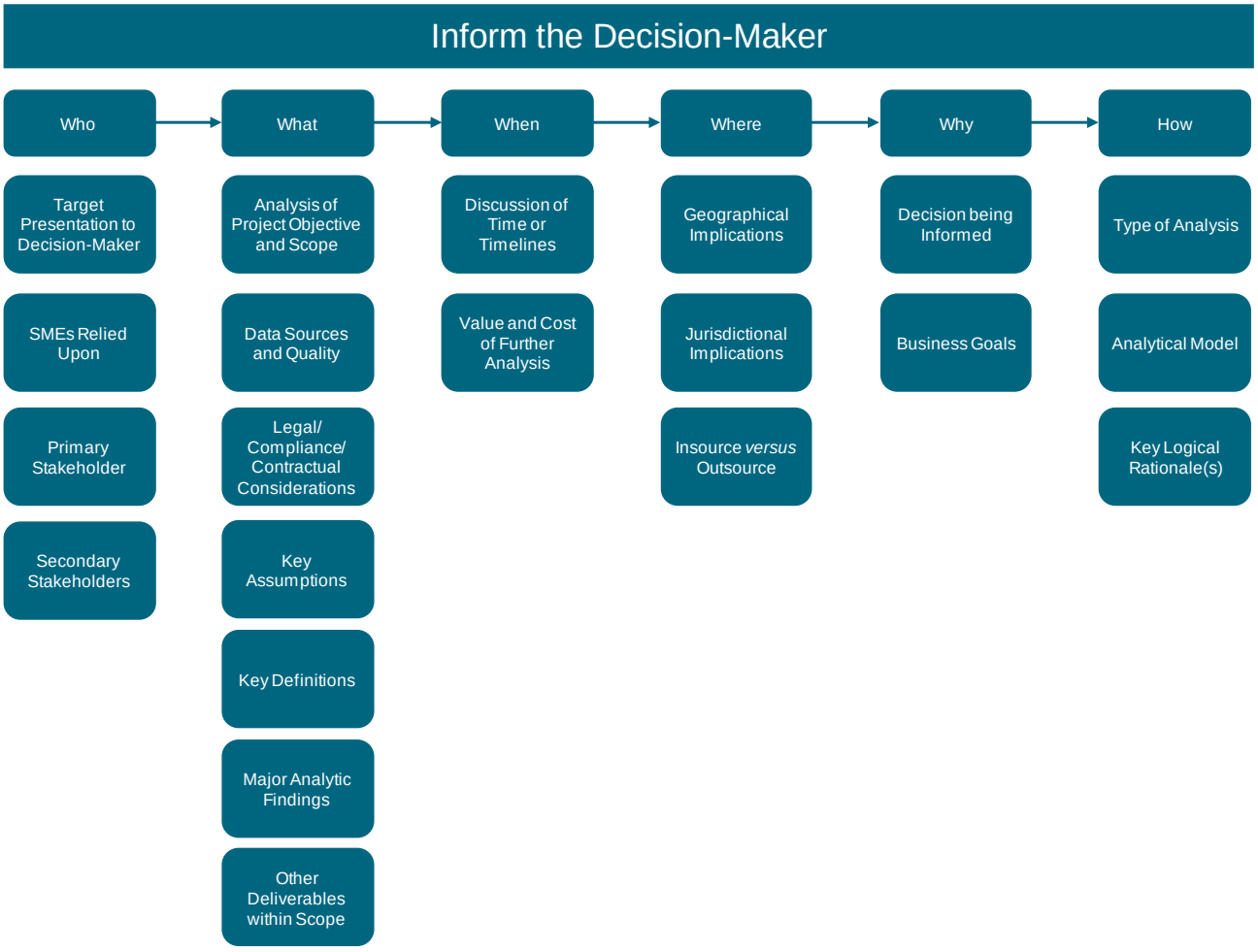

Figure 8: Communicating Risk Analysis Results

6.1 Who?

First and foremost, the risk analyst must remember the audience for the risk analysis: the decision-maker requesting the analysis. If the decision-maker is entirely unfamiliar with the Open FAIR framework, the risk analyst may need to include a brief overview in the report. If the decision-maker does not understand the Open FAIR format and process, the risk analyst can use the rationale documented throughout the analysis to help show the value of an Open FAIR risk analysis.

The risk analyst should also include any SMEs consulted during the analysis. This will allow the decision-maker to understand the analysis results and the origin of the information provided by the SMEs, as well as provide an avenue for future research or confirmation of data. Moreover, it will provide credibility to values used within the analysis, assuming they came from an SME.

The risk analyst must also include the focus of the analysis: the Primary Stakeholder(s) and Secondary Stakeholder(s).[9] As discussed earlier, the Primary Stakeholder is most likely the organization sponsoring the analysis; however, the risk analyst may have found additional or different stakeholders during the scoping process.

6.2 What?

When informing the decision-maker, the risk analyst must be sure to include the project object and scope of the analysis. The risk analyst should already have a project objective statement from the initiation phase but may need to update it if the project went in a different direction during the scoping phase. Including the project objective will allow the decision-maker to understand the goal of the analysis and whether it was reached, and including information about the scope of the project will allow the risk analyst to justify the data included.

If data did not come from an SME, the risk analyst must be sure to document their source(s). This will add credibility to the data chosen and allow the decision-maker to confirm the results of the analysis. With this, the risk analyst must also include any assumptions made during the analysis and definitions of any unfamiliar terms or values.

Finally, the risk analyst must include the overall results of the analysis. This should include legal, compliance, or contractual considerations of which the risk analyst is aware. Depending on the purpose of the risk analysis, this could also include a recommendation for what action the decision-maker should take as well as justification for the action. For instance, a Greenfield analysis simply explains the current state of risk, so offering a recommendation on it will likely not be useful; however, for an alternative prioritization or remediation project, a recommendation on what action to take may be valuable to the decision-maker.

6.3 When?

The risk analyst should include any relevant information on the time or timeliness of the analysis. For instance, if a proposed alternative would experience different costs at different points in the future, the risk analyst should describe these.

[9] If there are any Secondary Stakeholders.

If the risk analyst found that more in-depth or additional analysis would not be cost effective, justification should be included for the risk analysis performed. As stated earlier, the goal of informing the decision-maker is not to present all information found during the risk analysis but to present information relevant and valuable for making informed decisions.

6.4 Where?

If there are any jurisdictional or geographic implications in the risk analysis, the risk analyst must be sure to present them. The risk analyst should also include insourcing and outsourcing and any implications that may arise as a result.

Note that this information may not always be relevant to the decision-maker.

6.5 Why?

The risk analyst must be sure to include the purpose of the analysis when informing the decision-maker. Because the risk analyst should have confirmed the purpose of the analysis with the decision-maker earlier in the analysis, this information should not be new. However, including the purpose will allow the risk analyst to present other findings to support the purpose. The risk analyst should also include any organizational goals the risk analysis supports, if there are any of which they are aware.

6.6 How?

The risk analyst may find that an explanation is needed of how the risk analysis was performed, depending on how familiar the decision-maker is with the Open FAIR framework. If the decision-maker is completely unfamiliar with the Open FAIR framework, the risk analyst will likely need to describe how and why quantitative risk analysis was chosen instead of qualitative risk analysis. The risk analyst must also be sure to describe the analytical model used to reach the conclusions as well as the rationale behind the decisions made throughout the analysis.

6.7 Presenting Findings

The exact way the risk analyst chooses to present the findings will rely upon personal and organizational preferences. In presenting the findings, the risk analyst must always remember that the risk analysis should help the decision-maker make informed decisions that can lead to effective management. Therefore, the risk analyst should provide data that is useful for the decision the stakeholder is trying to make. In other words, the risk analyst must select and present results that are fit for the purpose of the analysis.

7 Conclusion

The stages presented above equip the risk analyst to complete an Open FAIR risk analysis. The Open FAIR risk analysis framework and taxonomy provide the risk model that can be used to make meaningful measurements. In turn, these measurements allow effective comparisons that act as the basis for well-informed decisions and, in turn, guide effective management of risk.

By ensuring sufficient preparation goes into initiating and scoping the analysis, the risk analyst works to ensure that the results from the analysis directly address the concern of the decision-maker.

However, the risk analyst must consider that there are diminishing returns to gathering more data, investigating more data, and drilling deeper into the Open FAIR taxonomy. The risk analyst must ultimately ensure that the results presented are usefully precise to the decision-maker.

Moreover, the risk analyst may find it valuable to consider an organization's capacity for loss and management's tolerance for loss when informing the decision-maker, though this will ultimately depend on the purpose of the analysis and whether those details are available to the risk analyst.

If risk qualifiers are present, the risk analyst must also be sure to convey them when informing the decision-maker. This is critical to ensure that the decision-maker understands that there may be some subtle distinctions in the quantitative results that could ultimately impact how the decision-maker uses the analysis.

While the risk analyst will have avoided using ordinal scales as inputs in the risk analysis, the decision-maker may wish or require that quantitative results are conveyed using qualitative statements. This may require further consultation with management to ensure that the scales used have their approval and are understood by all parties involved; note that it is inappropriate for the risk analyst to define and use qualitative scales that represent a personal tolerance for loss or a personal interpretation of what is believed to be the organization's tolerance for loss.

Finally, the risk analyst should be prepared to defend the results of the analysis. This may involve revisiting any and all assumptions and rationale that were documented during the analysis process; it may involve diving deeper into the Open FAIR taxonomy to provide estimates of lower-level risk factors; or it may involve completing one or more additional analyses to compare results from different input data or assumptions.

Index

actionable project plan..... 20
annual loss exposure..... 4
Asset..... 9
clarifying questions 13
execution phase 21
Greenfield analysis..... 4
initiate phase..... 7
insurance..... 4
Loss Scenario 17
model the risk question..... 21
Monte Carlo..... 4
Monte Carlo simulation..... 22
planning phase..... 19
Preliminary Asset 13
preliminary project plan 10, 11
preliminary risk question..... 11
present state of risk..... 22
Primary Stakeholder..... 9, 13
project objective statement..... 11
proposal..... 5
ransomware attack..... 8
remediation project..... 5
Resistance Strength..... 16
resources..... 10
risk analysis..... 2
risk analysis phases 2
risk question 8
risk regimes..... 5
scoping phase 12
Threat Agent 9, 14
Threat Community 14
Threat Event..... 10
threat metrics..... 15
threat vector..... 15
time and budget..... 10
transfer risk 4