Open Group Guide

Open FAIR™ Risk Analysis Process Guide

Open Group Guide

Open FAIR™ Risk Analysis Process Guide

ISBN: 1-947754-06-5

Document Number: G180

Published by The Open Group, January 2018.

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

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

or by electronic mail to:

ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 550 organizations includes customers, systems and solutions suppliers, tools vendors, integrators, academics, and consultants across multiple industries.

The Open Group aims to:

- Capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- 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/library.

This Document

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

This Guide 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 Risk Analysis (O-RA) and Risk Taxonomy (O-RT) Open Group standards (see Referenced Documents). Moreover, the Guide assumes the analyst has done some form of qualitative analysis.

The appendices of this Guide include a blank analysis worksheet template. Also included is a completed worksheet template for a sample Open FAIR risk analysis undertaken to serve as an example. This risk analysis write-up is published as its own White Paper: Putting Open FAIR™ Risk Analysis Into Action (see Referenced Documents).

Trademarks

Acknowledgements

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

- John Linford, San Jose State University, principal author of the body of the Guide (Chapter 1 through Chapter 7)
- Eva Kuiper, DXC Technology, principal author of the templates in Appendix 5.2 and Appendix B
- Mike Jerbic, San Jose State University, team leader and contributor of the diagrams in Chapter 1 through Chapter 7
- John “Jay” Spaulding, Director of The Open Group Security Forum
- And the Member Organizations and their Representatives of The Open Group Security Forum who reviewed this document

Referenced Documents

The following documents are referenced in this Guide.

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

- FAIR – ISO/IEC 27005 Cookbook, an Open Group Guide (C103), November 2010, published by The Open Group; refer to: www.opengroup.org/library/c103
- Putting Open FAIR™ Risk Analysis Into Action: A Cost-Benefit Analysis of Connecting Home Dialysis Machines Online to Hospitals in Norway, White Paper (W176), May 2017, published by The Open Group; refer to: www.opengroup.org/library/w176
- Risk Analysis (O-RA), an Open Group Standard (C13G), October 2013, published by The Open Group; refer to: www.opengroup.org/library/c13g
- Risk Taxonomy (O-RT), Version 2.0, an Open Group Standard (C13K), October 2013, published by The Open Group; refer to: www.opengroup.org/library/c13k
- The Open FAIR™ – NIST Cybersecurity Framework Cookbook, an Open Group Guide (G167), October 2016, published by The Open Group; refer to: www.opengroup.org/library/g167

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 Guide 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 Guide also provides many questions for risk analysts to answer before doing any analysis.

2 Defining the Purpose of Risk Analyses

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 "Greenfield" risk analysis of the current state or *status quo*
- 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 Guide and are depicted in Figure 1.

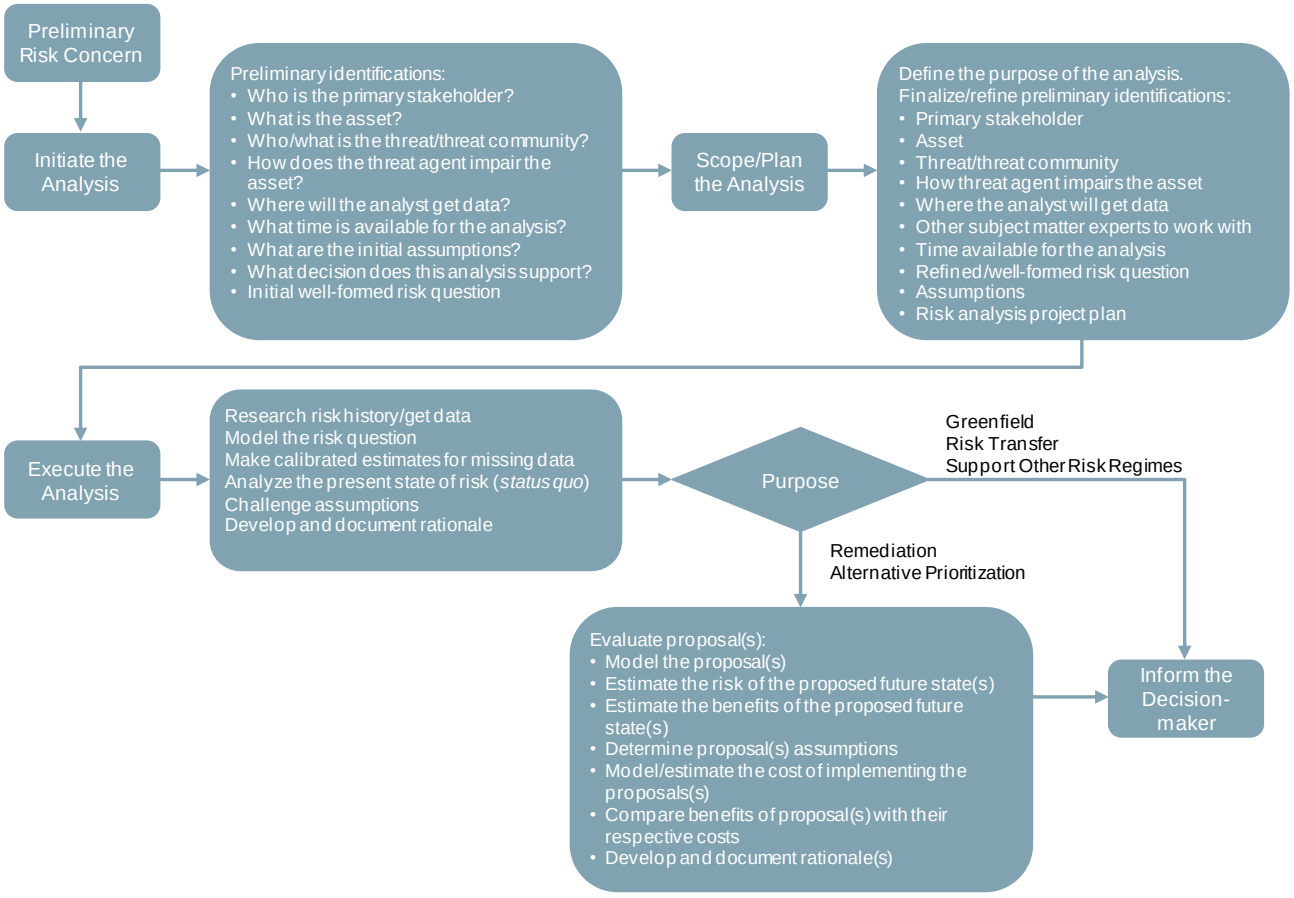

Figure 1: Open FAIR Analysis Process Flow Chart

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.

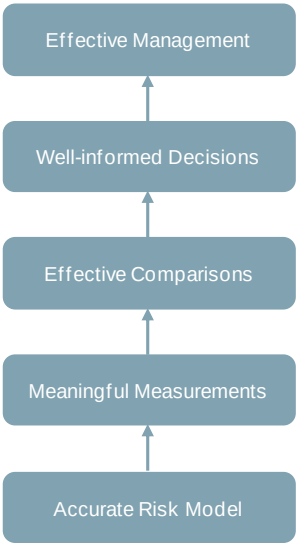

Figure 2: The Open FAIR Risk Stack

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 perform 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 just be used 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 need to 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 that 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[1] 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. 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. Fortunately, there are already the FAIR – ISO/IEC 27005 Cookbook and the Open FAIR™ – NIST Cybersecurity Framework Cookbook (see Referenced Documents) that the risk analyst can use to understand how these standards complement each other. 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.

2.5 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 risk scenarios and mitigation options. Therefore, a decision-maker can compare multiple Open FAIR risk analyses to determine which projects are worth pursuing or are most worthwhile to the decision-maker.

Management will likely focus on those projects 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

[1] ISO/IEC 27001:2013: Information Technology – Security Techniques – Information Security Management Systems – Requirements.

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 risk scenario for management to use when deciding how to address it.

If management has more than one risk scenario but only wants to mitigate the greatest risk, the analyst can create a portfolio of risk 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 risk 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 risk 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 while informing the decision-maker. Chapter 7 follows the same steps and organization as Chapters 3, 4, and 5, but describes a sample risk analysis that is published as its own White Paper: Putting Open FAIR™ Risk Analysis Into Action (see Referenced Documents). This White Paper serves to show an example of informing the decision-maker, which is the focus of Chapter 6.

3 Initiating a 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. However, the risk concern is usually vague and rarely presented in the Open FAIR format of loss event frequency and magnitude. For instance, a generic concern of a decision-maker could be as simple as "I saw several firms in my industry were hacked; 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 risk 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 Guide 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 risk scenario, and the information needed to form the project objective statement as well as the preliminary risk question.

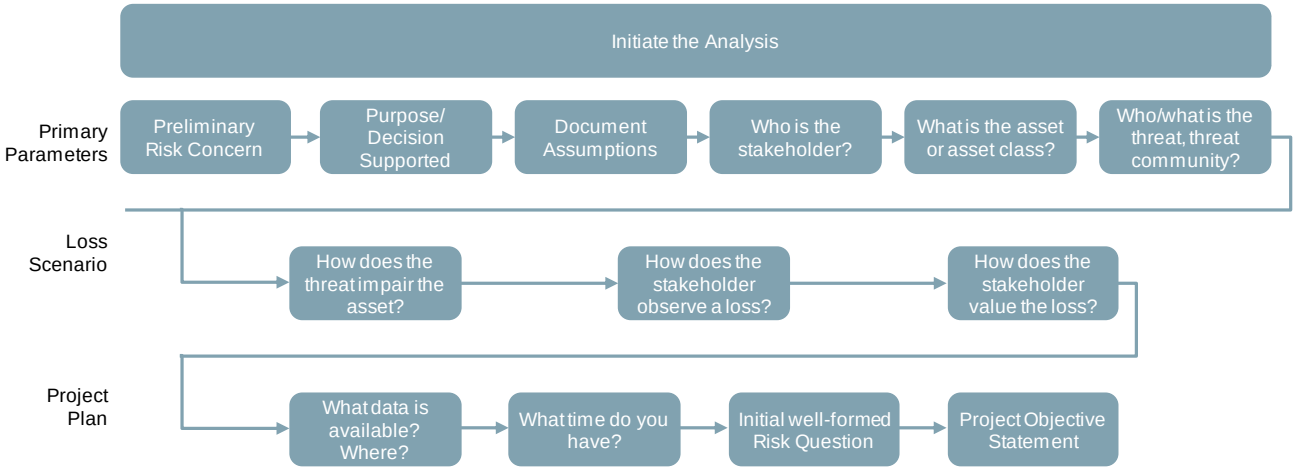

Figure 3: Initiation Phase Steps

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 risk 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 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/community also includes people who may or may not realize they could impair or compromise the asset.

As the risk 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/community will be more specific than others, which will require initiating a separate analysis for each newly defined threat agent/community.

3.4 Identify How the Asset can be Impaired or Compromised

Threat agents can act in a wide variety of ways to impair or compromise the asset. 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 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 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 company 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?".[2] 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 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 risk 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.

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

4 Scoping and Planning a 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 risk 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.

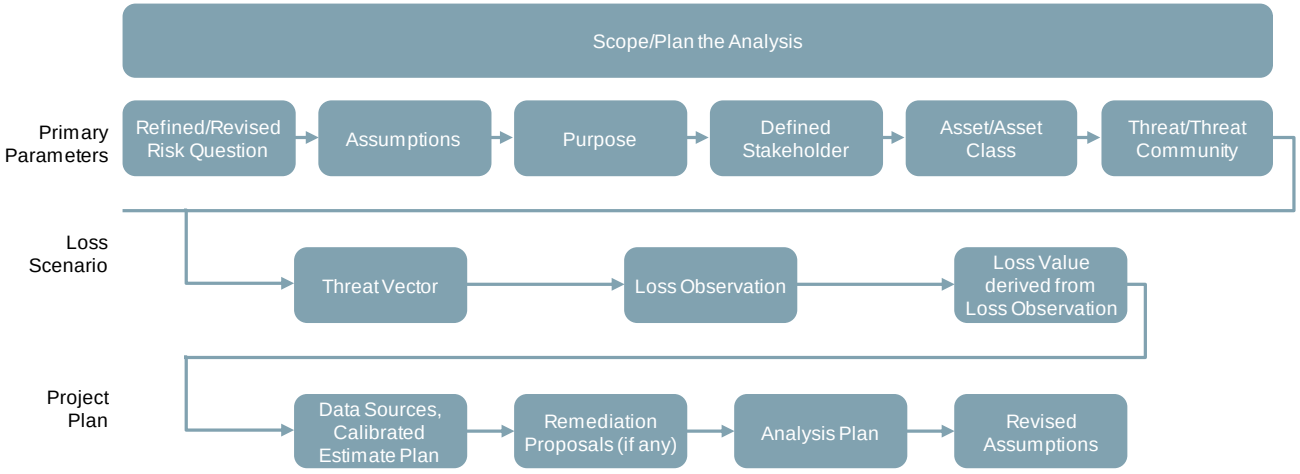

Figure 4: Scoping and Planning Phase Steps

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)/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 could impact the asset, 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.

Throughout the scoping process the risk analyst must stay in consistent communication with the decision-maker. During the scoping process, the analyst may find that an alternative threat is of greater concern, so the risk analyst would need the approval of the decision-maker to change focus, even for a small change, because all changes will affect the risk question and, therefore, the entire risk analysis.

Before beginning the scoping phase, though, 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 as well as begin to consider the various factors. 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, committed 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 company 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 a company. 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 that Needs to be Protected and for which Losses Need to be Calculated?

The analyst should have already identified a preliminary asset. Depending on the concerns of the decision-maker, the asset may need additional definition. 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, 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. 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 risk scenario(s) better, this asset can become more specific.

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, which will be discussed later in this section. The analyst should consider the company 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 company's ability to make decisions about risk.

Because the asset is a fundamental part of loss, the analyst should understand information including 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 What is the Threat Agent or Threat Community that could Impair or Compromise the Asset?

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 community will act directly against the asset, and "rational" human threat agents will act against these assets to accomplish an objective 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. 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 1 depicts some examples of various threats possible.

Table 1: Threat Examples

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

Human		Malware	Event/Circumstance Beyond Control
Internal	**External**		
Non-Privileged	Technical Amateur		Animals
	Non-Technical Professional		Flooding
	Non-Technical Amateur		

Although the Open FAIR framework does not specifically address threat actions, 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, and the ability of the threat agent or 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 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 How does the Threat Agent or Community Act upon the Asset to Impair or Compromise it?

The answer to this question describes the loss event(s) and part of the loss scenario(s). Specifically, this question seeks to understand the specific method that the threat agent will use to impair the asset, also known as the threat vector. The threat vector chosen by the threat agent will ultimately depend upon the controls used by the company. Controls in the Open FAIR framework are those things that will contribute to the ability to resist the actions of a threat agent or community. The Open FAIR framework specifies four categories of controls: avoidance, deterrent, vulnerability, and responsive.

Resistance strength, which is a vulnerability-related control, 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 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 are 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 done using common and comparable units, meaning numerous analyses can be compared and costs can be discussed and contrasted without difficulty, thereby allowing the analyst to address more easily the concerns of the decision-maker. 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 describe clearly 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 6) 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 company 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 actually 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 sequence of events caused by the threat agent that leads to an observable

loss. This loss scenario essentially is the story of how the loss will occur. 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 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 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.

Table 2 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 2: Open FAIR Six Forms of Loss

Forms of Loss	
Productivity	The reduction in an organization's ability to generate its primary value proposition (e.g., income, goods, services, etc.).
Response	Expenses associated with managing a loss event (e.g., internal or external person-hours, logistical 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, etc.).
Competitive Advantage	Losses associated with diminished competitive advantage. Competitive advantage loss is specifically associated with assets that provide competitive differentiation between the organization and its competition (e.g., trade secrets, merger and acquisition plans, etc.).
Fines/Judgments	Legal or regulatory actions levied against an organization. Note that this includes bail for any organization members who are arrested.
Reputation	Losses associated with an external perception that an organization's value proposition is reduced or leadership is incompetent, criminal, or unethical.

In an Open FAIR risk analysis, the probability of a primary loss event and the losses attributed to that event actually 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.

Continuing the hypothetical risk scenario, a tornado causing a power outage that prevents devices from communicating would likely face all three of the primary losses: the company 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 Guide 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 actually understand what additional work is necessary to complete the risk analysis project. This means the risk analyst should understand where the necessary information 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.[3] Therefore, the outputs of the scoping phase of the risk analysis are the threat agent/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 loss scenario.

If the decision-maker prefers a shorter version of the risk question, the risk analyst can swap "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

[3] 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.

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.

5 Performing 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.[4] 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 5 depicts what steps are required for the different risk analysis purposes, which was already described in Chapter 2.

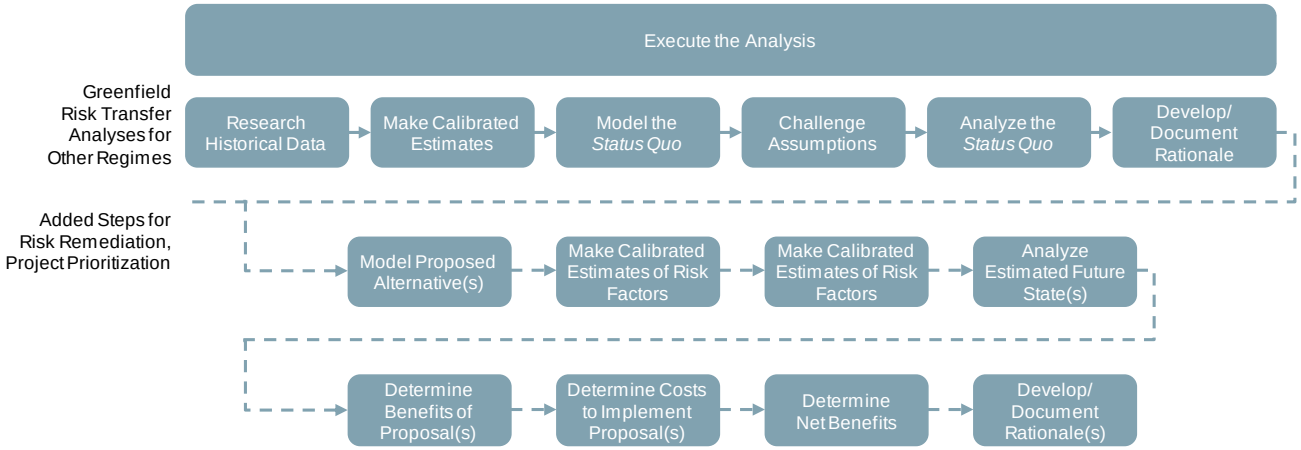

Figure 5: Steps for Risk Analysis Purposes

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 6).

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 Management 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.

[4] Sometimes, the risk 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.

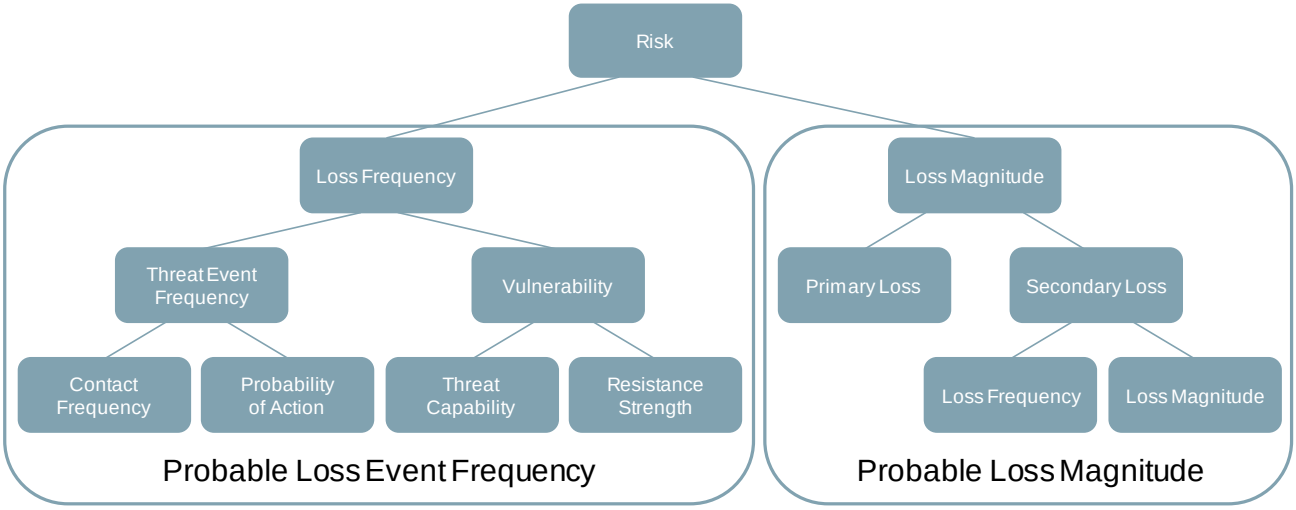

Figure 6: The Open FAIR Risk Tree

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 an 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 specific control (e.g., avoidance, deterrent, vulnerability, responsive) or 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 be rather straightforward and should include calibrated estimates for risk factors that include the proposed changes. Rerunning the model provides 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 result of 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 documented well. The purpose of the risk analysis will ultimately dictate what information the risk analyst must include, 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 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 company 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 7. With this information, the decision-maker can determine what (if anything) should be done about the current risk.

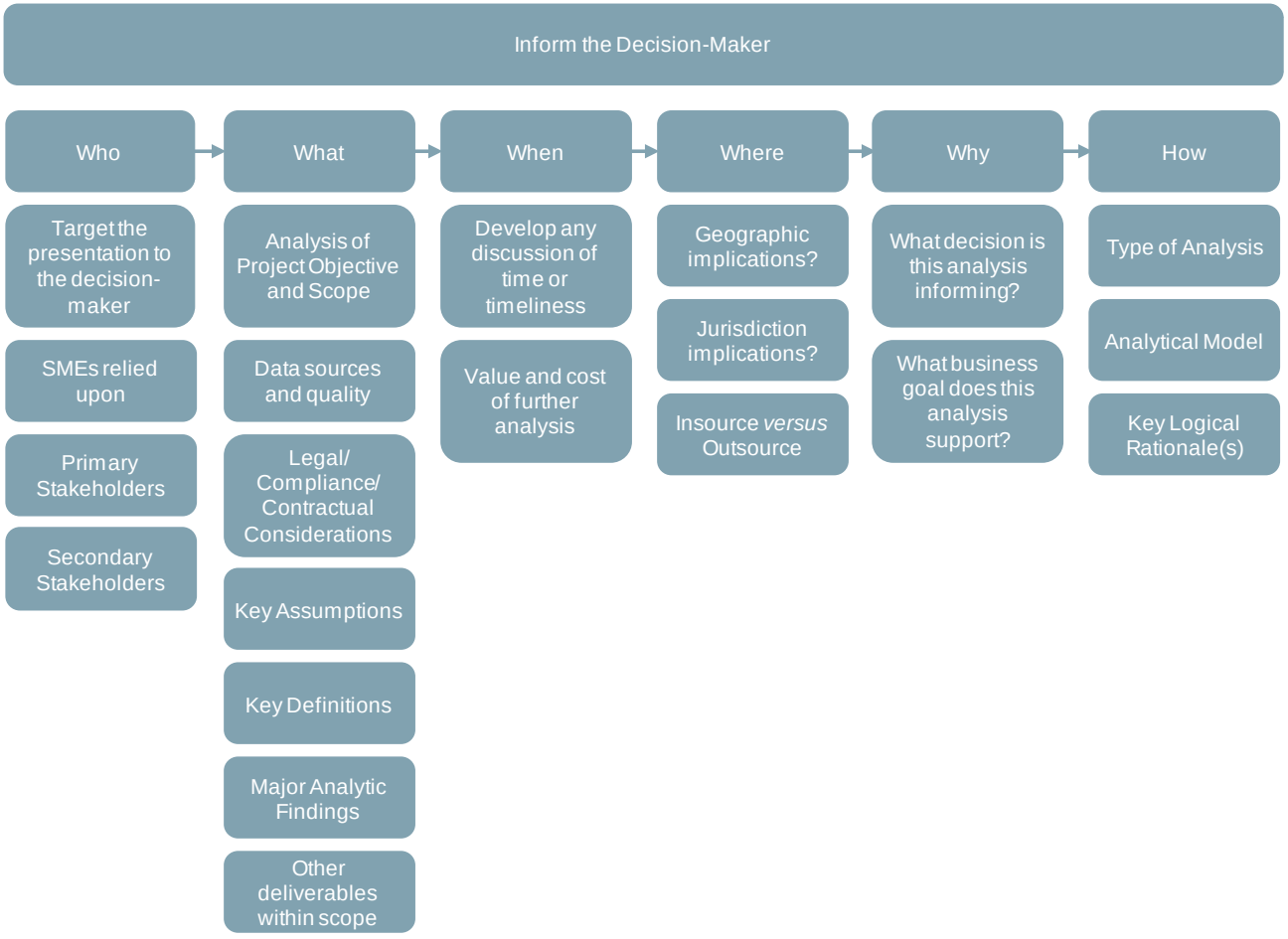

Figure 7: Communicating Risk Analysis Results

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).[5] 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 its source.. 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 be pointless; 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.

[5] 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 when informing the decision-maker. 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?

The risk analyst may find that this information is not relevant to informing the decision-maker. However, 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.

6.5 Why?

The risk analyst must also 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 business 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 company 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 must consider if the information included is relevant to making informed decisions.

7 Stepping through a Risk Analysis Scenario

This chapter will walk through a sample Open FAIR analysis. It will go through the process of completing the analysis and explain how the analysis might look if it were done for several of the purposes described in Chapter 2. This chapter will use the same analysis throughout, but it will continue to add information as necessary. The example analysis falls between a quantitative and qualitative analysis to showcase the use of the process phases rather than to demonstrate how to perform Open FAIR calculations.

This example analysis follows the process undertaken by the risk team doing the analysis, and it accounts for changes in information when the team learned about them. Section 7.1 follows Chapter 3 and documents the project initiation phase; Section 7.2 follows Chapter 4 and documents the scoping and planning phases; Section 7.3 follows Chapter 5 and describes the execution phase; and Section 7.4 is the inform stage, and it contains the link to the White Paper: Putting Open FAIR™ Risk Analysis Into Action (see Referenced Documents).

The project originated from The Open Group Healthcare Forum. It came from an Enterprise Architect who works for a company that contracts with one of the Norwegian Regional Healthcare Authorities and who saw inefficiencies with the current method of treatment. This risk analysis was performed only to be an example for this Guide.

The Enterprise Architect presented the following scenario to the risk team at the beginning of the project. Some of the information in this scenario did eventually change, but it will be specified when that occurs.

> The Regional Healthcare Authority (RHA) in Norway has a choice: it can allow patients to complete much needed dialysis treatments at the hospital, or it can allow patients to complete dialysis at home.
>
> With improvements in technology, home dialysis is becoming much more common and offers a cheaper alternative to in-center treatment. Currently, only 200 of the 1,350 people in Norway receiving dialysis treatment complete the treatment at home instead of the hospital. The cost for completing dialysis treatment at the hospital three times a week for four hours per treatment is roughly between $148,000 and $316,000 per patient. However, it is estimated that allowing patients to complete dialysis at home would save 30,000 USD *per capita*.
>
> Patients currently completing dialysis treatment at home must download their treatment plan data onto a memory stick and bring it to the nearest hospital or satellite clinic. An alternative to this method would be for patients to use the Internet to send their dialysis treatment plans to their respective doctors/physicians, who could then examine the data and update the treatment plans accordingly. However, the RHA is concerned about potential losses of privacy from allowing patients to do this, despite the fact the Norwegian RHA already has a VPN (Virtual Private Network) solution in place and could feasibly encrypt both ends of the connection. Specifically, the RHA is concerned the connection could be utilized to upload malware or ransomware into the systems of hospitals and/or satellite clinics.

7.1 Initiate the Risk Analysis Project

The first step to completing any risk analysis is to initiate the project. As described in Chapter 3, the risk analyst/team must answer some initial questions before attempting to begin the analysis. These questions allow the risk analyst/team to put the information from the decision-maker's

concerns into the Open FAIR format, which will then inform the analyst/team on what information is missing and needs to be found while scoping the risk analysis.

7.1.1 Identify the Primary Stakeholder

Given the risk scenario above, the primary stakeholder for this analysis seems decently straightforward: the Norwegian RHA is the primary stakeholder. In other words, the risk analysis will be from the point of view of the RHA. Moreover, the RHA is the entity that would suffer a loss from a malware or ransomware attack.

However, the RHA is not the only primary stakeholder. Rather, it is one of two primary stakeholders. The scenario describes that the RHA authorities are concerned about losses to patient privacy, which means patients are the other primary stakeholder. As a result, at least two separate Open FAIR analyses are needed to account for the two different perspectives. For the second risk analysis, the primary stakeholder is any dialysis patient completing dialysis treatment at home rather than at a hospital or satellite clinic.

7.1.2 Identify the Asset or Asset Type

For this analysis, information on the threat was provided in the risk scenario. As a result, the risk team decided to use it to identify assets that could be affected. A malware or ransomware attack focuses on the confidentiality, integrity, and availability of information assets; more specifically, ransomware targets the availability aspect, and malware targets all three aspects. These attacks target hospital information and effectively prevent the RHA from using it to treat patients and provide needed medical assistance. As a result, the asset would be the actual information assets in the RHA's possession.

For the patient privacy concern, the risk team initially assumed the asset would be the medical records themselves. However, this initial assumption changed during the scoping phase and is described in Section 7.2.1.1.2.

7.1.3 Identify the Threat Agent or Threat Community

Initially, the risk team assumed a threat agent using a malware/ransomware attack would be financially motivated criminals. For the patient privacy concern, the risk team assumed, too, that the threat agent would be financially motivated; however, this assumption would also change and was merely a starting point for the analysis.[6]

7.1.4 Identify How the Asset can be Impaired

Given that ransomware is a more extreme form of malware, how the asset (information system availability) is impaired will be much the same for ransomware and malware attacks. For either attack type to be successful, the threat agent must plant the virus in the hospital's systems. At this stage, the team had not yet conducted additional research on how the virus might be planted, but it had decided on initial possibilities.

[6] The risk team was mainly based in the US and had the most experience with the US healthcare system. As such, the team's assumptions were first based on motives for US-based threat agents targeting the US healthcare system.

7.1.5 Identify Available Resources and Information Sources

The risk team consisted of Mike Jerbic, a lecturer in the economics department at San Jose State University in California, and Sushmitha Kasturi, a recent graduate from the economics department at San Jose State.

The team received assistance from Biljana Strageland, PhD, who gathered information on the status of home dialysis in Norway and several other countries, helped with some medical information, and assisted with translating documents from Norwegian to English for the risk team. The risk team also communicated regularly with Stig Hagestande, who is the Enterprise Architect mentioned earlier and who, as his normal job, worked with the Norwegian RHA throughout the project.

The risk team relied on peer-reviewed research and studies whenever possible. It also utilized industry reports when they were available. However, ransomware attacks are a relatively new trend, so the team experienced a subsequent lack of much data.

7.1.6 Identify Time and Budget Constraints

The risk team received the project in July 2016 and set an initial target to complete the risk analysis project in roughly six months. However, The Open Group projects are undertaken by volunteer members working full-time in other capacities, so although the team wanted to complete the project in six months, it accepted a flexible schedule based upon the "best efforts" of its contributors, consistent with most Open Group volunteer member projects. Moreover, as a project whose purpose was to exemplify an analysis for this Guide, the budget available for this project was negligible.

7.1.7 Create a Preliminary Risk Question

The preliminary risk question(s) should contain as much information as possible to ensure the risk analysis is as focused as possible from the very beginning. Using the information known so far, the risk team formed the following preliminary risk questions. These risk questions will be refined in the scoping phase of the risk analysis, so they are currently missing information needed to conduct the risk analysis.

- What is the risk associated with a malware attack on the Norwegian RHA by compromising a home dialysis machine through the connection between it and hospitals/satellite clinics?
- What is the risk associated with a ransomware attack on the Norwegian RHA by compromising a home dialysis machine through the connection between it and hospitals/satellite clinics?
- What is the risk associated with compromising control of patient medical records due to an exploitation of the connection between home dialysis machines and hospitals/satellite clinics?

Clearly, the first and second risk preliminary risk questions are nearly identical: the only difference between them is how specifically malware is defined, with ransomware being the more specific form of malware. The third preliminary risk question is included to show that there are three feasible risk analyses present, even though the risk team eventually decided not to conduct all three analyses.

7.1.8 Exit the Initiation Phase

At this stage, the risk team had a rough idea of how long it would take to complete the risk analysis as well as where it would find the information necessary to complete it. Moreover, the risk team had formed preliminary risk questions that it would refine through scoping in the next project phase. It had also created a project objective statement:

- To analyze the information availability, integrity, and confidentiality risk to the Norwegian Health Authority from malware and ransomware and the privacy risk to the people Norway of connecting home dialysis machines online to hospitals in six months with a team of volunteer analysts and no financial budget

7.2 Scope and Plan the Risk Analysis

Using the information provided and categorized, the risk team could begin scoping and planning the risk analysis. It had the groundwork for its analyses in place and a general understanding of what research might be necessary as well as a very rough project plan for completing the project and successfully informing the decision-maker. To simplify things, the risk team decided to combine the first two risk questions and address them at the same time:

- What is the risk associated with a malware/ransomware attack on the Norwegian RHA by compromising a home dialysis machine through the connection between it and hospitals/satellite clinics?
- What is the risk associated with compromising control of patient medical records through an exploitation of the connection between home dialysis machines and hospitals/satellite clinics?

7.2.1 Scope the Risk Analysis

At this phase, the risk team had a decent understanding of what was left to be done to complete the risk analysis in the time it had set for itself. Therefore, it was ready to scope the risk analysis. The first step of this phase is to answer clarifying questions.

7.2.1.1 Answer Clarifying Questions

As expected, many of these questions are similar to the questions in the initiation phase; however, these questions rely on the risk analyst/team researching the decision-maker's concern, which could yield new or unexpected information that alters the risk analysis.

7.2.1.1.1 Who is the Primary Stakeholder?

As stated earlier, the primary stakeholder for the first risk question appears to be the Norway RHA. However, it is possible to be more precise about defining the primary stakeholder. Specifically, the primary stakeholder for a malware/ransomware attack is the RHA itself, a hospital, a physician's office, or any other facility that directly interacts with the patient in delivering dialysis treatment and care.

For the patient privacy concern, the primary stakeholder has not changed: it is still the patients.

7.2.1.1.2 What is the Asset or Asset Type that Needs to be Protected and for which Losses Need to be Calculated?

Ransomware and malware attacks both target the confidentiality, integrity, and availability of information assets. A ransomware attack, in particular, would prevent a hospital or satellite clinic from accessing patient records, treatment data, medication information, etc.

In meetings with the Enterprise Architect, the risk team learned that the RHA was concerned with the theft of medical records, so for the analysis focusing on patient privacy concerns, the asset would be patients' control of their medical records and information, not the medical records themselves, as was previously assumed. The specific privacy risk to information is the control over who can read that information and tie that information to a specific, personally identifiable patient.

7.2.1.1.3 What is the Threat Agent or Threat Community that could Impair the Asset?

Using the information gathered while initiating the risk analysis, the risk team continued the assumption that the malware/ransomware threat agents would be financially motivated. This follows from reports on ransomware attacks both in the US and in other countries. Moreover, the risk team determined that the threat agent was likely external to the hospital, for any internal threat agent would achieve a data manipulation or theft objective utilizing a threat vector easier than penetrating a home dialysis machine.

However, in the United States, most medical record theft is completed to attempt insurance fraud. This is the result of the healthcare system that the US has in place.[7] In contrast, the Norwegian healthcare system operates differently: it is a "single-payer system", which means the government pays for most medical treatments. Moreover, the threat agent would specifically be accessing dialysis treatment data, which contains little to no information possible of generating revenue for a threat agent.

Therefore, at this point, the risk team decided to no longer expend resources on the patient privacy analysis: without motivation, the risk to patient privacy was purely speculative, meaning risk was possible, but highly improbable. The team decided instead to focus entirely on the malware/ransomware analysis; this example scenario will also no longer include information on the patient privacy analysis and will only focus on the malware/ransomware analysis.

7.2.1.1.4 How does the Threat Agent or Community Act upon the Asset to Impair the Asset?

Ransomware attacks do exactly as their name implies: they hold systems ransom. If a ransomware attack were successfully completed, the RHA would either need to pay the attackers to release hospital systems and restore access or need to recover the hostage information through its backup and restore capability. A malware attack can work in much the same way, especially given the motivation identified by the risk team.

Given that the analysis is still focusing on the *status quo*, which does not involve any connection between a home dialysis machine and the RHA, the threat agent might attempt to initiate an attack using a memory stick. Currently, home dialysis patients transport their treatment plans to and from hospitals and satellite clinics on a memory stick. However, this threat vector would involve switching the memory stick of a patient with one containing a virus. The original scenario presented to the risk team assumed that patients would be going to and from a hospital or satellite clinic two to three times per week, which was roughly how often patients complete dialysis at a hospital or satellite clinic.

[7] As stated already, the majority of the risk team was based in the United States and so was familiar with the US medical system.

However, the risk team learned that dialysis patients completing their treatments at home only visit their doctor to have treatment plans updated every few weeks; some patients may need to have their plans updated more frequently, but others reportedly only need their treatment plans updated every six weeks, which is about how often patients visit their doctors for routine check-ups while on dialysis. As a result, swapping a patient's memory stick with one containing the malware or ransomware would only have a chance at being successful once every several weeks.

A more likely method of attack would be to use the connection between home dialysis machines and the hospital or satellite clinic, assuming the patient had the connection established. The threat agent could then use the connection to plant the malware or ransomware. As stated in the scenario, though, the dialysis machine could be connected to the hospital using a VPN, and the hospital could easily encrypt both ends of the connection.

Through brief discussion with a manufacturer of home dialysis machines capable of connecting to a network, the risk team also learned that an additional security measure could easily be implemented: a cloud-based "drop box" of sorts could be set up to accept treatment data from the machines. The patients would not need to do much more than press a button to transmit the data, and the doctors would merely need to access the cloud storage to view and edit treatment data.

7.2.1.1.5 How does the Asset's Owner Know that the Asset has been Compromised?

For a ransomware or malware attack, the asset owner would be able to tell rapidly, if not immediately, if an attack had successfully impaired the asset. As noted above, a successful ransomware attack will prevent hospital staff and physicians from accessing their systems. Only once the ransom has been paid – typically through the transfer of a cryptocurrency – or the RHA had restored its systems using data stored elsewhere could the staff and physicians regain control of their systems.

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

The RHA would certainly face productivity and response losses from an attack. It could potentially face fines and judgments; however, given the nature of Norway's healthcare system, these costs are unlikely. The RHA would have replacement costs, too, if it attempted to restore its systems by copying good data in from a data point that was known to be secure or if it simply paid the ransom; its decision on which option to choose would ultimately depend on the costs incurred due to the extent and method of the attack.

7.2.1.1.7 Where will you Find Information on the Loss?

Information on losses came from studies done by companies in the industry as well as from peer-reviewed journal articles. The risk team also relied on contributions from Biljana Strageland, who translated documents from Norwegian to English for the risk team and communicated with European sources to find information unavailable to the US-based risk team members. The team focused on publicly available, no cost publications, research, and other information sources.

7.2.1.2 Describe the Loss Scenario

At this point, the analysis is still describing the *status quo*, which means the home dialysis machines are still not connected to the Norwegian RHA. Regardless, the loss scenario involves the use of malware/ransomware to prevent the RHA from being able to access its systems. Given the scenario described at the beginning, a threat agent would likely need to replace a patient's memory stick containing his/her treatment plan with one containing the malware/ransomware.

Once the memory stick is inserted in a computer at the hospital, the virus would enter the system and encrypt the files until the ransom is paid, at which point the files would be decrypted and the RHA would once again have control of its files.

The RHA would undoubtedly face productivity and response costs. It could also face replacement costs if it attempted to restore its systems using known good data instead of paying the ransom. However, the RHA could also face fines and judgments, depending on the reaction of the Norwegian government. As noted earlier, though, the Norwegian healthcare system is a single-payer system, so the response of the Norwegian government is uncertain.

7.2.2 Plan the Risk Analysis

As said earlier, the risk team received the project in July 2016 with a six-month target schedule, and The Open Group projects are undertaken by people working full-time in other capacities.

The team planned to spend roughly 15% of its time working on this project and met weekly. The final deliverables for this project were a concise White Paper documenting the analyses: Putting Open FAIR™ Risk Analysis Into Action (see Referenced Documents), and a presentation to be presented at an Open Group event.

7.2.3 Exit the Scoping and Planning Phases

At this stage, the risk team had enough information to understand what it would be analyzing and how to revise the risk questions, meaning the team ensured the risk questions contained proper Open FAIR terminology and structure. The scoped risk question is still a combination of the first two preliminary risk questions due to the risk team finding that malware and ransomware threat agents have similar motivations and threat vectors.

- What is the probable frequency and probable magnitude of future loss associated with a financially motivated threat agent launching a malware/ransomware attack on the Norwegian RHA by compromising the connection between home dialysis machines and hospitals/satellite clinics?

At this stage, the scoping phase, the privacy question was analyzed sufficiently to determine that the risk associated with privacy loss was negligible and did not warrant further inquiry.

7.3 Execute the Risk Analysis

7.3.1 Model the Status Quo

In modeling the risk question, the risk team considered the Open FAIR risk tree (Figure 8). Due to the Open FAIR framework relying on a top-down approach, the risk team did not need to begin at the lowest levels of the tree.

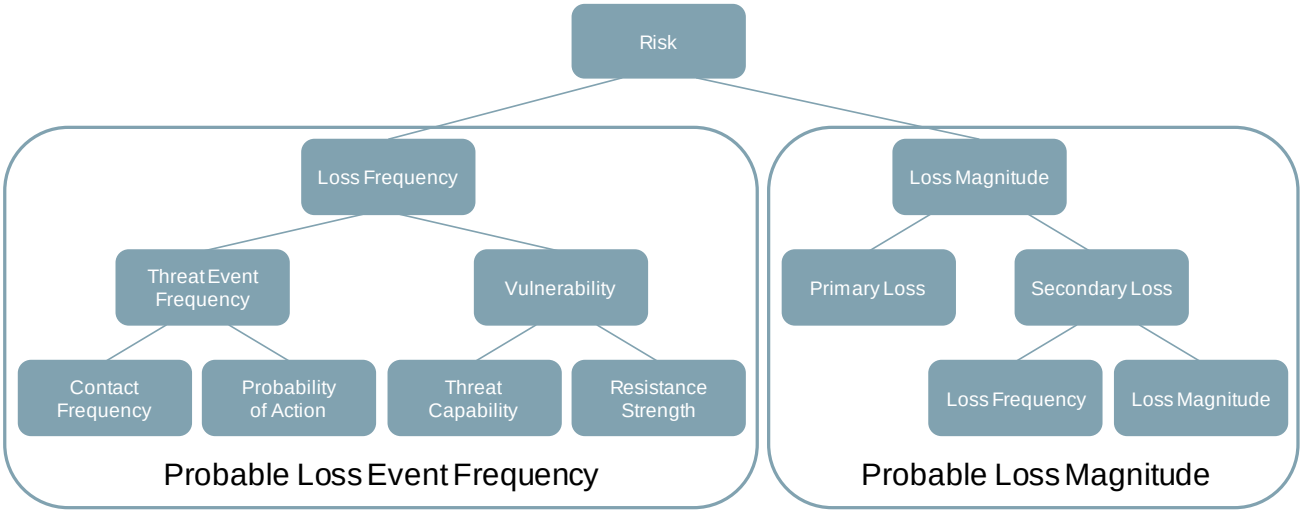

Figure 8: The Open FAIR Risk Tree

Ransomware attacks on hospitals are not a common occurrence. This is due to the fact that ransomware itself is a fairly new method of compromising a system.[8] As a result, the risk team struggled to find reliable data on the loss frequency side of the tree. However, the majority of the attacks that the team did find information on occurred in the US; as already discussed, US threat agents face different incentives than those in Norway.

Moreover, due to these differences, the team also struggled to find much useful information on vulnerability, which depends not only upon the security of the RHA's systems but also on the attentiveness of patients, doctors, physicians, staff, etc. who handle the memory sticks containing treatment data.

Information on loss magnitude was also scarce due to the newness of ransomware. The risk team did identify several instances of hospitals needing to pay in order to decrypt their files, but specific information was unavailable.

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

Given the lack of data, the risk team was unsure of how exactly to analyze the present state of risk. The Norwegian RHA has not yet faced a ransomware attack, so specific information on it was unavailable. Moreover, the information the risk team had found came from different countries with different threat agents, which meant the team could only speculate – at best – how to apply that to Norway. As a result, the risk team did not find a specific monetary estimate of losses per year due to malware/ransomware attacks. However, the risk team was still able to inform effectively without a monetary value.

By not allowing any online connection between home dialysis machines and medical services providers, the RHA decision-makers avoided all risks associated with those connections. However, that's only half of the question. What was the RHA giving up in terms of improved patient health outcomes, lower medical service delivery costs, and improved quality of patient life? These are all foregone benefits that are the price of avoiding malware and ransomware risks associated with connecting dialysis machines online. As part of the present state analysis, the team analyzed those foregone benefits to evaluate a prospective future state where the public and

[8] This was true as of 2017, when the risk analysis was completed.

patients received the benefits of online connections at the cost of some incremental risk associated with malware and ransomware.

7.3.3 Model a Proposed Alternative

The proposed alternative would be the switch from patients delivering treatment data on a memory stick to having the home dialysis machines communicate treatment data with the RHA using the Internet. Some machines in Norway would simply require their network connection to be enabled to do this, while others would need to be replaced with more modern machines that could connect to the Internet.

Unfortunately, because the risk team was unable to find many values while modeling the *status quo*, it was also unable to update those values while modeling the proposed alternative. The team, however, analyzed the relative benefits to attackers who chose malware/ransomware as their weapon of choice and discussed the relative likely benefits to attackers using the home dialysis machine as an attack vector over alternative attack vectors to accomplish their goals. By decomposing the risk into its factors, the team critically thought through the attack from the perpetrator's perspective.

Key to modeling the proposed alternative was the architecture of the communication link between the dialysis machine and the hospital network. Because that link was not known and because the malware and ransomware risk depended upon the architecture, the team could not accurately model a specific implementation.

7.3.4 Estimate the Risk of the Proposed Future State

At this stage of the analysis, the risk team could not estimate the risk from the change; it had reached out to several companies that produce home dialysis machines in an attempt to learn more about how they would communicate the treatment data, but the company that the risk team did eventually talk to was unable to share specifics about how its devices communicate over a network. As a result, the risk team was unable to estimate vulnerability because resistance strength will depend on how the machines communicate and exchange information, on which the team did not have any actual information.

Nevertheless, the risk team was able to identify several potential methods for how a home dialysis machine could communicate with a hospital/satellite clinic. As described in the original scenario, the machines could use a VPN to transmit treatment data. Moreover, the machines could encrypt the treatment data before uploading it to an intermediary drop box. Data validation and verification before use and digital signatures would also substantially increase the resistance strength of the connection. To put it in Open FAIR terminology, encrypting the data would be privacy or confidentiality control, and signing the data would be an integrity control.

Therefore, the risk team found that the risk from malware/ransomware would depend upon the architecture of the dialysis machine, its interconnection with the hospital/satellite clinic, and the hospital's use of the transmitted data. In essence, available technology could arbitrarily reduce the risk to any desired level approaching zero. As a result, the risk team concluded that the risk question should be reframed into an architectural and engineering challenge: the risk of a malware/ransomware attack could be as low as desired, given the design of the system. The question architects and engineers then had to answer was: "Are the public and patient benefits worth the cost of incurring the risk as architected and designed?".

7.3.5 Evaluate the Alternative

In evaluating the alternative, the risk team could assume a solution might exist if it only knew what the public and private benefits were. The original scenario presented to the risk team assumed patients would need to go to and from a hospital/satellite clinic several days each week, just like patients completing dialysis treatment at a hospital/satellite clinic. However, the team learned this assumption was inaccurate; rather, home dialysis patients only need to visit a hospital every four to six weeks to have their treatment plans updated. As a result, the original benefits that the team identified are not immediately relevant, but they are still useful.

Patients in Norway are reimbursed for travel expenses to and from a hospital/satellite clinic to complete treatment. Although this does not really apply to the immediate analysis, it can still be useful for informing decision-makers. Completing dialysis at home instead of at a hospital/satellite clinic saves about 434,000 Krone ($50,000 to $52,000) per patient per year. However, many patients eligible for home dialysis do not wish to take this option and instead prefer in-clinic treatments, in part due to concerns about privacy.

Depending on the online system architecture put in place, these privacy concerns could be thoroughly addressed, thus allowing for more patients to complete treatments at home. This would have a significant impact on leisure time available to the patients: they could complete their treatments while they sleep instead of travelling to a hospital/satellite clinic several times per week for four to eight-hour long treatment sessions, effectively allowing these dialysis patients and their companion/spouse to have three waking days of their week back. It would also mean that these patients would not need to travel multiple times per week and would instead only need to visit a hospital/satellite clinic every four to six weeks.

Moreover, acceptance of digital transmission of data would open the door for increased telemedicine. Telemedicine is already a growing trend in multiple countries around the world and is seeing increased quality-of-life measures for patients and decreased costs for healthcare systems.

The cost of switching to using a home dialysis machine that transmits treatment data over the Internet could be small for some patients and costlier for others. A patient new to home dialysis would need a home dialysis machine as well as training on how to use it. Hospital/satellite clinic personnel would also need to be assigned to work with patients to ensure the machines are transmitting correctly. Moreover, it could potentially be costly to develop and implement the online system architecture needed. However, patients with home dialysis machines that can communicate via the Internet would simply need to enable the connection.

In evaluating the alternative, the analyst looked at not just the risk associated with the information technology, but also the benefits to all stakeholders from assuming that risk. The analysts in this study took a pure cost-benefit approach that places a money-value cost on risk that can be compared to money-valued benefits of taking that risk.

7.3.6 Prepare to Inform the Decision-Maker

Although the risk team was not able to present a monetary estimate for the present state of risk or the proposed change, it was still able to use the Open FAIR framework to provide useful information to the decision-makers. Ultimately, the decision-makers were concerned about losing control of their systems due to a malware/ransomware attack. However, the risk team found that the risk of transmitting treatment data over the Internet could be reduced to an

arbitrarily small value, depending on the online system architecture in place. Therefore, although a risk could exist, the risk team found it highly improbable for the risk to be unmanageable.

As a result, the risk team could identify that a different question needed to be asked. It was not a question of how much risk there is, but is instead a question of how to design and implement a system that meets the decision-makers' acceptable level of risk at an acceptable cost. If that challenge can be met, the benefits of accepting the residual risk outweigh the costs of the risk itself, especially due to the potential for increased use of telemedicine.

7.4 Inform the Decision-Maker

At this stage, the risk analyst/team must inform the decision-maker. As stated already, this section does not contain much other than the link to The Open Group White Paper that this section describes:

- Putting Open FAIR™ Risk Analysis Into Action: A Cost-Benefit Analysis of Connecting Home Dialysis Machines Online to Hospitals in Norway, White Paper (W176), May 2017, published by The Open Group; refer to: www.opengroup.org/library/w176

This White Paper contains all the information described in Chapter 6. However, the format of the paper is the direct result of Open Group White Paper formatting guidelines and likely will not be suited for other purposes.

7.5 Conclusion

Despite the fact that this analysis did not follow the Open FAIR methodology exactly,[9] it is still useful for highlighting how the Open FAIR framework can help decision-makers. Specifically, this example scenario showed that multiple analyses may need to be done when there is more than one perspective and, therefore, multiple risk questions. When there are multiple risk questions that need to be answered, the risk analyst will need to complete multiple analyses. However, it will not always be clear at the beginning of the project that there will be more than one risk question, which is why scoping the risk analysis is absolutely vital.

Through using the Open FAIR methodology and utilizing their backgrounds in economic thinking and analysis, the risk team was able to identify the question that the decision-makers actually needed to ask. As a result, the decision-makers could now ask this question and focus on finding a method for transmitting patient data that meets their acceptable level of risk. By focusing on this, the Norwegian RHA would be able to make steps to advance how patients are treated, improve patient health outcomes, and increase patient quality-of-life, all while decreasing costs to administer healthcare.

[9] The risk team was unable to find values for loss frequency and loss magnitude.

A Open FAIR Risk Analysis Worksheet Template

This appendix contains a blank template of the worksheet the risk team used to organize information for the case study analysis.

A.1 Stage 0: Analysis Initiation Phase – Gather Organizational Information Required for the Analysis

Required Information	Response/Detailed Comments
Analysis Initiation Phase	
Has an owner/stakeholder been identified for the analysis?	Yes/No
Name the owner/stakeholder for the analysis.	
Have the resources been identified for performing the risk analysis?	Yes/No
Name of the resources identified to perform the analysis.	
Has the owner/stakeholder provided an initial risk question?	Yes/No
Brief description of the initial risk question to be scoped.	
Have resources been identified who can provide data for scoping the initial risk question?	Yes/No
Name the resources who will be providing the data required for scoping the risk question.	
Describe the activities needed to take place to perform the analysis; e.g., data collection, research, meetings.	
Provide the timeline during which the activities will take place. If possible, provide a work breakdown of the activities by date with the planned start and end date.	

Required Information	Response/Detailed Comments
Analysis Initiation Phase	
Has the owner/sponsor allocated a budget for the analysis which includes resources plus any necessary research for obtaining data?	Yes/No

A.2 Stage 1: Identify Scenario Components (Scope the Analysis)

Required Information	Response/Detailed Comments
Develop the Risk Question	
What is the problem statement or concern to be analyzed? Provide the initial risk question to be scoped from Stage 0.	
What is the asset or asset class that needs to be protected and for which losses are to be calculated?	
Who is the primary owner/stakeholder who would be directly accountable for the loss?	
Identify the organizational scope of the asset(s); e.g., enterprise, business unit, etc.	
Who or what is the threat?	*Identify all the threats that can impact the asset(s) and list them in Table 3.*
Who or what are the threat agents/communities?	*Identify all the threat communities in Table 3.*
What action needs to take place to impair the asset?	*Identify the actions in Table 3.*
How does the asset owner observe the loss?	*Identify how the actions are observed in Table 3.*
How does the asset owner value or measure the loss as observed?	*Identify how the loss is valued or measured in Table 3.*
What data is known to be available and how will it be obtained?	

Table 3: Threats to Asset Table

Threat No.	Asset at Risk	Threat	Threat Community	Threat Action	Observation	Valuation of Loss
1						
2						
3						
4						
5						

Using Table 3, identify potential loss scenarios that could be analyzed and compared and enter them in Table 4.

Table 4: Loss Scenario Table

Define Potential Loss Scenario(s) to be Analyzed for the Asset at Risk	
Loss Scenario 1	
Loss Scenario 2	
Loss Scenario 3	

Choose the loss scenario to be analyzed. This section may be repeated when comparing losses for different loss scenarios. Enter these below, adding extra rows as necessary.

Model the Risk Question for the Loss Scenario to be Analyzed	
Describe loss scenario for the analysis chosen from Table 4.	

A.3 Stage 2: Evaluate Loss Event Frequency (LEF)

Determine the Loss Event Frequency	Response/Detailed Comments
Is there sufficient data about the chosen scenario to determine the LEF? If Yes, provide details	Yes/No
Is the data available current?	Yes/No
Have there been any changes to the environment since the data was collected?	Yes/No

If the answers above are Yes	
Describe the potential frequency with which the threat agent(s) in the loss scenario may come into contact with the asset(s).	
What is the probability that the threat agent will act against the asset?	
Based upon the known potential frequency and probability, what is the derived LEF?	

If the answers above were No, go down one level to determine the LEF in Table 5.

Table 5: Threat Event Frequency (TEF)

Determine the Threat Event Frequency	Response/Detailed Comments
For the scenario under analysis, what is the Contact Frequency of the threat vector upon the asset?	
What is the Probability of Action of the threat vector upon the asset?	
How valuable is the asset to the actor; i.e., what are the motives for the actor acting upon the asset?	
Are there any deterrents which might affect the attack?	
Determine the Vulnerability	
What is the threat capability of the threat actor?	
What resources are available to the threat agent?	
What level of skills or experience does the threat agent require?	
What is the Resistance Strength of the asset?	
What controls are in place to protect the asset from the specific threat capability?	
How effective are these controls in protecting the asset from the specific attack?	

Determine the Threat Event Frequency	Response/Detailed Comments
Derive the level of vulnerability based upon the difference between the threat actor's attack abilities and the asset's abilities to resist the attack.	
Derive the LEF from the TEF and Vulnerability	
Value obtained for TEF.	
Value obtained for Vulnerability.	
Methodology used to derive LEF.	
Derived LEF value.	

A.4 Stage 3: Evaluate Loss Magnitude

Evaluate Loss Magnitude	Response/Detailed Comments
Evaluate Primary Loss Factors	
From the threat table below, identify the threat action to be evaluated for its loss potential.	
If more than one threat action will be evaluated for comparison, identify those as well here.	

For each of the threats to be evaluated for loss potential, identify the loss forms in Table 6 and Table 7, entering the parameters for each form of loss. Note that the Primary Loss and Secondary Loss parameters below assume that the risk analyst will be using PERT distributions in the model. The table may need to be modified to collect the required parameters for input into other models.

Table 6: Primary Loss Forms

Threat No.		Primary Loss Forms					
		Productivity	**Response**	**Replacement**	**Fine/ Judgments**	**Competitive Advantage**	**Reputation**
1	**Min value**						
	Most likely						
	Max value						

Threat No.		Primary Loss Forms					
		Productivity	Response	Replacement	Fine/ Judgments	Competitive Advantage	Reputation
	Confidence level						
2	Min value						
	Most likely						
	Max value						
	Confidence level						
3	Min value						
	Most likely						
	Max value						
	Confidence level						

Table 7: Secondary Loss Forms

Threat No.		Secondary Loss Forms					
		Productivity	Response	Replacement	Fine/ Judgments	Competitive Advantage	Reputation
1	Min value						
	Most likely						
	Max value						
	Confidence level						
2	Min value						
	Most likely						
	Max value						
	Confidence level						

Threat No.		Secondary Loss Forms					
		Productivity	**Response**	**Replacement**	**Fine/ Judgments**	**Competitive Advantage**	**Reputation**
3	**Min value**						
	Most likely						
	Max value						
	Confidence level						

A.5 Stage 4: Derive and Articulate Risk

Analysis Results	**Response/Detailed Comments**
Primary LEF from above.	
Primary LM from above.	
Secondary LEF from above.	
Secondary LM from above.	
Primary Risk.	
Secondary Risk.	

Documenting Rationale	**Response/Detailed Comments**
Document any specific rationale and assumptions which determined the choice of data for the analysis and the choices for the specific loss scenarios used for the analysis.	
Fragile qualifiers – document any conditions where a single point of failure could change a situation where LEF is low in spite of high TEF.	
Unstable qualifiers – situations where LEF is low solely because TEF is low, and where a change in conditions for TEF could change LEF.	

Documenting Rationale	Response/Detailed Comments
Capacity for loss for the organization – what is the documented loss capacity established by upper management?	
Tolerance for loss for the organization – what is management's documented tolerance for loss relative to the capacity for loss?	

B Completed Open FAIR Risk Analysis Worksheet

This appendix contains the completed worksheet for the case study risk analysis. This worksheet only applies to the malware/ransomware risk analysis.

B.1 Stage 0: Analysis Initiation Phase – Gather Organizational Information Required for the Analysis

Required Information	Response/Detailed Comments
Analysis Initiation Phase	
Has an owner/stakeholder been identified for the analysis?	Yes
Name the owner/stakeholder for the analysis.	The Norwegian RHA
Have the resources been identified for performing the risk analysis?	Yes
Name of the resources identified to perform the analysis.	Stig Hagestande Mike Jerbic Sushmitha Kasturi Biljana Strageland
Has the owner/stakeholder provided an initial risk question?	Yes
Brief description of the initial risk question to be scoped.	The risk from malware/ransomware entering the connection between home dialysis machines and hospitals.
Have resources been identified who can provide data for scoping the initial risk question?	Yes
Name the resources who will be providing the data required for scoping the risk question.	Stig Hagestande Sushmitha Kasturi Biljana Strageland
Describe the activities needed to take place to perform the analysis; e.g., data collection, research, meetings.	Data collection, regular meetings of both the risk team and the risk team with the Norwegian RHA representative, research on prevalence of attacks.

Required Information	Response/Detailed Comments
Analysis Initiation Phase	
Provide the timeline during which the activities will take place. If possible, provide a work breakdown of the activities by date with the planned start and end date.	The project was planned to be completed by the end of January 2017, culminating in a presentation at an Open Group conference.
Has the owner/sponsor allocated a budget for the analysis which includes resources plus any necessary research for obtaining data?	N/A

B.2 Stage 1: Identify Scenario Components (Scope the Analysis)

Required Information	Response/Detailed Comments
Develop the Risk Question	
What is the problem statement or concern to be analyzed? Provide the initial risk question to be scoped from Stage 0.	
What is the asset or asset class that needs to be protected and for which losses are to be calculated?	The confidentiality, integrity, and availability of information assets.
Who is the primary owner/stakeholder who would be directly accountable for the loss?	Any hospital or satellite clinic connected to a home dialysis machines as well as the Norwegian RHA.
Identify the organizational scope of the asset(s); e.g., enterprise, business unit, etc.	N/A
Who or what is the threat?	*Identify all the threats that can impact the asset(s) and list them in Table 8.*
Who or what are the threat agents/communities?	*Identify all the threat communities in Table 8.*
What action needs to take place to impair the asset?	*Identify the actions in Table 8.*
How does the asset owner observe the loss?	*Identify how the actions are observed in Table 8.*
How does the asset owner value or measure the loss as observed?	*Identify how the loss is valued or measured in Table 8.*
What data is known to be available and how will it be obtained?	Little data exists on the frequency or severity of ransomware attacks due to their recent development.

Table 8: Threats to Asset Table

Threat No.	Asset at Risk	Threat	Threat Community	Threat Action	Observation	Valuation of Loss
1	The confiden-tiality, integrity, and availability of information assets.	Loss of control of information assets.	Financially motivated individuals external to the hospital.	The connection between the hospital/ satellite clinic and the home dialysis machine.	N/A	N/A

Using Table 8, identify potential loss scenarios that could be analyzed and compared and enter them in Table 9.

Table 9: Loss Scenario Table

Define Potential Loss Scenario(s) to be Analyzed	
Loss Scenario 1	The threat agent successfully uploads ransomware or malware to the hospital/satellite clinic's system through the connection with the home dialysis machine, preventing patient care as well as access to patient information.

Choose the loss scenario to be analyzed. This section may be repeated when comparing losses for different loss scenarios. Enter these below, adding extra rows as necessary.

Model the Risk Question for the Loss Scenario to be Analyzed	
Describe loss scenario for the analysis chosen from Table 9.	N/A: Only one loss scenario.

B.3 Stage 2: Evaluate Loss Event Frequency (LEF)

Determine the Loss Event Frequency	Response/Detailed Comments
Is there sufficient data about the chosen scenario to determine the LEF? If Yes, provide details	No: These attacks are new, and few businesses disclose much information about them.
Is the data available current?	No
Have there been any changes to the environment since the data was collected?	N/A

If the answers above are Yes	
Describe the potential frequency with which the threat agent(s) in the loss scenario may come into contact with the asset(s).	N/A
What is the probability that the threat agent will act against the asset?	N/A
Based upon the known potential frequency and probability, what is the derived LEF?	N/A

If the answers above were No, go down one level to determine the LEF in Table 10.

Table 10: Threat Event Frequency (TEF)

Determine the Threat Event Frequency	Response/Detailed Comments
For the scenario under analysis, what is the Contact Frequency of the threat vector upon the asset?	Unknown
What is the Probability of Action of the threat vector upon the asset?	Unknown
How valuable is the asset to the actor; i.e., what are the motives for the actor acting upon the asset?	The threat agent is financially motivated: A successful ransomware attack ends with the threat agent receiving a payment.
Are there any deterrents which might affect the attack?	Unknown
Determine the Vulnerability	
What is the threat capability of the threat actor?	Unknown
What resources are available to the threat agent?	Unknown
What level of skills or experience does the threat agent require?	Unknown
What is the Resistance Strength of the asset?	Unknown
What controls are in place to protect the asset from the specific threat capability?	Unknown
How effective are these controls in protecting the asset from the specific attack?	Unknown

Determine the Threat Event Frequency	Response/Detailed Comments
Derive the level of vulnerability based upon the difference between the threat actor's attack abilities and the asset's abilities to resist the attack.	Unknown
Derive the LEF from the TEF and Vulnerability	
Value obtained for TEF.	Unknown
Value obtained for Vulnerability.	Unknown
Methodology used to derive LEF.	Unknown
Derived LEF value.	Unknown

B.4 Stage 3: Evaluate Loss Magnitude

Evaluate Loss Magnitude	Response/Detailed Comments
Evaluate Primary Loss Factors	
From the threat table below, identify the threat action to be evaluated for its loss potential.	The successful implementation of malware/ransomware through the connection between a home dialysis machine and a hospital/satellite clinic.
If more than one threat action will be evaluated for comparison, identify those as well here.	N/A

For each of the threats to be evaluated for loss potential, identify the loss forms in Table 11 and Table 12, entering the parameters for each form of loss. Note that the Primary Loss and Secondary Loss parameters below assume that the risk analyst will be using PERT distributions in the model. The table may need to be modified to collect the required parameters for input into other models.

Table 11: Primary Loss Forms

Threat No.		Primary Loss Forms					
		Productivity	**Response**	**Replacement**	**Fine/ Judgments**	**Competitive Advantage**	**Reputation**
1	**Min value**	N/A	N/A	N/A	N/A	N/A	N/A
	Most likely	N/A	N/A	N/A	N/A	N/A	N/A
	Max value	N/A	N/A	N/A	N/A	N/A	N/A

Threat No.		Primary Loss Forms					
		Productivity	**Response**	**Replacement**	**Fine/ Judgments**	**Competitive Advantage**	**Reputation**
	Confidence level	N/A	N/A	N/A	N/A	N/A	N/A

Table 12: Secondary Loss Forms

Threat No.		Secondary Loss Forms					
		Productivity	**Response**	**Replacement**	**Fine/ Judgments**	**Competitive Advantage**	**Reputation**
1	**Min value**	N/A	N/A	N/A	N/A	N/A	N/A
	Most likely	N/A	N/A	N/A	N/A	N/A	N/A
	Max value	N/A	N/A	N/A	N/A	N/A	N/A
	Confidence level	N/A	N/A	N/A	N/A	N/A	N/A

B.5 Stage 4: Derive and Articulate Risk

Analysis Results	**Response/Detailed Comments**
Primary LEF from above.	N/A
Primary LM from above.	N/A
Secondary LEF from above.	N/A
Secondary LM from above.	N/A
Primary Risk.	N/A
Secondary Risk.	N/A

Documenting Rationale	**Response/Detailed Comments**
Document any specific rationale and assumptions which determined the choice of data for the analysis and the choices for the specific loss scenarios used for the analysis.	Threat agents are financially motivated despite the Norwegian healthcare system being a single-payer system.

Documenting Rationale	Response/Detailed Comments
Fragile qualifiers – document any conditions where a single point of failure could change a situation where LEF is low in spite of high TEF.	N/A
Unstable qualifiers – situations where LEF is low solely because TEF is low, and where a change in conditions for TEF could change LEF.	N/A
Capacity for loss for the organization – what is the documented loss capacity established by upper management?	Unknown
Tolerance for loss for the organization – what is management's documented tolerance for loss relative to the capacity for loss?	Minimal

Index