Natural Resources Canada

IACS Cybersecurity Risk Methodology

Technical report supported by Natural Resources Canada under the Cyber Security and Critical Energy Infrastructure Program (CCEIP)

Prepared by: Ahmad Ahmadi, Ph.D., IACS Cybersecurity Specialist, BBA

Verified by: José Alvarado, P.Eng., GICSP, Department Manager, IACS Cybersecurity, BBA

Published on September 23, 2020 | bba.ca |

BBA Document No. / Rev. 6691001-000000-4S-ERA-0002 / RAB

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES


BBA
Natural Resources Canada
Chapter 1
Introduction

CHAPTER 1. INTRODUCTION

Every industrial automation and control systems (IACS) environment has its specific risk profile, shaped by the threats its components are exposed to, the likelihood of those threats arising, the vulnerabilities in the system, the consequences of having the system compromised and the risk tolerance of the organization.

This document will guide an organization to manage the cybersecurity risk of its IACS environment and, more specifically, through the process of assessing the cybersecurity risk of the IACS environment and mitigating identified risks into tolerable levels.

Risk assessment is one of the main components of organizational risk management. In IACS environments, cybersecurity risk assessments are used to identify, estimate and prioritize cyber risks to operational functions, assets, individuals, other organizations and the nation that result from operating and using automation and control systems.

The purpose of assessing cybersecurity risks at the operations system level is to support the implementation of organizational risk management more effectively. This will happen by informing decision makers and supporting risk responses by identifying (i) relevant threats to the operation or threats directed through operations against other organizations; (ii) vulnerabilities, both internal and external, to operations; (iii) impacts to operations that may occur given the potential for threats exploiting vulnerabilities and (iv) the likelihood that harm will occur. The result is a risk determination of the operational environment.

1.1 Scope

This document provides guidelines for cybersecurity risk management in an industrial automation and control system (IACS) environment. Figure 1 illustrates an example of the placement of IACS cybersecurity risk management in an organization. In this example, although IACS cybersecurity management is placed under the cyber management process, it covers all systems and processes in the organization that can impact IACS environment operations or can be impacted by the cyber threats of the IACS environment.

This document contains the following components:

- Description of cybersecurity risk management components and processes. The mechanism and procedure to conduct cybersecurity risk management.
- Process of assessing cybersecurity risk including high-level overview of the risk assessment process, the activities necessary to prepare for a risk assessment, the activities necessary to conduct a risk assessment, the relation between risk assessment components and other components of the risk management process and the activities necessary to communicate risk assessment results across the organization.
- Process of monitoring cybersecurity risk and monitoring risk management processes.

- Process of responding, maintaining and communicating cybersecurity risks and activities.
- The activities necessary to monitor and maintain the results of a cybersecurity risk assessment.
- Examples of cybersecurity risk management and risk assessment components relevant to IACS environments, such as the risk framework, threat sources and events, vulnerabilities and predisposing conditions, impact, likelihood of threat event occurrence, risk determination and risk acceptance.

Since the scope of this document is limited to cybersecurity risk, the term “risk management” is used instead of “cybersecurity risk management” for easier reading. The same applies to all risk-related factors, e.g. the term “threat” is used instead of “cybersecurity threat.”

1.2 Normative references

The concepts and guidelines associated with the cybersecurity risk management and assessment processes and approaches contained in this document are intended to be consistent with the processes and approaches described in the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the National Institute of Standards and Technology (NIST) and the Open Group Consortium standards.

The approach described in this document is inspired by multiple security standards and guidelines available for managing, assessing and analyzing cybersecurity risk in IT and OT environments. Some of these guidelines and standards include:

- NIST-SP 800-30, Guide for Conducting Risk Assessments
- ISO/IEC 27005, Information Security Risk Management
- IEC 62443-3-2, Security Risk Assessment and System Design
- ISO 31000, Risk Management Guidelines
- NIST-SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- NIST-SP 800-82, Guide to Industrial Control Systems (IACS) Security
- ISO 31010, Risk Management - Risk Assessment Techniques
- Open FAIR O-RA, Risk Analysis Technical Standard

Adjusting the concepts and guidelines of these international standards to fit IACS environments and promoting the reuse of risk assessment results helps organizations with operational sites to understand, contain and manage the cybersecurity risks that are threatening their business.

1.3 Intended audience

This document applies to all types of organizations that intend to manage cybersecurity risks that can compromise their operational environment.

This document is relevant to managers, asset owners, system integrators, product suppliers, service providers and staff concerned with cybersecurity risk management within an organization operating an IACS.

1.4 Document structure

The remainder of this document contains the description of the cybersecurity risk management concepts, processes, activities, examples and other supporting information as follows:

- **CHAPTER 2** describes the concept and components of cybersecurity risk management within operational environments and their relationship with organizational risk management. It describes **what** the components of operational cybersecurity risk management are.

  The "Risk Framework" is about defining the **scope, context and requirements** for developing processes of the other components.

- **CHAPTER 3** describes the processes of risk management components mentioned in Chapter 2. It describes **how to** develop the components of operational cybersecurity risk management.

  The following format is used to describe each activity in this chapter:

  Input: identifies the input values the activity needs to operate

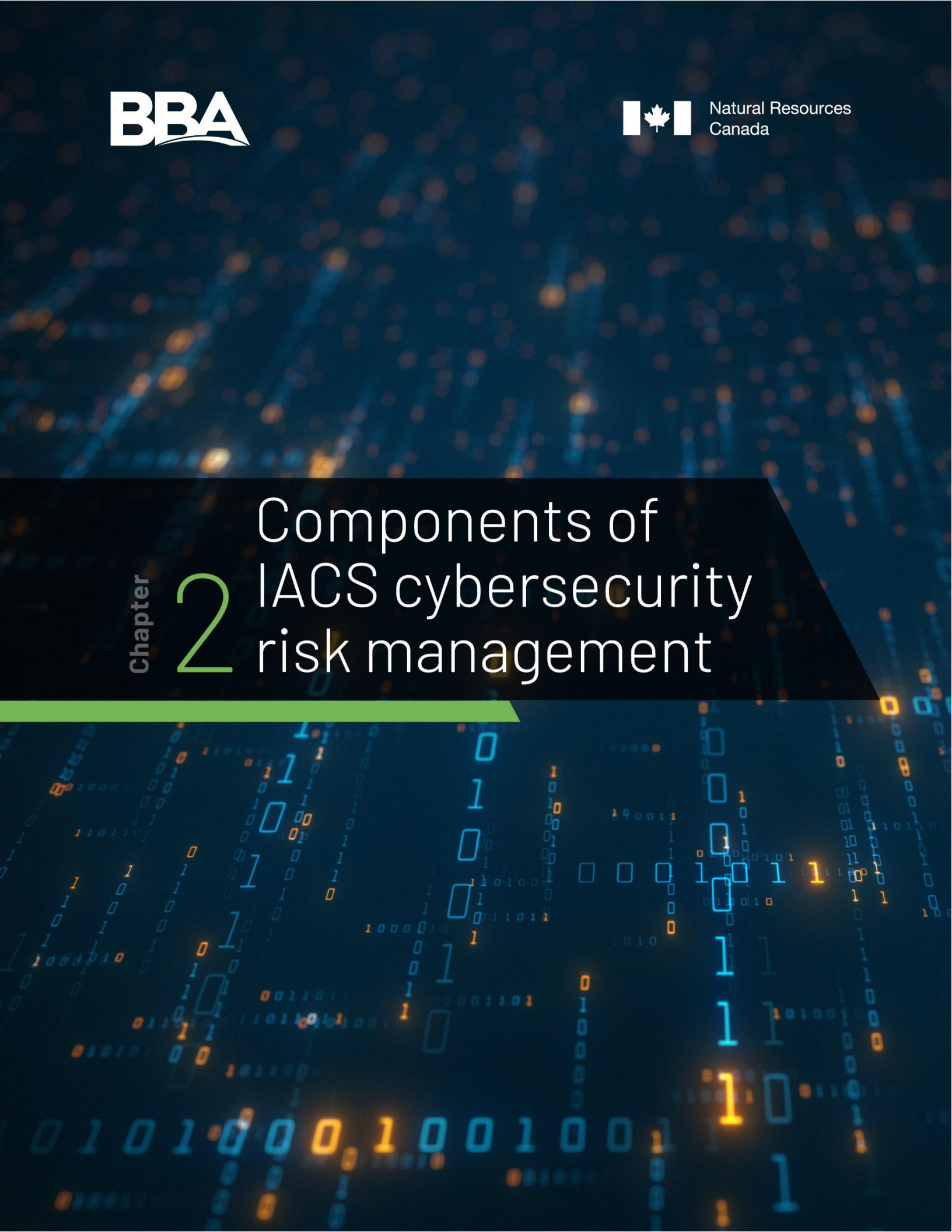
  Action: describes the activity

  Output: identifies the activity deliverables

  Implementation guidance:

  Provides guidance to develop the action process based on the relevant risk framework components.

- **SUPPORTING APPENDICES** provide detailed definitions, conceptual examples, procedural examples and additional information about the concepts, which have been discussed in the previous chapters more specifically related to cybersecurity risk management in industrial and automation control systems.


BBA
Natural Resources Canada
Chapter 2
Components of IACS cybersecurity risk management

CHAPTER 2. COMPONENTS OF RISK MANAGEMENT

This chapter describes the fundamental concepts associated with managing cybersecurity risks within an operational environment. A high-level overview of the risk management process, the role risk assessment plays in the risk management process and the basic concepts used in conducting risk assessment are provided.

We follow the risk management framework as defined in the *NIST Special Publication 800-39* [1]. Based on the model presented in the *NIST-SP 800-39* publication, we consider a simplified model that includes three risk management tiers from an organizational perspective: Organizational, Business Processes and Operational Systems.

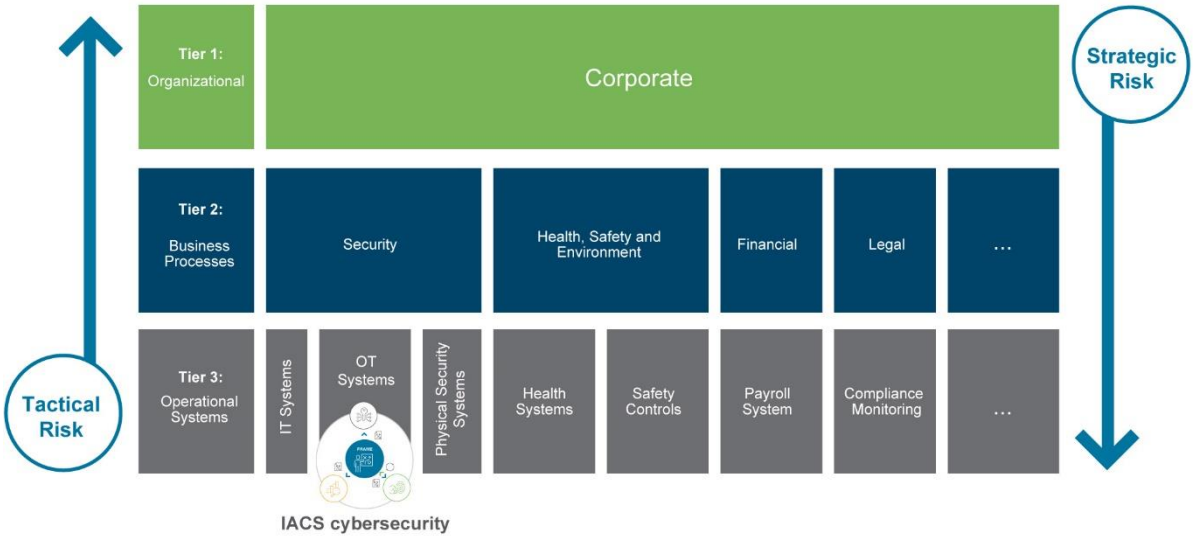


Figure 1: IACS cybersecurity risk management position

In this document, we focus on the activities of the risk management process that are related to cybersecurity, which are classified within the Operational Systems tier. The risk management activities in this tier include some activities carried out from the higher tiers, such as reflecting the organization's risk management strategy in the system architecture, and the activities related to the system development life cycle of operational and information systems.

Cybersecurity risk management activities, as a subset of all risk management activities of the Operational Systems tier, take place at every phase in the system development life cycle, with the outputs at each phase influencing subsequent phases. Each cybersecurity risk management activity can run once, iteratively or on a live process basis.

The cybersecurity risk management process consists of the following components:

(i) framing risk
(ii) assessing risk
(iii) responding to risk
(iv) monitoring risk

Figure 2 shows the components of the high-level risk management process.

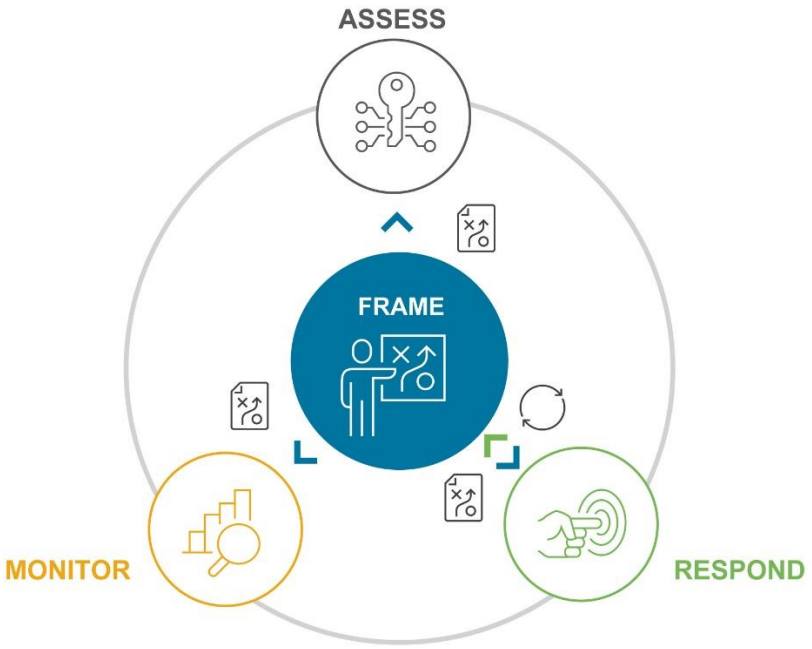


Figure 2: Operational risk management components

The first component of operational risk management defines the processes to **assess** cybersecurity risk within the context of the risk framework. The purpose of the risk assessment component is to identify (i) assets, their classification and their interdependency; (ii) threats to organizations (i.e. operations, assets, or individuals) or threats directed through organizations against other organizations or the nation; (iii) existing cybersecurity controls to protect against identified threats; (iv) vulnerabilities internal and external to organizations; (v) consequences and their impact, which may occur given the potential for threats exploiting vulnerabilities; (vi) the likelihood that those consequences will occur; and finally (vii) determination of risk (i.e. typically a function of the degree of impact and likelihood of consequence occurring). See Section 2.1 for details.

The second component of operational risk management establishes the procedure to **respond** to risk, once that risk is determined, based on results of a risk assessment, and actions and communications needed for maintaining and improving those results. The purpose of the risk response component is to provide a consistent, organization-wide response to risk in accordance

with the risk framework by developing alternative courses of action to respond to risk, evaluating the alternative courses of action, determining appropriate courses of action consistent with organizational risk tolerance, implementing risk responses based on selected courses of action and defining activities to maintain the results of risk assessments. See Section 2.2 for details.

The third component of operational risk management develops a mechanism to **monitor** cybersecurity risk over time. The purpose of the risk monitoring component is to (i) determine the ongoing effectiveness of risk responses (consistent with the risk framework); (ii) identify risk-impacting changes to the organization, business processes, operational systems and the environments in which these systems operate; (iii) verify that planned risk responses are implemented and cybersecurity requirements derived from and traceable to organizational business functions, federal legislation, directives, regulations, policies, standards and guidelines are met; and (iv) document all events, changes, decisions and communications based on the requirements of the risk framework. See Section 2.3 for details.

The fourth component of operational risk management determines the way the organization **frames** cybersecurity risk and defines risk context for making operational decisions. The purpose of the risk framing component is to develop an operational risk management strategy based on the guidelines of the organizational risk management strategy. The operational risk management strategy defines the scope and guidelines of how to model, assess, communicate, monitor, document, maintain and respond to risk. See Section 2.4 for details.

2.1 Risk assessment

IACS cybersecurity risk assessment addresses the potential adverse effects to organizational operations, assets, individuals, other organizations or the community, arising from the use of operation/information systems, tools and processes. This process identifies and analyzes the cybersecurity risks to the organization's operational environment from different aspects, such as safety, confidentiality, integrity, reliability, availability, environmental, etc.

Risk assessment is a key component of cybersecurity risk management that provides a step-by-step process for organizations on how to prepare for risk assessments, how to conduct risk assessments and how to analyze the data of risk elements in order to calculate risk. The outcome of risk assessments should be provided to decision makers so they can make responsive decisions about identified cybersecurity risks.

Cybersecurity risk assessment supports authorization decisions throughout the operational systems life cycle, risk management activities at the higher organizational tier and risk management activities throughout the operational systems life cycle.

A single IACS cybersecurity risk assessment result shows the status of risks to the operational environment at the time of assessment. In order to have up-to-date visibility over the current risk posture of the environment, the organization should employ risk assessments on an ongoing basis, throughout the risk management life cycle, across all organizational tiers. The risk

assessments should take place on a regular basis and when a major change occurs in the operational or business environment.

The steps that are included in the risk assessment are as follows:

- **Preparation for risk assessment:** Identify the purpose, scope, assumptions, information sources, risk model and analysis approach for conducting the risk assessment.
- **Asset profiling:** Identify and value organizational assets that are related to the operational environment and measure their dependencies.
- **Threat identification:** Identify and analyze threat sources and events.
- **Existing cybersecurity controls identification:** Identify existing controls and their protection coverage on assets and analyze their effectiveness.
- **Vulnerability identification:** Through various sources or testing, identify the vulnerabilities that are threatening organizational assets.
- **Impact Analysis:** Identify the exploitation consequence of vulnerabilities, extract the extent of damage on assets based on their dependencies, and analyze the worst-case impact of the threat events.
- **Likelihood determination:** Analyze the likelihood of exploiting vulnerabilities, despite the existence of cybersecurity controls, by a threat source to successfully make the threat event.
- **Risk determination:** Determine cybersecurity risks as a combination of likelihood of threat exploitation and its impact to the organization.

These steps are often executed sequentially as most of their procedures depend on the output of the previous steps. Figure 3 illustrates the flow of steps that are taken in a typical risk assessment and the immediate risk response activities to those steps (the activities on the right side of the figure).

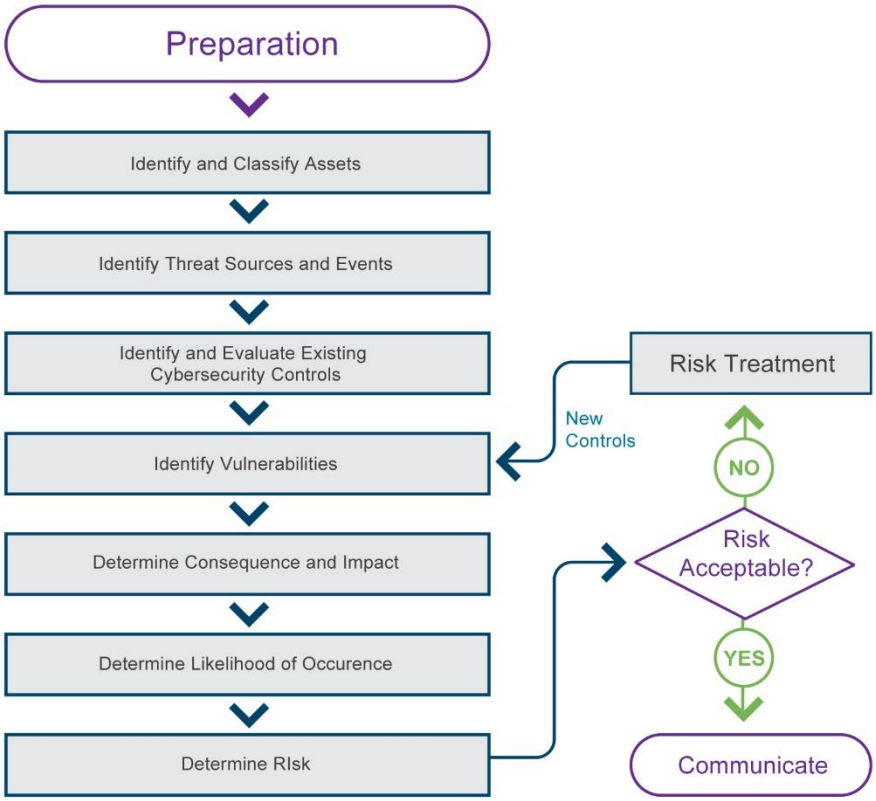


Figure 3: Typical flow of risk assessment steps

2.2 Risk response

Risk response identifies, evaluates, decides, communicates, implements and reviews appropriate courses of action for cyber risks and risk management processes.

The response component of risk management covers evaluation and decision-making about risk acceptability, taking action towards decisions about identified risks in order to treat them so they become satisfactory, communications between various risk management processes and stakeholders and reviewing and improving the risk management processes to operate more effectively.

Risk acceptance decisions are influenced by organizational risk tolerance developed as part of the risk framework. Those decisions should be made based on the outcome of the risk assessment, the expected cost and benefit of implementing each protentional decision, organizational risk tolerance, process value, asset criticality, and operational/business importance of each cybersecurity aspect and stakeholder expectations.

Some examples of risk acceptance decisions are accepting the risk, mitigating the risk, further analyzing the risk, shutting down service, maintaining existing risks or controls, sharing the risk and changing objectives. These decisions should specify the priorities of risk treatment actions.

In coordination with cybersecurity specialists, owners of processes, systems and services need to perform **risk treatment** planning and implementation in order to address risks. Risk treatment involves an iterative process of:

- formulating and selecting risk treatment options
- planning and implementing risk treatment
- evaluating the effectiveness of that treatment
- deciding on residual risk and possibly taking further actions.

Risk communication is to assist relevant stakeholders in understanding risk, the basis on which decisions should be made and the reasons why particular actions are required. Communication promotes risk awareness and obtaining feedback and information to support decision-making. Communications with appropriate external and internal stakeholders should take place within and throughout all steps of the risk management process and should be factual, timely, relevant, accurate and understandable.

The **risk review and improvement** process is used to improve effectiveness of various processes and risk management that are based on the outcome of evaluations in monitoring the process and the expected cost and benefit of implementing each protentional decision.

The tendency for security controls to potentially degrade in effectiveness over time reinforces the need to maintain risk assessments during the entire operation life cycle. As risk assessments are updated and refined, organizations use the risk assessment and monitoring results to update the risk management strategy, thereby incorporating lessons learned into risk management processes and improving responses to risk that are tailored to operational functions.

2.3 Risk monitoring

New vulnerabilities can emerge naturally over time as organizational missions or business functions evolve, operational environments change, new technologies proliferate and new threats emerge. In these situations, the existing security controls may become inadequate and reassessment may be needed.

The tendency for security controls to potentially degrade in effectiveness over time makes it necessary to develop continuous monitoring programs to obtain ongoing situational awareness of the organizational security posture.

Risk management strategies, policies, procedures and guidelines need to evolve and be updated over time based on the cybersecurity risk-related changes that are identified by continuous organizational and operational cybersecurity monitoring processes.

The monitoring component of risk management is responsible for monitoring and evaluating risk factors, monitoring and evaluating risk management processes and documenting changes, results, risk factors, responses, decisions, effects, processes, communications, etc.

Continuous cybersecurity monitoring processes evaluate the effectiveness of risk assessment and responses, identify the risk-impacting changes to information and IACS systems and operational environments, ensure that the cybersecurity requirements are derived from, and traceable to, organizational business functions, ensure compliance to federal legislation, directives, regulations, policies, standards and guidelines, and document all events, changes, decisions, and communications based on the requirements of the organizational risk framework.

2.4 Risk framework

The operational risk management framework is the orchestration book for the organization to mandate operational risk management processes, so they work together and are integrated with the higher-level risk management strategy, which is the outcome of the organizational risk framework. Figure 13 illustrates an example of the components of an overall organizational risk framework[1].

The operational risk management framework can determine components that are illustrated in Figure 4. Note that this list of components is an example and can be altered based on the organizational profile.

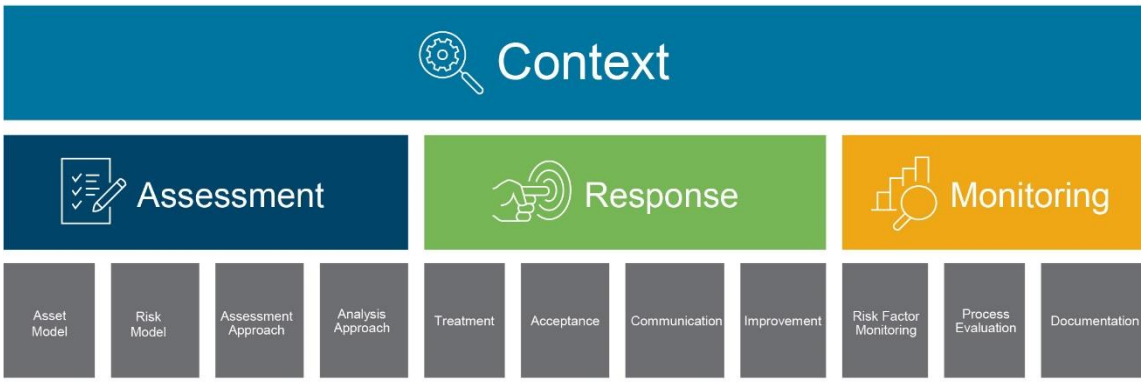


Figure 4: Operational risk framework

In the cybersecurity risk framework, the context for risk management should be established. This includes the scope and organization of risk management, the risk assessment methodology and

[1] This framework is introduced in ISO 31000 [6].

requirements, the risk monitoring and process evaluation scope and approach, risk communication and treatment methodology.

2.4.1 Context

It is essential to determine the purpose of risk management at the very first step based on the organization's strategic business objectives, as it affects the direction of context establishment. This is intended to prepare for a business continuity plan, an incident response plan, legal compliance and defining security requirements for products, services, third parties, etc.

Main stakeholders need to be identified and analyzed to establish expectations and perceptions about the overall risk approach.

At this stage, scope, boundaries, assumptions, constraints, priorities and basic necessary criteria for risk management should be established. Different approaches can be applied depending on the purpose and the scope of operational risk management. The approach can change over time or in each iteration. The components of a risk management approach are described in the following sections. Each of these components can be integrated with an organizational risk management framework and their approach monitored.

2.4.2 Assessment methodology

A risk assessment methodology[2] includes (i) an asset model, defining asset types and organization, their interdependency, their cybersecurity protection requirements and their cybersecurity controls; (ii) a risk model, defining risk factors and their relationships; (iii) a risk assessment process, indicating the detailed risk assessment steps; (iv) a risk assessment approach, specifying the range of values and taxonomy of risk factors and their combination; and (v) a risk analysis approach, describing how combinations of risk factors determine the significance of the identified risk concern. Each of these items will be characterized below.

Risk assessment methodology is a component of the risk management strategy developed during the risk framing step of the risk management process. An organization may choose to define multiple risk assessment methodologies for different situations.

Asset model

Asset models define criticality and operational types and organization of assets, their interdependency, their cybersecurity protection requirements and their cybersecurity controls. An asset model establishes the operational importance of assets and their interdependency based on availability, confidentiality, integrity, safety and reliability criteria.

These factors form the organization's asset profile from a cybersecurity perspective. These factors are used in identifying, classifying and valuating assets, and identifying controls. Asset valuation

[2] Inspired from the model presented in NIST SP 800-30 [2].

assigns a normalized scale for assets to be rated from a risk perspective. It also defines criteria for assigning a particular value on that scale for each asset. The decision to use a quantitative scale or a qualitative scale is a matter of organizational preference and the assets being valued.

An example of an asset model that defines asset organization and protection requirements is categorizing assets into different zones; the protection requirements are defined for each zone[3]. Appendix B | Asset profile describes the process of identifying and valuating assets in more detail.

An asset model is required for developing a risk model, which is described in the following section.

Risk model

A risk model is based on risk factors and their relationships. Typical risk factors include threats, vulnerabilities, impact and likelihood.

The relationship between all risk factors indicates the organization's risk. In other words, a risk model consists of formulating all risk factors and the way they are arranged to calculate risk at the end. Figure 5 illustrates the components of a risk model and their relationship.

[3] ISA 62443-3-2 [10] categorizes assets into different zones and conduits, and each zone has certain cybersecurity requirements.

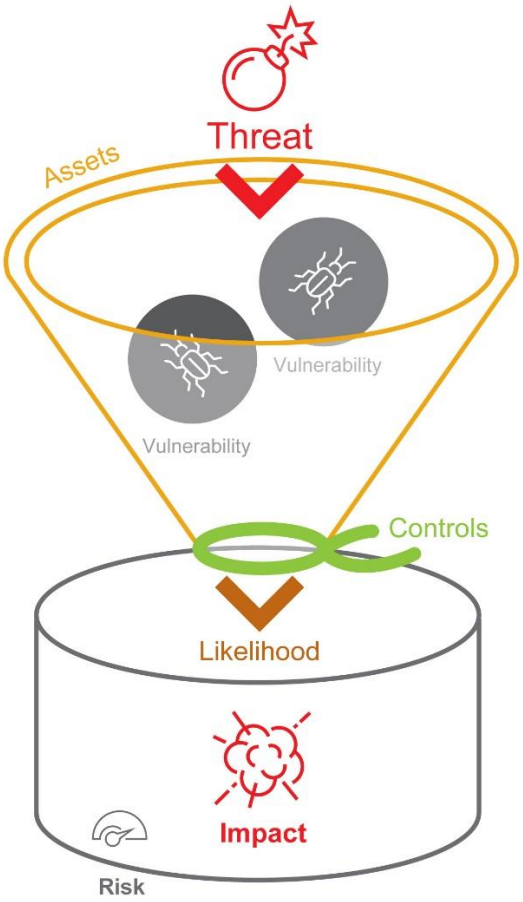


Figure 5: Relationship of risk and risk factors

Risk factors form the organization's risk profile and operational environment, which are used as input to determine risk levels in the risk assessment process. The risk factors are also used to respond to risk and risk communications. The definition of these risk factors are presented in Appendix A | Glossary and some examples are provided in Appendix D | Threat sources and events to Appendix G | Likelihood of occurance.

Risk factors can be decomposed into more details, for example threats decomposed into threat sources and threat events.

Risk is a function of the likelihood of a threat event's occurrence and potential adverse impact when the event occurs [2]. This broad definition also allows risk to be represented as a single value or as a vector of values, where different types of impacts are considered separately. In this definition of risk, all the mentioned risk factors are involved.

Risks can be grouped into categories based on a combination of the risk factors. The most popular way to categorize risks is based on impact categories. Some typical high-level risk categories based on the impact are financial, reputational, legal, safety and environmental.

Appendix H | Risk provides some examples about how cyber risks are calculated and presented.

Risk assessment approach

The risk assessment approach defines the requirements and guidelines to identify and analyze risks and risk elements. It includes the steps of conducting a risk assessment and the deliverables of each step. An example of the list of steps and the included items in the risk assessment approach is shown in Figure 6.

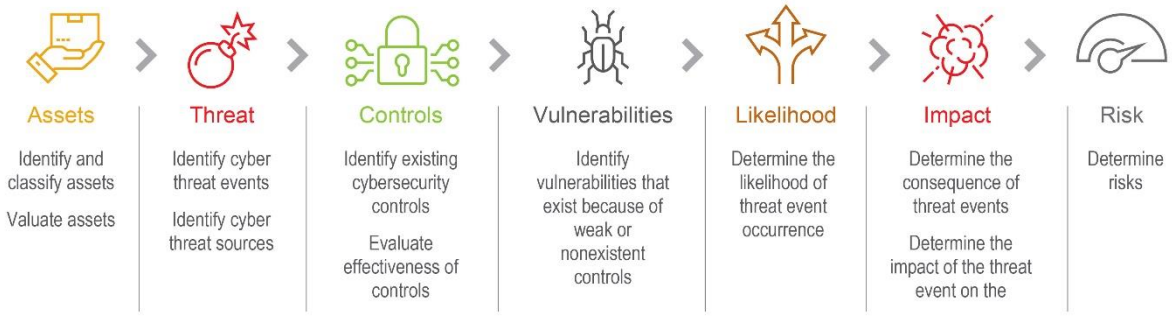


Figure 6: Steps of the risk assessment approach

Risk analysis approach

The risk analysis approach defines the quantification level that is to be used in the risk assessment process for various risk factors, the way to calculate these risk factors, how their combination determines the significance of the identified risk and how to evaluate effectiveness of existing controls. In other words, risk analysis is the calculation engine of the risk assessment process.

The quantification level of risk analysis can be in the range of quantitative, semi-quantitative and qualitative. The accuracy and the cut-offs between measurement scale levels are also defined as part of the analysis approach.

Selecting the appropriate risk analysis approach depends on the organizational and operational environment culture. More specifically, the communication culture and uncertainty have a great role in selecting the proper quantification level in the risk analysis approach.

The risk analysis approach defines the level of quantification in various risk assessment functions such as the risk model, the measurement or estimation of risk factors, risk scenarios, risk calculation and a detailed consideration of uncertainties.

Moreover, the span of the risk analysis approach goes beyond the scope of risk assessment, and it covers risk communication, risk monitoring metrics, risk acceptance and mitigation and risk process evaluation and improvement. The risk analysis approach defines how to evaluate effectiveness of controls and how to choose metrics (i.e. metrics for measuring the effectiveness and state distinction of all processes, controls, risks and risk factors) and combining them in order to calculate future action priorities, effect and cost.

The quantification meaning of a process (e.g. treatment, communication, monitoring, decision-making, etc.), risk factors, asset valuation and other risk-related elements may not always be clear in an organization. However, quantitative analysis approaches use numbers when defining methods, principles, metrics, factors or rules in assessing risk. Generally, in order to have a more effective cost-benefit analysis for different risks responses, it is better to use the more quantitative analysis. However, there can be numerous reasons that reduce the reliability and rigour of those quantitative results, such as unclear assumptions and constraints, too many uncertain values, or subjective determinations.

An example of a **quantitative** analysis approach would be assigning a quantitative scale (e.g. from 0 to 10) to all threats, based on measurable effects of the threat event on the organization. In this approach, the number of hours needed by experts to resolve that event indicates the value of the threat.

On the other hand, more **qualitative** assessment approaches use categories (e.g. low, medium, high) in defining methods, principles, metrics, factors or rules in assessing risk. In qualitative approaches typically, by having smaller diversity of values, it is harder to make relative prioritization in comparison to quantitative approaches. Moreover, it is easier to have subjective opinions affecting the results, which reduces the reproducibility of those results.

The qualitative risk analysis approach can be used:

- when it is more suitable based on the nature of the environment that is being evaluated.
- when the numerical data is inadequate or inaccurate for a quantitative risk analysis approach.
- for initial screening to identify risks that will require more detailed analysis later.

2.4.3 Response methodology

Risk response methodology defines the scope, requirements and methodology for stakeholder and process communications, risk treatment and mitigation, risk acceptance, review and improvement.

Acceptance

The acceptable risk scope and requirements should be developed in a risk framework. Risk acceptance criteria, used to make decisions, should be consistent with the defined external and internal cybersecurity risk management context.

A risk framework should define its own scales for risk acceptance levels while considering the following:

- organizational objectives and stakeholder views
- multiple thresholds, with a desired target level of risk, and defined circumstances for triggering specific decision paths
- defined risk acceptance criteria, considering estimated profit versus the estimated risk
- different risk acceptance criteria that can apply to different classes of risk
- acceptance criteria, which should include business, operations, technology, finance and safety factors.

Risk acceptance criteria can differ according to the expected lifetime of risks, e.g. short-term, long-term, etc.

Treatment

Risk treatment criteria should be developed to plan and implement appropriate risk-reduction controls or countermeasures for the identified cyber risks while considering the following:

- the organization's policies, goals and objectives
- the strategic value of the business information and operation process
- the criticality of the operational assets involved
- operational and business importance of safety, reliability, availability, confidentiality and integrity
- stakeholder expectations and perceptions and negative consequences.

The risk framework should define actions to be taken for each level of risk, e.g. accepting the risk as is, mitigating the risk, shutting down services to avoid risk or sharing the risk internally or externally.

Risk treatment criteria should also include risk maintenance requirements to develop processes for keeping the risks at the current level.

Communication

The risk management process entails ongoing communications among stakeholders to ensure that there is complete visibility and effective risk-based decision-making.

Risk communications criteria should include (but are not limited to):

- identification of all stakeholders
- definition of roles and responsibilities for all internal and external parties
- definition of information and decision transfer between operational and organizational roles and processes

- definition of information and decision transfer to and from external stakeholders
- feedback loop for continuous improvement
- traceable and transparent risk-based decision flow
- definition of decision escalation path
- risk awareness communications
- inter process communications
- definition of information and decision transfer within operational risk processes or systems.

Process improvement

A risk management review and improvement process criteria should be developed for continual improvement of the effectiveness, suitability and adequacy of an integrated risk management program.

The risk framework should develop, review and improve plans, including:

- the review tasks
- review roles and responsibilities
- measures that trigger the review of each risk management process
- review frequencies and conditions

2.4.4 Monitoring methodology

The risk monitoring methodology defines the scope of monitoring, requirements for controls in place with measurable monitoring metrics, procedures to monitor cybersecurity risk management processes and the requirements of the information to be documented.

The risk framework also defines responsibilities, requirements and guidelines for risk assessment and monitoring roles (e.g. for system evaluators, penetration testers, security control assessors, risk assessors, independent validators, inspectors general and auditors).

Risk factor monitoring

This process defines the scope and approach of monitoring changes related to assets and risk factors that can affect risk.

Process evaluation

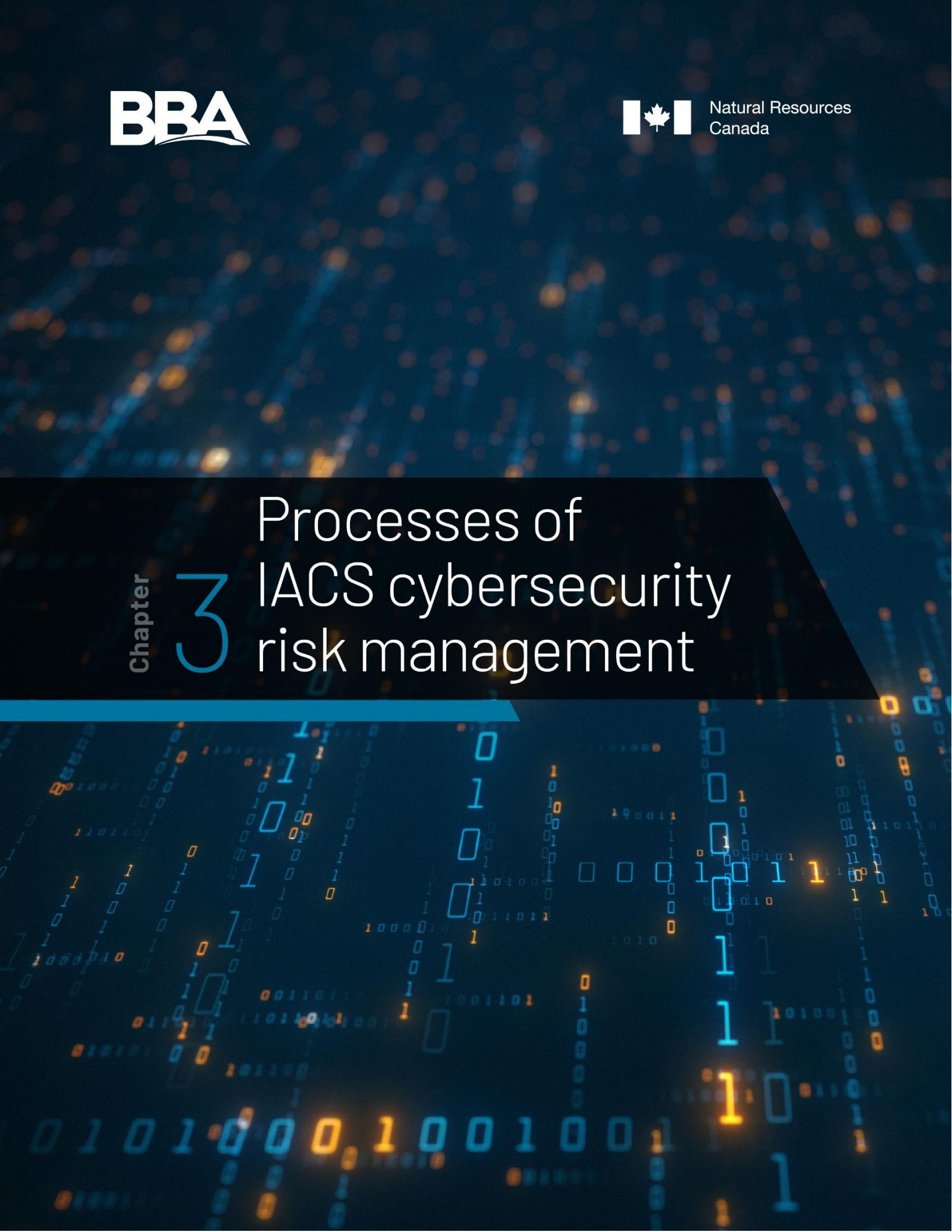
The scope of evaluating the risk management process, and the approach to evaluate the effectiveness of a risk management process are defined with the following in mind:

- Strategic values of the operational process
- Risk management process evaluation criteria

- The evaluation procedure of the cybersecurity risk management process

Documentation

The scope and requirements of documenting events, decisions and changes according to risk factors and risk management processes are defined in this framework component.


BBA
Natural Resources Canada
Chapter 3
Processes of IACS cybersecurity risk management

CHAPTER 3. PROCESSES OF RISK MANAGEMENT

This chapter describes the process of managing cybersecurity risk including (i) a high-level overview of risk framework development; (ii) the process of conducting an effective risk assessment; (iii) the activities necessary to decide upon, mitigate, maintain and communicate risks and review the effectiveness of risk management processes; and (iv) the activities necessary to document and monitor risks and risk processes.

3.1 Developing a risk framework

Input: high-level organizational and business values and objectives; operational profile of the organization.

Action: Develop different components of the risk framework.

Output: Risk management context and all components of assessment, monitoring and response methodology, including their interdependency and workflow.

Implementation guidance: As was mentioned earlier, a risk framework is the core element of the risk management process. It is critical to develop the risk framework at the first step of establishing the risk management program.

At this stage, cybersecurity specialists and organizational and operational managers consider the organizational mandates and the profile of the operational environment to develop the orchestration book of operational risk management.

They define context and scope of the risk management program and identify context and methodology, based on which each component of the program will run. See Section 2.4 for a description of those components.

It is critical to design this framework in a way to ensure it stays adaptive and self evolving against all changes throughout the course of the risk management program.

The overall workflow among the different risk management components is decided at this stage, along with their detailed requirements. Figure 7 illustrates an example of this workflow, which highlights the operational boundaries between risk framework, risk assessment, risk monitoring and risk response.

More information and examples on the risk framework can be found in Appendix C | Organizational risk framework.

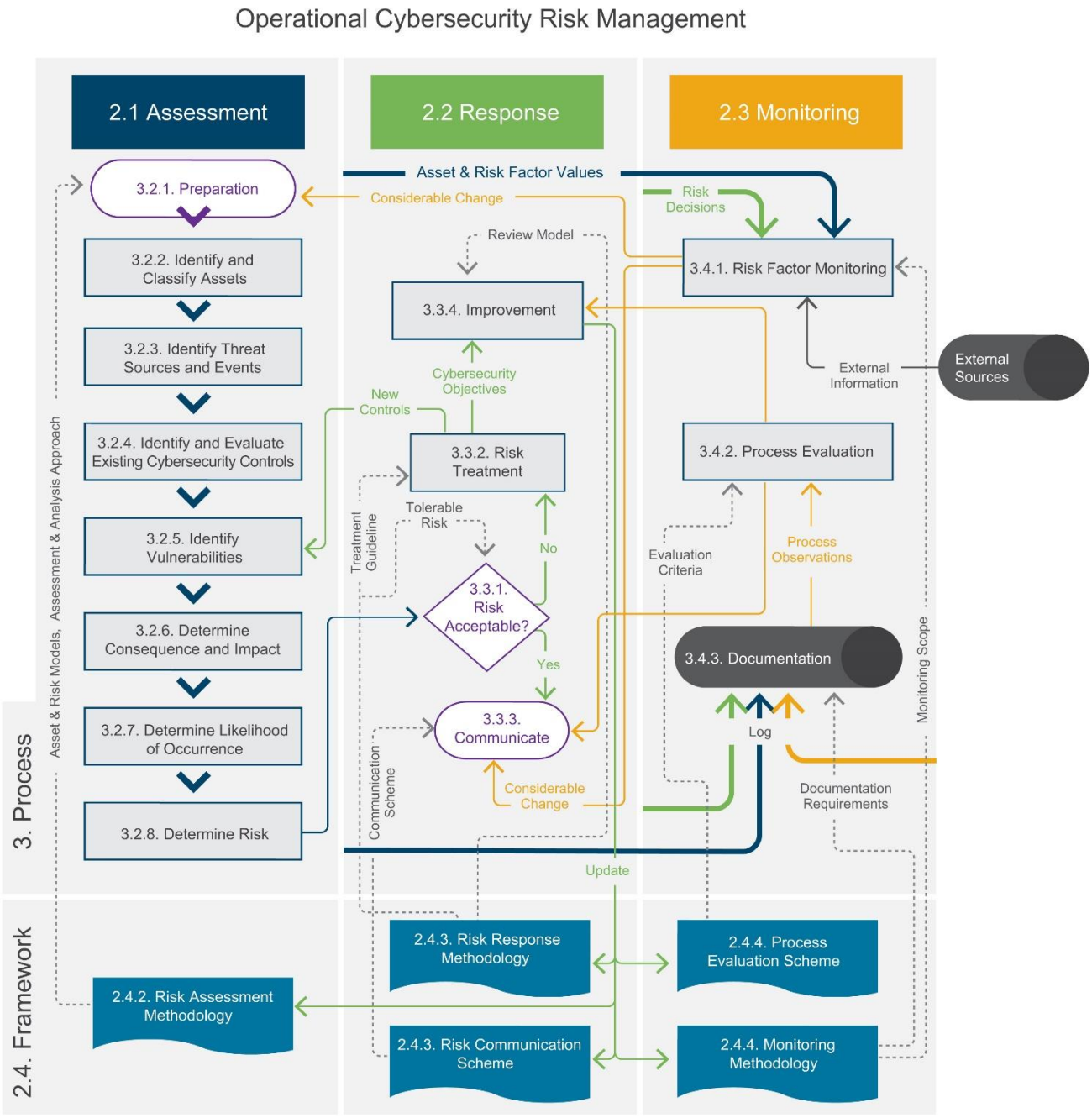


Figure 7: Example of the workflow among risk management components*

*The details of each item in this diagram are described in the noted section.

3.2 Conducting a risk assessment

Risk assessments are conducted periodically or based on need. Tasks related to the risk assessment process can be grouped into four major categories:

(i) prepare for the assessment
(ii) conduct the assessment
(iii) communicate assessment results
(iv) maintain the assessment results

Each of these categories can be divided into multiple steps. The latter two categories are covered in the risk response process that will be covered in Section 3.3. The former two categories are covered in the rest of this section and include preparing for and conducting the risk assessment. The structure of this section is influenced by NIST SP 800-30 [2] and ISO 27005 [3].

3.2.1 Preparing for a risk assessment

Input: History of previous risk assessments

Action: Identify the purpose of the risk assessment, which includes the intention for executing the assessment, the expected information in the report and the decisions that will depend on the assessment results.

Identify the scope of the risk assessment, which includes the effectiveness time frame of the report results and the applicability domain of the assessment.

Identify the constraints and assumptions about the elements of the assessment that need to be considered, e.g. focus on certain types of threats.

Identify the asset and risk models as well as the risk analysis and assessment approaches.

Identify the information sources about the risk factors, e.g. the source used to extract a list of vulnerabilities.

Output: Purpose, scope, assumptions, asset and risk models, assessment and analysis approaches and risk factor information sources.

Implementation guidance: Prior to conducting a risk assessment process, the risk assessment context is established at this stage. This context is a part of the risk framework that is either already developed in an organization (Section 3.1) or needs to be developed at this stage. In some cases, organizations may conduct various cybersecurity risk assessment instances in different contexts. In which case, the specific context needs to be picked from the risk framework at this stage.

The risk assessment context identifies organizational policies and requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors, the scope of these assessments, the rigour of analyses, the degree of formality and

requirements that facilitate consistent and repeatable risk determinations across the operational environment.

The **purpose of the risk assessment** needs to be explicitly stated in detail to support clear decision-making of risk management activities. The purpose of the risk assessment is influenced by the initiating cause of the risk assessment. If it is the initial assessment, the purpose of assessment can be establishing a risk baseline, identifying the risk factors or tracking their status overtime. If a reassessment is initiated because of a risk response decision, the purpose can be providing a comparative analysis for the alternative risk response actions or finding answers to a specific clarification request about risks or risk factors. If a reassessment is initiated because of a risk monitoring alarm, the purpose can be updating the risk baseline, determining effectiveness of existing cybersecurity controls, finding the effect of changes to the risk-related parameters in the operational environment, changing organizational policies, processes or objectives, resolving and performing a root-cause analysis of cybersecurity incidents or compliance requirements.

The **scope of the risk assessment**, determined by organizational officials and the risk management strategy, indicates the items that need to be considered in the risk assessment, e.g. field devices in the operational environment. The scope determines the range of information available to make risk-based decisions, decisions support by the assessment results, the assets and boundaries affected by the assessment and the way they are affected, effectiveness time frame of the results or what influences the need to update the assessment.

Specific **risk assessment assumptions and constraints** help to have greater clarity in the risk model, decrease subjectivity of measurements and increase reproducibility of risk assessment results. The key areas with assumptions relevant to risk assessment can include threat sources or threat events, assessment and analysis approaches, vulnerabilities and potential impacts.

The constraints in key areas related to the risk assessment can include priorities in operational or business functions, uncertainties, resources available for the assessment, skills and expertise required for the assessment, focus on certain types of threats or vulnerabilities and operational considerations related to operational or business activities. For example, assumptions about threat event impact evaluations can range from using worst-case scenarios to best-case scenarios. Impact criteria determines the evaluation method to be used for analyzing the impact, e.g. always consider the worst-case scenario impact.

A specific **asset and risk model, along with an assessment and analytics approach,** to use for conducting the risk assessment, need to be identified at this stage. Various assessment scales and algorithms to be used in different circumstances can be identified. For example, for low-impact assets, organizations could use qualitative values, while for moderate- and high-impact assets, semi-quantitative values (0-10) could be used.

There are various tools and methodologies available to help with some parts of the risk assessment workflow. For example, field-level risk assessment (FLRA) is an assessment method designed to examine operational and procedural systems to identify hazards and monitor risks.

The **sources of information** about risk factors need to be specified, which can be either internal or external to the organization. For instance, internal sources of information about threats and vulnerabilities can include risk assessment reports, vulnerability assessment reports, incident reports, security logs, IT/OT tickets and monitoring alarms.

For example, ICS-CERT provides information about identified threats and vulnerabilities across critical infrastructure. Figure 8 shows the number of reported ICS incidents, ICS incidents response deployments onsite and reported ICS vulnerabilities by ICS-CERT from 2010 to 2016 [4].

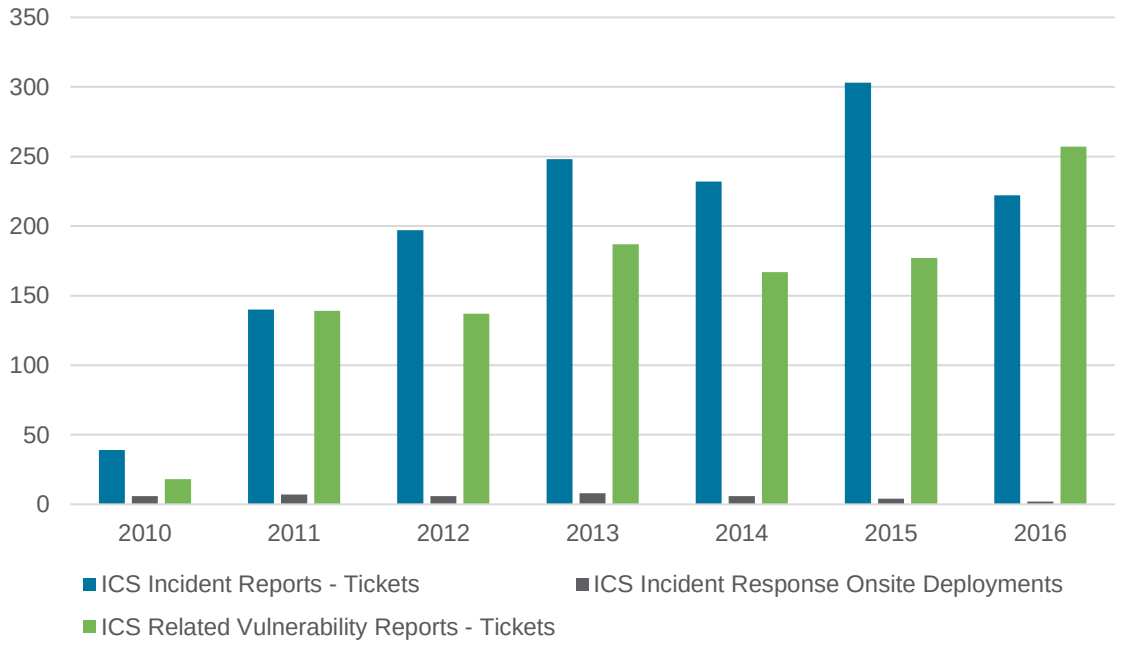


Figure 8: ICS-CERT reported incident by year

External sources of threat information can include cross-community organizations, sector partners, research and nongovernmental organizations, international forums and security service providers. The timeliness, specificity and relevance of threat information should be considered for external sources.

More information and examples can be found in Appendix D | Threat sources and events.

3.2.2 Identifying and classifying assets

Input: Scope and boundaries for the risk assessment to be conducted, asset model and list of constituents with owners, location, function, etc.

Action: The assets within the established scope should be identified, valuated, and their dependencies should be extracted according to the asset model.

Output: A list of assets with values and dependencies and a list of business processes related to assets and their relevance.

Implementation guidance: To identify assets, it should be considered that the scope of assets can include hardware, software, network, location, personnel, essential service, utilities, organizational structure and much more.

Asset identification should be performed at a suitable level of detail that provides sufficient information for the risk assessment. The level of details is defined in the asset model of the risk framework. The risk assessment scope may hold various levels of details for primary assets, their supporting assets and other assets.

An asset owner should be identified to be held responsible and accountable for the asset. The asset owner may not have property rights to the asset but is responsible for its production, development, maintenance, use and security.

The interdependency of the assets for different cybersecurity criteria (e.g., availability or safety) should be identified, and the processes that depend on assets need to be identified as well. The model of dependency is determined in the asset model. For example, the dependency of assets can be based on different zones for assets, or it can be based on individual types of services that are provided by each asset.

Asset valuation takes place on the assets that are in the scope of risk assessment by using the identified analytical model and the contribution of asset owners, cybersecurity specialists and, in some cases, process owners.

Appendix B | Asset profile provides more information and examples on identifying and valuating assets.

3.2.3 Identifying threats

Input: Information on threats obtained from incident event monitoring, asset owners and users and other sources identified in the risk assessment scope.

Action: Identify potential threat events and the threat sources that could initiate the events.

Output: A list of threats with the identification of threat type and source.

Implementation guidance: A threat has the potential to harm assets such as personnel, processes, systems and the organization. Threats can be accidental or intentional, and their origin can be natural, human, working culture, devices, systems or processes. A threat source can be from within or outside the organization. Threats should be identified based on the risk model in the risk assessment methodology. The threats can be classified by the type of source (e.g., insider,

nation states, cyber terrorists, script kiddies, hacktivists, etc.) or by the type of impact (e.g., environmental hazard, unauthorized actions, personnel safety, physical damage, technical failures). After threat classification, where required, individual threats within a class should be identified based on the scope of the risk assessment.

Some threats can affect more than one asset, and they can cause different impacts, depending on which assets are affected. Moreover, the dependency of assets may allow the threat to create a chain of impacts to different assets.

Multiple threat sources can initiate a single threat event, and a single threat source can potentially initiate multiple threat events. Therefore, the relationship between threat sources and events can be many-to-many, which can increase risk assessment complexity.

Input to the threat identification and valuation can be obtained from asset owners or users, human resources, facility management, and cybersecurity and physical security experts.

If a threat event is identified to be relevant, all potential threat sources could initiate the event. Each pairing of threat source and threat event can be identified separately, since the likelihood of threat initiation and success could be different for each pairing. Alternatively, the set of all possible threat sources that could potentially initiate a threat event can be identified.

Internal monitoring and investigation reports from incidents and past threat assessments should also be considered.

More information and examples on the identification cybersecurity threats can be found in Appendix D: Threat .

3.2.4 Identifying existing controls

Input: Documentation of controls, previous risk treatment implementation plans and their progress reports

Action: Existing and planned controls should be identified along with the assets they protect.

Output: A list of all existing and planned controls, their cybersecurity coverage type, assets that they cover, their implementation and usage status

Implementation guidance: Identification of existing controls should be made to understand the span and type of cybersecurity coverage there is for assets and to avoid unnecessary work or cost. Control effectiveness should be checked to understand what kind of protection is in place, other than having them on the shelves.

If a control does not work as expected, the protection potentially could be as effective as having no control in place or, sometimes, they can cause additional vulnerabilities, e.g., a weak authentication service can be used by the threat source as the origin of an unauthorized action.

Criticality of cybersecurity controls and the span of their coverage on assets should be determined, and the situations where they may fail in operation should be considered. This allows later identification of the places where complementary controls could be used to avoid the risk. The same process happens to the controls that are planned to be implemented.

An existing or planned control should be rated based on the risk assessment methodology in a qualitative or quantitative manner. If they are identified as unjustified or insufficient, the control should be checked to see whether it should be removed, replaced by another control or simply remain in place.

Some of the components that can be used to identify existing or planned controls are as follows:

- reviewing documents containing information about the controls (e.g. previous risk treatment implementation plans, cybersecurity assessment reports, procurement reports) that identify them, show their implementation status and identify the assets and processes that they intend to protect
- checking with the people responsible for operational or organizational cybersecurity (e.g., cybersecurity officer, IT manager, building manager or operations manager) and the users as to which controls are implemented (e.g., check their access rights)
- conducting an onsite review of the cybersecurity and physical controls, comparing those implemented with those that should have been implemented
- testing those implemented as to whether they are working correctly and effectively
- reviewing results of audits.

3.2.5 Identifying vulnerabilities

Input: A list of threats, lists of assets and existing controls

Action: Identify vulnerabilities that can be exploited by threat sources and the predisposing conditions that affect the likelihood of threat events that, despite existing cybersecurity controls, can cause harm to the identified assets.

Output: A list of vulnerabilities with an identified or unidentified relation to assets, threats and controls.

Implementation guidance: The presence of a vulnerability does not cause harm, as long as there is no threat to exploit them. A vulnerability that has no corresponding threat may not require implementing a control, but still needs to be identified and monitored for changes. Vulnerabilities arising from different sources need to be considered. New threats and vulnerabilities can be reported internally or published in external sources, e.g. specific forums.

Vulnerabilities can be related to asset properties and the deviation in asset use from its originally intended use.

Note that misused or incorrectly implemented controls can be ineffective or even be vulnerability themselves.

Vulnerabilities typically appear in:

- organizational information and control systems
- processes and procedures
- management routines
- personnel
- physical environment
- network environment
- system configurations
- hardware, software or communications equipment
- cybersecurity control systems
- dependence on external parties

A single threat event can occur because of the exploitation of multiple vulnerabilities, and a single vulnerability can cause multiple threat events. Therefore, the relationship between threat events and vulnerabilities can be many-to-many, which can increase the complexity of the risk assessment.

The severity and exposure of a vulnerability can later be derived from the assessment of risks and those impacts which are related to the vulnerability. This supports the prioritization of risk treatment decisions.

More information and examples about cybersecurity vulnerabilities can be found in Appendix E | Vulnerablities.

3.2.6 Analyzing consequence and impact

Input: A list of assets, processes, threats and vulnerabilities that are related to threats

Action: The consequences and potential incident scenarios of successful threat events should be identified, and the impact of different event scenarios on assets, processes and the organization should be analyzed based on the impact criteria and analysis approach.

Output: List of assessed impacts on assets, processes and the organization from successful threat events, along with the incident scenarios

Implementation guidance: The consequences to assets, processes and the organization that can be caused by successful threat events should be identified. The different potential incident scenarios should be determined and documented. The incident scenarios report should include the characteristics of the threat sources that could potentially initiate the events, the identified

vulnerabilities and predisposing conditions, the assets that could be negatively influenced by the event and the controls that are planned or implemented to prevent or delay the consequences.

The consequence of a successful threat event can be permanent, temporary or it can have other behaviours over time. The impact of these consequences can arise from different natures, e.g., financial, safety, environmental, reputation, etc.

The operational consequence of incident scenarios can be identified in terms of (but are not limited to):

- Environmental
- Health and safety
- Financial cost
- Regulatory enforcement
- Time lost
- Opportunity lost
- Skill lost or needs to recover
- Reputation lost

The impact of different incident scenarios should be determined and analyzed based on the impact criteria and analysis approach, which is determined in the preparation step. For example, the impact criteria may enforce the need to always consider adverse impacts.

Various impacts can have different natures and, as a result, they can be expressed in qualitative or quantitative forms. For example, some impacts can be assigned with a monetary value (i.e., repair costs), human value (i.e., cost of life), skill value, time value or others. However, it always helps to normalize them in a single scale for efficient decision-making.

At this stage, the numerical and relationship data provided from the previous steps will be used to analyze the impact of incident scenarios, e.g., asset valuation numbers, asset dependencies, control effectiveness, control coverage and vulnerabilities related to threats.

More information and examples about impact analysis can be found in Appendix F | Impact.

3.2.7 Determining incident occurrence likelihood

Input: A list of identified threat events and relevant incident scenarios with affected assets and exploited vulnerabilities, along with a list of all existing and planned controls with their effectiveness, intended asset coverage, implementation and usage status

Action: The likelihood of the incident scenarios that are identified based on the impact criteria should be calculated.

Output: Likelihood of incident scenarios causing the intended impact

Implementation guidance: A three-step process to determine the likelihood of incident scenarios needs to be executed:

1. Analyze the likelihood that threat events will be initiated by the threat source, which could be a natural cause, a cyber attacker, etc. This may involve cost-benefit analysis from the threat source perspective.
2. Analyze the likelihood of the threat event happening and causing different incidents scenarios despite the existence of cybersecurity controls.
3. Analyze the likelihood of incident scenarios successfully causing the impact that is identified in the impact criteria.

A combination of these three steps allows calculation of the likelihood of impacts. The assessment and analysis approach determine the scales and techniques to be used for impact calculations, e.g., taking the highest value from the three steps in a qualitative analysis, or multiplying the values of all three steps in a quantitative analysis.

Calculation of the likelihood in all three steps should reflect the following:

- frequency of exploiting attempts
- experience and applicable statistics for threat likelihood
- frequency of incidents
- effectiveness of controls
- complexity of exploiting the vulnerabilities
- for intentional threat sources: exploitation cost-benefit analysis from attacker perspective, skill level, motivation and available resources
- for unintentional threat sources: geographical factors, possibility of extreme weather conditions and factors that can influence human errors and equipment malfunction
- vulnerability severity and exposure level

3.2.8 Determining risk

Input: A list of incident scenarios, their impact and likelihood

Action: Determine cybersecurity risks from threat events considering the impact and the likelihood of the events.

Output: A list of risks with assigned values and prioritized according to the risk assessment criteria

Implementation guidance: Using the values assigned to the likelihood and impact of an incident scenario, the risk analysis assigns value to the identified risk. Each estimated risk is a combination of one or multiple incident scenarios, their likelihood and impact. Some related minor risks can be aggregated to form fewer major risks.

More information and examples about calculation of risk can be found in Appendix H | Risk.

3.3 Responding to risk

Risk response is a reactive process that makes decisions and conveys them based on the output of different evaluations that have been performed through risk monitoring and assessment processes.

Risk response activities can be grouped into four different categories:

3.3.1 Accepting risk

Input: list of risks with assigned value levels, organizational risk tolerance, cost-benefit assessment of in-place and potential assets, processes and controls, operational importance and priorities.

Action: The level of each risk should be compared against risk acceptance criteria and decisions should be made for each risk.

Output: A list of risks, prioritized according to incident scenarios that lead to those risks, along with risk treatment decisions, including potential target risk levels and the rationale for selecting the treatment options

Implementation guidance: The nature of the decisions related to the identified risks is decided when establishing the context of risk acceptance in the risk framework. These decisions should be revisited in more detail at this stage when more is known about individual identified risks. The individual estimated risks should be compared with the risk acceptance criteria.

Decisions taken in the risk acceptance activity are mainly based on the acceptable level of risk. They also depend on organizational preference of relying on some specific risk factors, such as consequences and likelihood, and the degree of confidence in the risk identification.

At this point, aggregation of multiple low or medium risks that can result in higher overall risks should be addressed accordingly.

If the level of risk meets the risk acceptance criteria, there is no need for implementing additional controls. Most often in these cases, the organization only needs to consider decisions to maintain the level of risk to stay at the same level.

In the decision-making process, the importance of cybersecurity properties and business processes or activities supported by a particular asset should be considered. If one cybersecurity criterion is not relevant for the environment (e.g., loss of confidentiality), then all risks impacting this criterion may not be relevant. If the process is determined to be of low importance, risks associated with it should be given lower consideration.

However, justification for risk treatment decisions are broader than solely economic considerations and should reflect all the organization's obligations, voluntary commitments and stakeholder views. Decisions that can be made in this activity can include:

- whether an activity should be undertaken to mitigate the risk, e.g., taking extra cybersecurity controls
- priorities for risk treatment considering estimated levels of risks
- accepting the risk as is
- demanding further analysis
- shutting down services, activities or processes
- maintaining existing risks or controls
- sharing the risks and responsibilities with internal or external parties
- changing cybersecurity objectives

As a rule in risk treatment decision-making, the extreme consequences of risks should be made as low as reasonably practicable and irrespective of any absolute criteria. In the case of rare but severe risks, justification of implemented controls does not need to be only on strictly economic grounds.

If it is decided to treat a risk, the selection of risk treatment options should be made and prioritized in accordance with the organization's objectives, risk criteria and available resources.

When selecting risk treatment options, the values, perceptions and potential involvement of stakeholders and the most appropriate ways to communicate and consult with them should be considered.

3.3.2 Treating risk

Input: prioritized list of risks with potential risk scenario and risk treatment decision, current risk values and target risk values, and cost-benefit assessment of in-place and potential assets, processes and controls related to each risk; rationale for the selected risk treatment options, including expected benefits

Action: The risk treatment plan should be defined for the decisions that have been made. Implement controls to reduce, retain, avoid or share the risks.

Output: implementation report in respect to the risk treatment plan, residual risks subject to the risk acceptance decisions and escalation report with details of unmitigated risks in order to change cybersecurity objectives

Implementation guidance: The purpose of risk treatment is to implement the chosen risk treatment option. Treatment planning instructs the way treatment will be implemented, so arrangements are understood by those involved. The treatment plan should specify the order in

which risk treatment actions should be implemented and implementation progress against the plan should be monitored.

Appropriate stakeholders from organizational and operational tiers should be involved in developing treatment plans in order to have integrated risk management plans, processes and communications.

The risk treatment plan should include:

- roles and responsibilities for approving and implementing the plan
- approval and communication model
- proposed actions
- resources required, including contingencies
- performance measures
- constraints
- required reporting and monitoring
- when actions are expected to be undertaken and completed

All stakeholders should be aware of the nature and extent of the remaining risk after the risk treatment is implemented. The remaining risk should be documented and subjected to monitoring, review and, where appropriate, further treatment.

Cybersecurity controls can provide the following types of protection: correction, elimination, prevention, impact minimization, deterrence, detection, recovery, monitoring and awareness.

During control selection to mitigate risks, it is important to weigh the cost of acquisition, implementation, administration, operation, monitoring and maintenance of the controls against the value of the assets being protected. Furthermore, the return on investment in terms of risk reduction and potential to exploit new business opportunities afforded by certain controls should be considered. Additionally, consideration should be given to specialized skills that may be needed to define and implement new controls or modify existing ones.

There are many constraints that can affect the selection of controls. Technical constraints such as performance requirements, manageability (operational support requirements) and compatibility issues can hamper the use of certain controls or can induce human error, either nullifying the control, giving a false sense of security, or even increasing the risk beyond not having the control (e.g., requiring complex passwords without proper training, leading to users writing down passwords). Moreover, it can be that a control affects performance. Managers should try to identify a solution that satisfies performance requirements, while guaranteeing sufficient information security. The result of this step is a list of possible controls with their cost, benefit and priority of implementation.

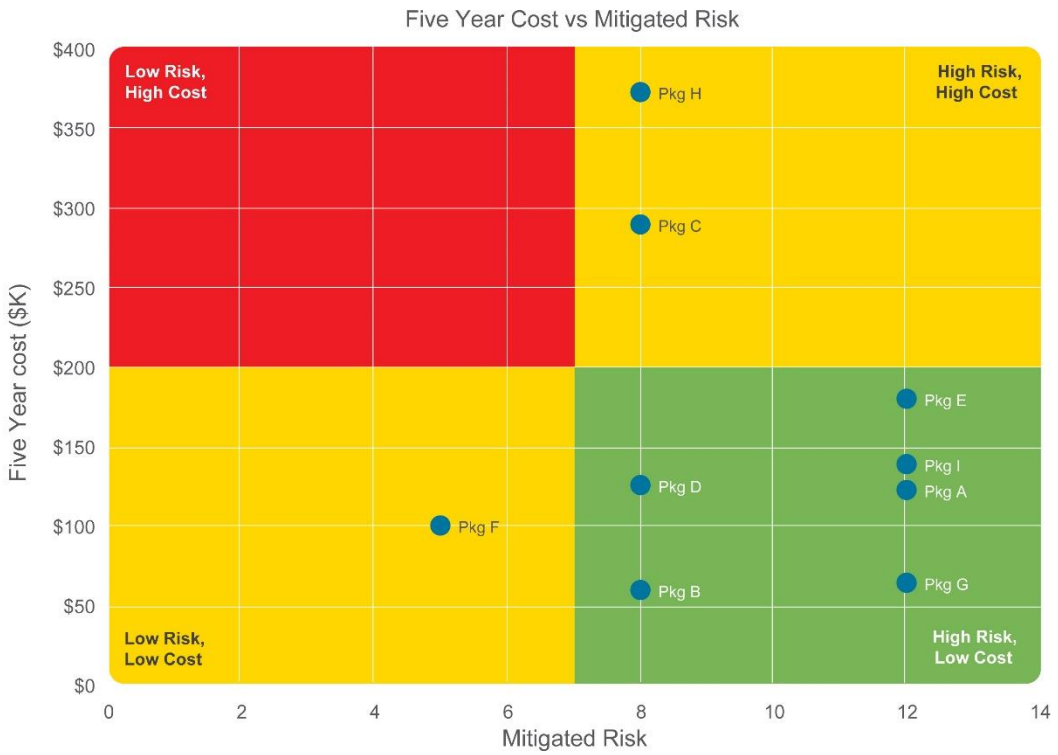


Figure 9: Risk treatment cost-benefit example

Figure 9 shows one of the most popular ways to navigate the priority of risk packages and their treatment decisions. Risks in the green zone have the highest priority and those in the red zone have the lowest priority to treat or mitigate.

Various constraints should be considered when selecting controls and during implementation. Typically, the following are considered:

- time constraints
- financial constraints
- technical constraints
- operational constrains
- cultural constraints
- ethical constraints
- environmental constraints
- ease of use
- personnel constraints
- constraints for integrating new and existing controls

If there are no treatment options available, or if treatment options do not sufficiently modify the risk, the risk should be recorded and kept under ongoing review. The potential decisions for this case can be:

- changing cybersecurity objectives
- avoiding the risk by removing services, operations or systems
- sharing the risk with another party that can manage the risk more effectively

These decisions can be costly, create new risks or modify existing, identified risks. Therefore, additional risk treatment may be necessary.

3.3.3 Communicating risk

Input: all risk information obtained from the cybersecurity risk management processes, including decisions, results, monitoring events, etc.

Action: Information about cybersecurity risks and risk activities should be exchanged or shared between the decision-maker and other stakeholders.

Output: ongoing and comprehensive understanding of cybersecurity risk management decisions, processes and results

Implementation guidance: Risk communication is a risk management activity that spans through all risk activities in monitoring, assessment and response processes. Risk communication is necessary to manage risks by exchanging or sharing information about risks between the decision-makers and other stakeholders. The information includes, but is not limited to, the characteristic of cybersecurity risks; risk treatment plan, progress and results; risk acceptance of risks and decisions; risk improvement process and results; risk management process evaluation results; and cybersecurity risk factor events.

Risk communication plans should be developed for normal operations and emergency situations. Risk communication activities should be performed continually. It is important to designate a communication unit within the organization to coordinate all risk-related communications and make sure all stakeholders and processes concur with it.

Communication among stakeholders is very important, as it can have significant impact on decisions to be made and ensures that those responsible for implementing risk management, and those with interest, understand the basis on which decisions are made, what particular actions are required to be carried out and how to perform them. Perceptions of risk can vary due to differences in stakeholder assumptions, concepts, needs, issues and concerns. They are likely to make judgments on the acceptability of risk based on their perception. It is especially important to ensure that the perception of stakeholders about risk and benefits is identified, justified, documented and clearly understood and addressed.

Communication between risk management activities and processes is critical for effective operation of overall risk management. It is important that the scope, expectations, requirements, format and regulations about reports, alarms, thresholds, reviews, activity initiations and operational decisions are clearly defined, understood and implemented.

Risk communication benefits risk management in the following ways:

- informs responsibilities and enforces accountability for decision-makers and stakeholders about risks
- collects risk information
- obtains new cybersecurity knowledge and enough oversight to support decision-making
- brings different areas of expertise together for each step of the risk management process
- ensures that different views are appropriately considered when defining risk criteria, evaluating risk, reviewing processes and making decisions about risks
- coordinates with other parties and plans responses to reduce consequences of any incident
- coordinates operation of different risk activities, such as sharing the results from the risk assessment and presenting the risk treatment plan
- reduces occurrence and consequence of cybersecurity breaches due to the lack of mutual understanding among decision-makers and stakeholders
- improves awareness and builds a sense of inclusiveness and ownership among those affected by risk
- informs near misses, substandard conditions, substandard practices and deviance from standard procedures
- gets help from experts and resources to mitigate or share risk

Organizations can provide guidance and educate decision-makers on how to capture and present information produced by different risk assessment processes. For example, using a defined organizational template for a risk assessment report or using a defined template for describing threat events to identify how each event could potentially harm organizational operations and assets, individuals or the nation.

3.3.4 Reviewing and improving

Input: evaluation, ongoing progress and final reports for all risk management processes, scheduled tasks and activities

Action: Procedures, actions, measurements, expectations, communications, deliveries, monitoring, documentation, evaluations and decisions-making processes should be reviewed from an effectiveness perspective to improve or maintain them.

Output: continual updating of risk framework components, responsibilities, requirements, procedures, controls or tools

Implementation guidance: The organization should make sure that the cybersecurity risk management processes and related activities remain effective by periodically reviewing them based on the input received from monitoring and evaluating different processes. Then, decisions should be made with the managers and cybersecurity specialists to improve current risk management processes, so the criteria used to measure the risk and risk management processes are still valid and consistent with business objectives, strategies and policies according to the constantly changing nature of the business context.

The factors that are considered in improvement include (but are not limited to):

- changes identified
- risk assessment iterations
- cultural behaviors
- objectives of the cybersecurity risk management process (e.g., business continuity, resilience to incidents, and compliance)

As a result of process improvement, any of the following can happen to the approaches, methodologies, procedures or tools:

- updating risk framework
- updating processes and communications
- demanding risk assessment
- demanding changes to the organizational risk framework and cybersecurity strategy

These improvements should help enhance the cybersecurity risk management practice. All improvements to process guidelines should be reflected in the risk framework, appropriate managers should be notified of the procedures that need to be improved and deployment of those changes need to be verified in order to make sure that:

- no risk or risk element is overlooked or underestimated
- the best possible necessary actions are taken
- risk management activities are adaptable to the changes exposed to the organization
- a realistic risk understanding is provided to decision-makers
- the necessary ability to respond to risks is present

This review activity should address (but is not be limited to):

- business context
- risk assessment approach
- asset profile and cost of ownership
- risk impact criteria
- risk process evaluation criteria

- risk acceptance criteria
- necessary resources
- new identified vulnerabilities
- cybersecurity controls
- measured communication and documentation metrics
- risk tolerance
- risk treatment options

Moreover, the organization should ensure that risk assessment and risk treatment resources are continually available to review risk, to address or change new threats or vulnerabilities and to advise management accordingly.

The organization should review all risks and risk treatment options regularly and when major changes happen. Risk treatments, even if designed and implemented carefully, might not produce the expected outcomes and could produce unintended consequences.

Process and risk review need to be an integral part of the implementation of each process to give assurance that the different forms of processes, communications, decisions and treatments become and remain effective.

3.4 Monitoring risk

Risk monitoring is a live process that continuously observes all cybersecurity risk management events based on the scope that is defined in the risk framework. The observed events are documented or communicated according to risk framework requirements.

Risk monitoring activities can be grouped into three different categories as follows:

3.4.1 Monitoring risk factors

Input: value of assets, risk factors (i.e., threats, controls, vulnerabilities, impacts, likelihood of occurrence), risks, risk treatment and acceptance decisions, risk-related communications and information about the operational environment from internal and external sources

Action: Assets, risk factors and risks should be monitored and evaluated to identify any changes in the context of the organization and to maintain an overview of the complete cyber risk picture.

Output: initiating risk assessment by identifying considerable changes; communicating to proper stakeholders based on the level and type of changes detected on assets and risk factors; or logging the identified changes

Implementation guidance: The scope and requirements of the asset model, the risk model, the risk assessment approach, the risk analysis approach, risk acceptance, risk communication, risk

treatment, risk documentation and framework of risk factor monitoring should be extracted from the risk framework in order to design a process that complies with all of them.

Risk processes, even if designed and implemented carefully, might not produce the expected outcomes and could produce unintended consequences. Monitoring needs should be an integral part of the risk process implementation to give assurance that the various forms of risk actions become and remain effective.

The organization controls some changes to the inputs of this activity (e.g., assets), and some changes can happen without notice, such as threats, vulnerabilities, likelihood or consequences and therefore, the risks. As such, constant monitoring is necessary to detect considerable changes as early as possible.

In this process, it is necessary to ensure that the following are constantly monitored in information and IACS systems and the operational environments[4]:

- assets that have been included in the risk management scope, using the measures defined in the risk framework
- necessary modification of assets and asset values, e.g., due to changes in environment and requirements
- new potential threats outside and inside the organization that have not been assessed
- defined measures to evaluate the effectiveness of controls in place, e.g., frequency of incidents
- possibility that raising vulnerabilities allow threats to exploit them
- identified vulnerabilities to determine those getting exposed to new or re-emerging threats
- increased impact or consequences of assessed threats, vulnerabilities and risks in aggregation resulting in an unacceptable level of risk
- the status of operational systems based on measures defined in risk framework for cybersecurity incidents to update risk factors such as, new threats, new vulnerability, update on likelihood and risk
- the results of system evaluations, such as penetration testing, security control assessment, identity and access assessment, etc.

Change in risk factors can change risks that have already been assessed. Review of low and accepted risks should consider each risk separately, and all such risks as an aggregate as well, to assess their potential accumulated impact. If risks do not fall into an acceptable risk category as defined in Section 3.3.1, they should be treated as in Section 3.3.2.

Major changes should be a reason for a more specific review. Therefore, risk monitoring activities should be repeated regularly or constantly. The outcome of risk monitoring activities indicates the

[4] Based on recommendations of ISO 27005 [3]

level of changes based on the risk framework (e.g., major and minor), and this is input to other risk review activities.

3.4.2 Evaluating the risk management process

Input: risk treatment logs and acceptance decisions, risk-related communications, output of risk assessment processes and recorded system observations, including incident behavior, output of the risk factor monitoring process, the documentation process and information about the operational environment from internal and external sources.

Action: All risk management processes should be continually monitored, and their effectiveness should be evaluated, along with their interdependency with the operational environment and other processes.

Output: initiating review and improvement process by identifying effectiveness measures and protentional gaps; communicating to proper stakeholders based on the level and type of gaps detected in the process; or logging the identified process analysis and gaps.

Implementation guidance: The process evaluation framework should be extracted from the risk framework to design effectiveness measures for all risk management processes. Effectiveness metrics for each process should be designed with respect to the scope and requirements of that process, which is specified in its related component of risk framework.

The risk management evaluation processes should monitor all processes on a continual basis, and it should include (but not be limited to):

- regularly verifying that the criteria used to measure the risk and its elements are still valid and consistent with business and cybersecurity objectives, strategies and policies
- ensuring that cybersecurity requirements are derived from, and traceable to, organizational business functions
- verifying compliance with federal legislation, directives, regulations, policies, standards and guidelines
- regularly verifying that changes to the business context are taken into consideration adequately during the cybersecurity risk management process
- checking whether the planned and in-place risk responses are addressing the risks identified by the risk assessment process
- monitoring the risk-related communication flow and measuring the effectiveness of the decision escalation flow
- checking risk acceptance to ensure it is in line with the business strategy
- monitoring the effect of changes in different risk responses on behavior of cyber incidents
- monitoring resource availability for risk response in respect to identified risk levels
- evaluating the effectiveness of the risk factor monitoring process

- evaluating asset classification and the valuation process
- evaluating the soundness of the risk assessment approach
- evaluating documented patterns, logs and reports to extract near misses, substandard conditions, substandard practices and deviance from standard procedures
- evaluating documented and non-documented details of processes, incidents and log files to identify culture and competency gaps in various processes.

The risk management evaluation process is the intelligence brain in risk management. This evaluation analyzes individual and overall processes. The risk management evaluation should have specific metrics and thresholds for process effectiveness. The evaluation determines whether to call on process review and improvement (Section 3.3.4) and communicates to relevant stakeholders (Section 3.3.2) based on the value of those metrics.

3.4.3 Documenting risk

Input: the data from every single process, inter-process interactions and information about the operational environment from internal and external sources.

Action: A selected portion of input data from all other processes should be securely recorded and reliably available.

Output: feeding the observed data to the risk management evaluation process, the review and improvement process, risk factor monitoring processes, risk assessment processes and the risk communication process

Implementation guidance: Risk management processes and their outputs should be documented through an appropriate mechanism. In this process, the scope, criteria, factors and metrics of documentation are taken from documentation requirements of the risk framework. This mechanism should select some factors from the data generated by each process, which allows comprehension, investigation, analysis and repetition of considerable events within that process or inter-process communications.

All events, changes, results, risk factors, regulations, thresholds, requirements, decisions, responses, effects, processes and communications get recorded accordingly.

REFERENCES

[1] "NIST Special Publication 800-39, managing information security risk: Organization, mission, and information system view," National Institute of Standards and Technology, 2011.

[2] "NIST Special Publication 800-30 - Guide for Conducting Risk Assessment," National Institute of Standards and Technology, 2012.

[3] "ISO/IEC 27005 - Information Security Risk Management," International Organization for Standardization, 2018.

[4] "ICS-CERT Landing | CISA," [Online]. Available: https://www.us-cert.gov/ics.

[5] "CSA Z1002: Occupational health and safety - Hazard identification and elimination and risk assessment and control," CSA, 2017.

[6] "ISO 31000: Risk Management - Guidelines," International Organization for Standardization, 2018.

[7] "NIST Special Publication 800-82 - Guide to Inductrial Control Systems (ICS) Security," National Institute of Standards and Technology, 2015.

[8] "Open Risk Analysis Technical Standard (O-RA)," The Open Group, 2013.

[9] "ISO 31010: Risk Management - Risk Assessment Techniques," International Organization for Standardization, 2019.

[10] "ISA-62443-3-2 Security Risk Assessment and System Design," International Society of Automation, 2018.

Natural Resources Canada

Apendix

A Glossary

In this section, there are cybersecurity risk management concepts that are either mentioned in the body of the document or are related topics to cybersecurity risk management.

A.1. Glossary

- **Threats** are any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation), assets, IACS, individuals, other organizations or the community through an information, automation, monitoring or control system via intentional or unintentional unauthorized access, destruction, disclosure of information, modification of information or decision flow, malfunction, modification of workload or control path or denial of service.
- **Threat events** are caused by a single or multiple threat sources. A **threat source** is characterized as the intent and method targeted at the exploitation of a vulnerability, or a situation and method that may accidentally exploit a vulnerability. In general, types of threat sources include hostile cyber or physical attacks, human errors of omission or commission, structural failures of organization-controlled resources (e.g., hardware, software, environmental controls) and natural and man-made disasters, accidents and failures beyond the control of the organization. Multiple subsets of threat sources can initiate or cause the same threat event.

  In different standards, some other terminology is used for threat events and threat sources. For example in CSA Z1002 OHS [5], **Harm** is defined as physical injury or damage to health, which is captured as threat event above; and **Hazard** is defined as a potential source of harm to a worker, which is captured as threat source above.
- **Threat vector** is the path, paths or means by which a threat source can make the threat happen.
- **Threat scenario** describes how the events caused by a threat source can contribute to or cause harm. Development of threat scenarios is analytically useful, since some vulnerabilities may not be exposed to exploitation unless and until other vulnerabilities have been exploited. Analysis that illuminates how a set of vulnerabilities, taken together, could be exploited by one or more threat events is therefore more useful than the analysis of individual vulnerabilities.
- **Threat landscape** is a summary of all available threat information, such as threat event, source, vectors and trends that may affect a defined target (i.e., organizational operations, assets, IACS, individuals, other organizations or the community).
- **Threat shifting** is the response of adversaries to perceived safeguards or cybersecurity controls, in which adversaries change some characteristic of their intent or targeting in order to avoid or overcome those safeguards or security controls.
- **Vulnerability**: any weakness in a system (information, automation, monitoring or control system), system security procedures, internal controls or implementation that could be exploited by a threat source. Most information, automation, monitoring and control system vulnerabilities can be associated with security controls that either have not been applied (either intentionally or unintentionally) or have been applied but retain some weakness.

  Vulnerabilities can also be inherited from organizational risk management, for example they could be found in organizational governance structures (e.g., the lack of effective risk

management strategies and adequate risk framing, poor intra-agency communications, inconsistent decisions about relative priorities of missions or business functions, or misalignment of enterprise architecture to support mission or business activities), external relationships (e.g., dependencies on particular energy sources, supply chains, technologies, and telecommunications providers), business processes (e.g., poorly defined processes or processes that are not risk-aware) and enterprise or information security architectures (e.g., poor architectural decisions resulting in the lack of diversity or resiliency in organizational information systems).

- **Likelihood**: the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event results in adverse impacts).

  For adversarial threats, an assessment of likelihood of occurrence is typically based on adversary intent, adversary capability and adversary targeting. For other than adversarial threat events, the likelihood of occurrence is estimated using historical evidence, empirical data or other factors.

- **Impact**: the level of impact from a threat event is the magnitude of harm that can be expected to result from consequences of cybersecurity violations by a variety of organizational and non-organizational stakeholders.

  For the impact analysis, it is important to define and document the process used to conduct impact determinations, assumptions related to impact determinations, sources and methods for obtaining impact information, and the rationale for conclusions reached by impact determinations.

- **Risk**: risk is a function of the likelihood of a threat event's occurrence and potential adverse impact when the event occurs. This broad definition also allows risk to be represented as a single value or as a vector of values, where different types of impacts are considered separately. In this definition of risk, all the above risk factors are involved.

  Risks can be grouped into some categories based on a combination of the risk factors. The most popular way to categorize risks is based on impact categories. Some typical high-level categories of risks based on impact are financial, reputational, legal, safety and environmental.

- **Predisposing condition** is a condition that exists within an organization, a mission or business process, enterprise architecture, information system or environment of operation that affects the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, other organizations or the nation. Some vulnerabilities can be caused by predisposing conditions.

- **Aggregation** is a way to group multiple discrete or lower-level risks together into a more general or higher-level risk. In aggregating risks, the relations between various risks should be considered. The risks with more similarity, such as in category of risk or causality sequence of risk, can be aggregated more easily.

- **Cybersecurity control** is an action, tool, procedure or technique that reduces a cyber threat, vulnerability or attack, by reducing the harm it can cause or by increasing visibility over cyber incidents in order to take corrective actions.
- **Uncertainty** is inherent in the risk assessment process due to considerations such as: (i) possible assets, processes, cybersecurity controls and human factors in the system life cycle that have not been scoped; (ii) imperfect or incomplete knowledge of the threat (e.g., characteristics of adversaries including tactics, techniques and procedures); (iii) undiscovered vulnerabilities in processes, technologies and systems; (iv) unrecognized dependencies, which can lead to unforeseen impacts; and (v) limitations on the extent of the future resembling the past.

  The degree of uncertainty in risk assessment results can be communicated in the form of the results or be potentially reduced by some risk analysis techniques.

BBA

Natural Resources Canada

Apendix

B Asset profile

In this appendix, asset identification and valuation are described in more detail based on the ISO/IEC 27005 [3] method and examples are provided.

B.1 Asset identification

In this example two kinds of assets are distinguished:

- primary assets:
  - business processes and activities
  - operational
- supporting assets, on which the primary assets rely:
  - hardware
  - software
  - network
  - location
  - essential services
  - utilities
  - personnel
  - organization's structure

Identification of primary assets

This activity consists of identifying the primary assets by managers, cybersecurity specialists and users. In this example, the two types of primary assets are identified:

- Business processes and activity examples:
  - processes whose loss, or interruption prevents the organization to carry out the mission
  - processes that, if modified, can greatly affect the accomplishment of organizational missions
  - processes that are necessary to comply with contractual, legal and regulatory requirements
- Operational asset examples:
  - vital systems to keep business production running
  - systems that are critical to personnel safety
  - preventive systems for environmental hazards
  - information systems that contain strategic information for achieving business objectives or personal information that are required by regulatory authorities to be kept safe

The assets that have not been identified as sensitive after this point, have no defined classification. This means that even if those assets are compromised, the organizational mission can still be accomplished.

However, they normally inherit the controls that have been identified to protect sensitive assets.

Identification of supporting assets

This activity consists of identifying the assets that the primary assets depend on, and if they were compromised, the primary assets could be impaired. Here is an example of different types of the supporting assets:

- Hardware:
  - Field devices: devices that are in direct contact with production line, e.g., actuator, valve and thermostat
  - Control system equipment: devices in charge of using and regulating the behavior of field devices
  - Transportable equipment: portable computer equipment
  - Fixed equipment: computer equipment used on the organization's premises
  - Processing peripherals: equipment connected to a computer via a communication port for entering, conveying or transmitting data, such as printers
  - Data medium: these are media for storing data or functions
  - Other media: static, non-electronic media containing data
- Software:
  - Operating system: all the programmes of a computer making up the operational base from which all other programmes are run
  - Service, maintenance or administration software: software that complements the operating system services, e.g., web services, backup services, malware protection services, etc.
  - Business application: applications that give users direct access to the services and functions they require from their information or operation systems in their professional context, e.g., control system software, accounts software, etc.
- Network:
  - Medium and supports: communications and telecommunications media or equipment are characterized mainly by the physical and technical characteristics of the equipment and the communication protocols, e.g., ethernet, WiFi 802.11, ADSL, FireWire, etc.
  - Relay devices: all devices that are intermediate in communications; these devices often include routing and/or filtering functions and services, employing communication switches and routers with filters, e.g., router, hub, switch, etc.
- Location:
  - External environment: all locations in which the organization's means of security cannot be applied, e.g., urban area, hazard area and personnel’s home

  - Premises: environments controlled by the organization that are bounded by a perimeter directly in contact with the outside, e.g., building
  - Zone: physically protected boundary forming partitions within the organization's premises, e.g., server room and control room
- Essential services: all services required for the organization's equipment to operate
- Utilities:
  - Services and means required for providing power to information/operation equipment and peripherals, e.g., power supply
  - Water supply
  - Waste disposal
- Personnel:
  - Decision-maker: owners of primary assets, organizational managers or project managers
  - Users: personnel who have special access to the systems to handle sensitive elements in the context of their activity and who have a special responsibility in this respect, e.g., human resource managers and control system operators
  - Operation/maintenance staff: personnel who have special access to the systems in order to operate and maintain the operation or information systems, e.g., system administrator, back-up operator, application deployment operator
  - Developers: personnel with high-level access in developing the organization's applications; they do not act on the production data
- Organization:
  - Organization’s structure: the various branches of the organization, including its cross-functional activities, under the control of its management, e.g., human resources management, IT management, purchasing management, business unit management, building safety service, fire service and cybersecurity
  - Subcontractors/suppliers/manufacturers: other entities that provide the organization with a service or resources and bound to it by contract, e.g., material suppliers and consultancy companies

Dependencies

Dependencies of assets, on business processes and other assets, should be identified, since this can influence the values of the assets. The more business processes supported by an asset, the greater the value of the asset is.

The dependencies across assets can be categorized into five criteria: confidentiality, integrity, availability, reliability and safety. Note that one asset can depend on another asset in one criterion and have no dependency in a different criterion. For example, from safety perspective, a valve depends on the control system. If the control system gets compromised, then the valve can

potentially cause harm to personnel. While from a confidentiality perspective, there is no dependency between the valve and the control system. Figure 10 and Figure 11 illustrate other examples of dependencies between some assets from an integrity and availability perspective.

Information about dependencies helps to assure that the true value of the assets (through the dependency relationships) is given to the assets.

If the values of the dependent asset are greater than the value of the asset considered, then the value of the considered asset should be increased according to:

- the degree of dependency
- the values of the dependent assets

Identification of asset dependencies will later assist with the identification of threats and vulnerabilities in risk assessment process and indication of the appropriate level of protection in risk treatment process.

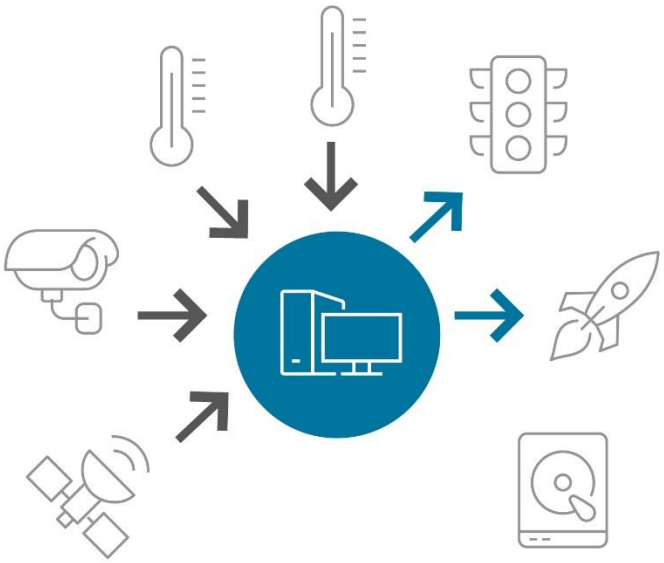


Figure 10: Example of dependencies between assets from an integrity perspective

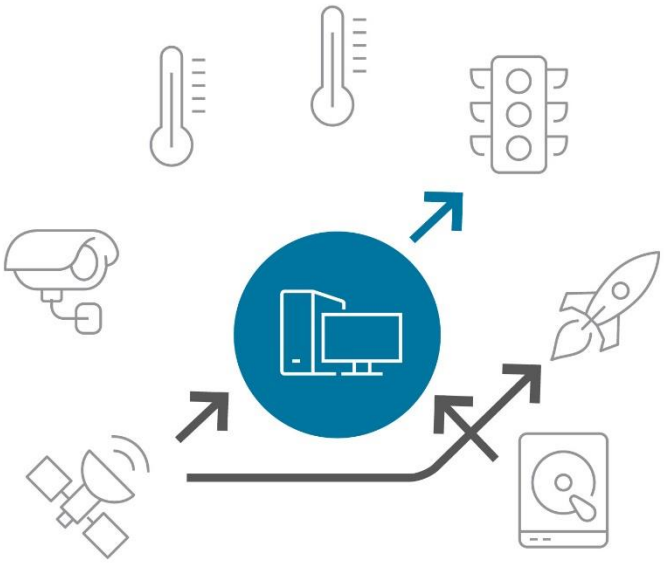


Figure 11: Example of dependencies between assets from an availability perspective

B.2 Asset valuation

After asset identification, it is time to agree on the scale to be used for assigning values to assets and then the criteria for assigning a specific value on that scale to each asset. Some assets have

a known monetary value, and others have a more qualitative value, for example, ranging from “very low” to “very high”. The organization decides to use quantitative or qualitative scale based on the characteristics of each asset, needs for security, organizational size and other organization specific factors. Both valuation types can be used for the same asset.

Criteria

The criteria used as the basis for assigning a value to each asset should be clearly stated. This is often one of the most difficult steps of asset valuation, as the values of some assets may have to be determined by multiple individuals, and at the same time being subjective.

Possible criteria to determine an asset’s value can include the following:

- its original cost
- its replacement or re-creation cost
- the value of an organization’s reputation
- the costs incurred due to the loss of confidentiality, integrity, availability or safety
- the costs incurred due to the loss of non-repudiation, accountability, authenticity or reliability

Some assets can have multiple values assigned from different perspectives. For example, a line of products can be valued based on labour expended or based on its value to a competitor. The assigned value can be the maximum, the sum of some, or all of the possible values.

Scale

In the next step, the organization should agree on a general scale. First, the number of levels in the scale should be decided. The more levels, the more granular the scale is. It is important to have a consistent approach throughout the whole risk assessment process. Normally, any number of levels between 3 and 10 (e.g., low, medium and high) can be used.

These levels should be assessed according to the criteria selected (e.g., for possible financial loss, they should be given in monetary values, and possibly for personal safety, some other criteria of values should be selected).

Finally, the organization decides to define the limits of each level, i.e., what is considered a “low” or “high” consequence. Note that same consequences can have different levels, if different organizations. An example of asset levels is shown in Table 1: Example of asset value levels.

Table 1: Example of asset value levels

Level	Rate	Description
High	3	The value of asset based on business objectives is high in comparison with other similar assets.
Medium	2	The value of asset based on business objectives is average in comparison with other similar assets.

Level	Rate	Description
Low	1	The value of asset based on business objectives is low or nonexistent in comparison with other similar assets.

Reduction to common baseline

All asset valuations need to be reduced to a common base. This can be done based on the impact of the possible consequence categories, such as loss of confidentiality, integrity, availability, safety, non-hazardous, non-repudiation, accountability, authenticity or reliability of assets.

Some examples of those consequences are:

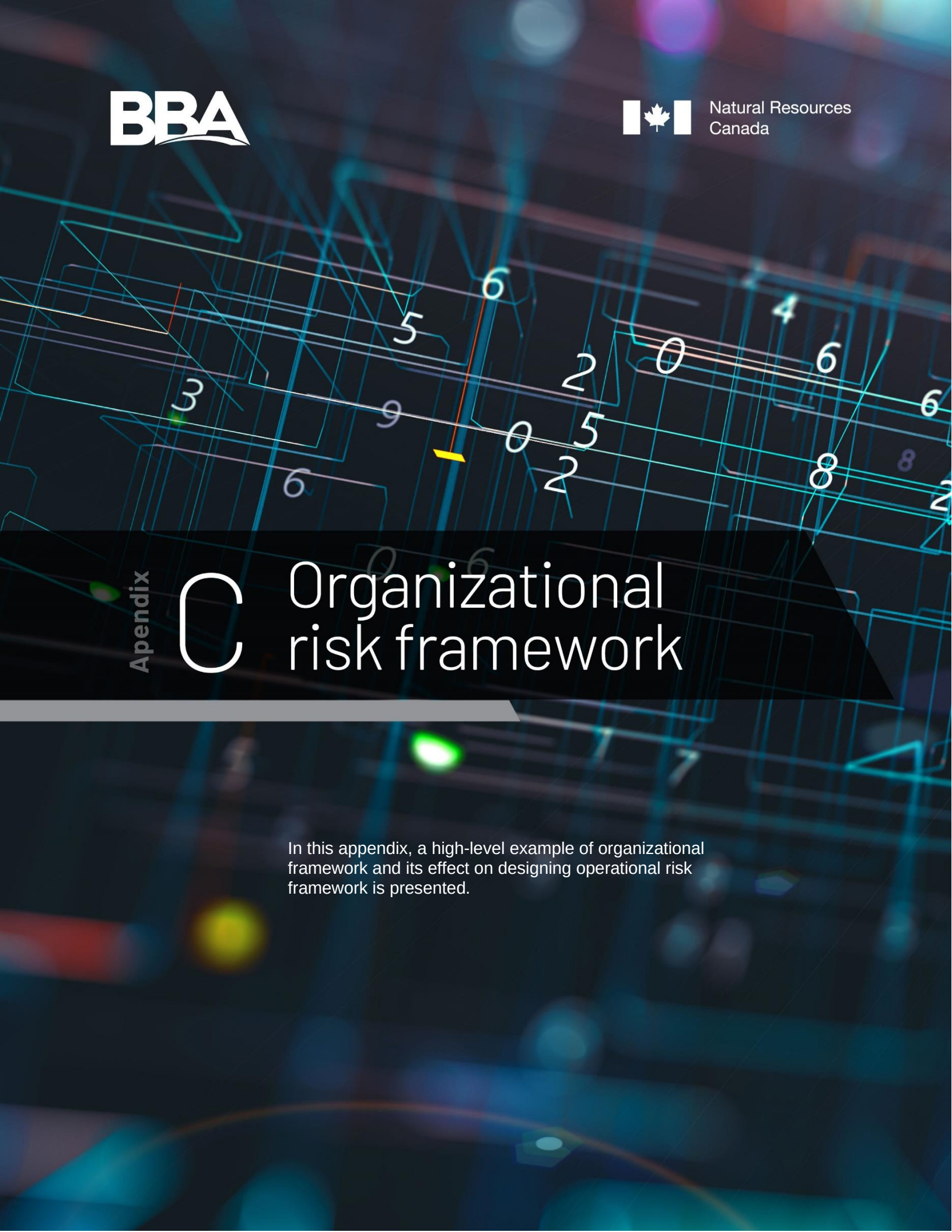
- impairment of business performance
- endangerment of personal safety
- loss of goodwill or negative effect on reputation
- breach associated with personal information
- adverse effects on law enforcement
- disruption of a third party's operation
- financial loss
- environmental damage

The final output of an asset profile is a list of assets and their values relative to disclosure (preservation of confidentiality), modification (preservation of integrity, authenticity, non-repudiation and accountability), non-availability and destruction (preservation of availability and reliability), unsafety and replacement cost.

A simple example of reducing the asset values into a common baseline is presented in Table 2 by accumulating the values of different criteria.

Table 2: Example of asset values

Asset	Safety Value	Integrity Value	Availability Value	Reliability Value	Environmental Value	Total Value
Actuator 002	3	1	2	2	1	Medium 9
Controller 001	2	2	2	3	2	High 11
Sensor 003	1	2	1	2	1	Low 7



Natural Resources Canada

Apendix C

Organizational risk framework

In this appendix, a high-level example of organizational framework and its effect on designing operational risk framework is presented.

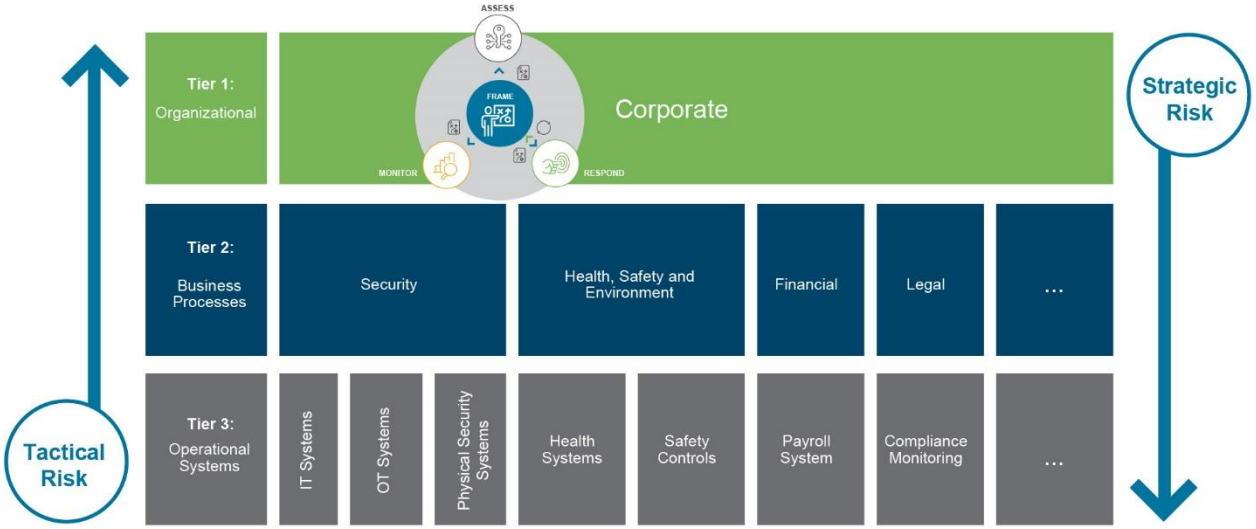


Figure 12: Organizational risk management position

Figure 12 shows the position of high-level organizational risk management, which contains the similar four components that were stated earlier, i.e., frame, assess, respond and monitor. ISO 31000 [6] suggests considering the items that are illustrated in Figure 13 as the components of the organizational risk framework.

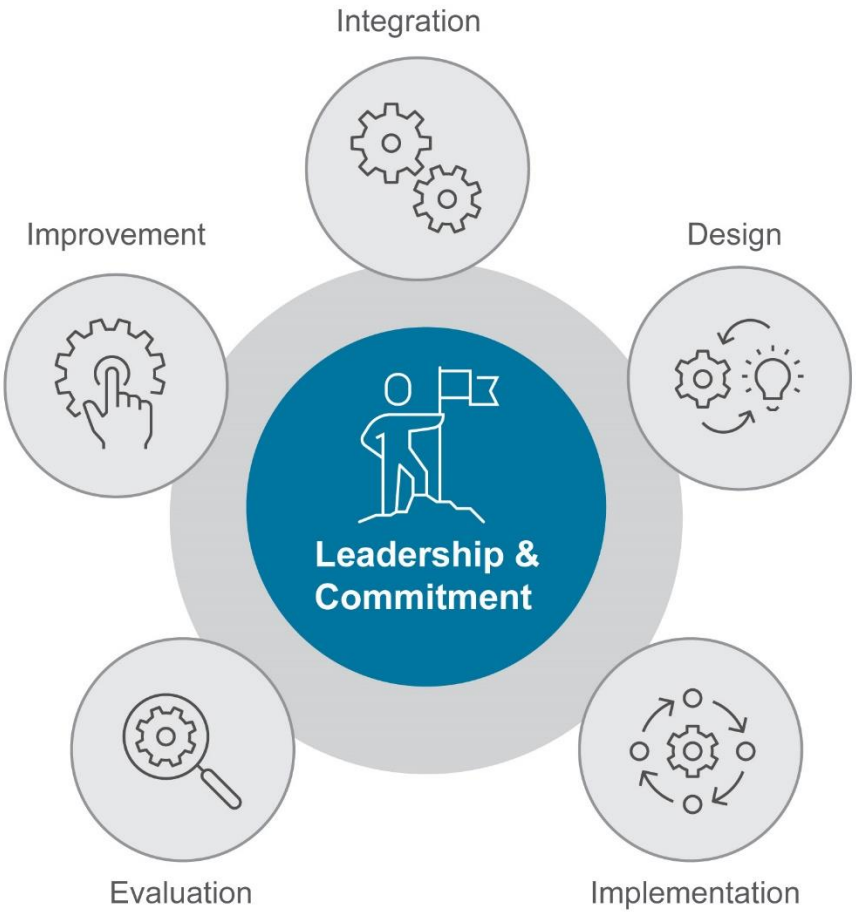


Figure 13: Organizational risk framework ISO 31000 [6]

Describing the components of organizational risk framework is not in the scope of this document. However, in the design process of the cybersecurity risk framework, the guidelines and policies that are developed in the organizational risk framework should be considered.

For example, during the development of the “Review and Improvement” criteria in the cybersecurity risk framework, the policies and principles of “Improvement” and “Evaluation” in Figure 13 should be followed.

Natural Resources Canada

Apendix D

Threat sources and events

In this appendix, some examples of threat source and threat event identification, classification and taxonomy are presented based on NIST SP 800-30 [2] and NIST SP 800-82 [7].

D.1 Threat source

Table 3: Taxonomy of threat sources

Type of threat source	Description	Characteristics
ADVERSARIAL ❖ Individual ■ Outsider ■ Trusted outsider ■ Insider ■ Privileged insider ❖ Group ■ Ad hoc ■ Established ❖ Organization ■ Competitor ■ Supplier ■ Partner ■ Customer ❖ Nation-State	Individuals, groups, organizations, or states that seek to exploit the cyber resources of the organization that are related to the operational environment.	Capability, Intent
UNINTENTIONAL/BEHAVIOURAL ❖ User ❖ Privileged user	Erroneous individual behaviours in execution of their everyday responsibilities.	Range of effects
SYSTEMS ❖ Cyber equipment ■ Storage ■ Processing ■ Communications ■ Display ❖ Utilities ■ Power supply ■ Water supply ❖ Control systems ■ Sensor ■ Controller ■ Temperature/Humidity controls ❖ Software ■ Operating system ■ Networking ■ Backup application ■ General-purpose application ■ Mission-specific application ■ Cybersecurity application	Failures of equipment, control systems, or software under different circumstances which leads to failure.	Effects on the operation

Type of threat source	Description	Characteristics
ENVIRONMENTAL ❖ Natural or man-made disaster ■ Fire ■ Flood ■ Storm ■ Earthquake ■ Bombing ■ Overrun ■ Disease ❖ Infrastructure failure/outage ■ Telecommunications ■ Electrical power	Disasters and failures of critical infrastructures outside control of the organization with operational effects.	Range of operational effects

The adversarial capabilities of an attack source can be assessed with quantitative, semi-quantitative or qualitative approaches. A quantitative approach is rather unusual, since it is hard to accurately identify and estimate the capabilities of attack sources. Table 4: Adversarial capabilities presents an example of qualitative and semi-quantitative approach for classifying the capabilities of adversaries.

Table 4: Adversarial capabilities

Qualitative	Semi-Quantitative		Description
Very High	96-100	10	Very sophisticated level of expertise, unlimited possible resources that can generate opportunities to support multiple/continuous successful coordinated attacks.
High	76-95	8	Sophisticated capabilities, significant network of resources and opportunities to support multiple successful coordinated attacks.
Moderate	21-75	5	Average resources expertise and opportunities to conduct one or multiple successful attacks.
Low	6-20	2	Limited resources expertise and opportunities to conduct a successful attack.
Very Low	0-5	0	Very little resources expertise and opportunities to conduct a successful attack.

The adversarial intent from performing an attack can be assessed with semi-quantitative or qualitative approaches. Table 5: Adversarial Intent capabilities presents an example of qualitative and semi-quantitative approaches for classifying the intents of adversaries.

Table 5: Adversarial Intent

Qualitative	Semi-Quantitative		Description
Very High	96-100	10	The adversary analyzes information obtained via reconnaissance and attacks to target a specific organization, program or business function, focusing on specific high-value or mission-critical information, operation, resources, supply flows, functions, supporting infrastructure providers or partnering organizations.
High	76-95	8	The adversary analyzes information obtained via reconnaissance to target a specific organization, program or business function, focusing on specific high-value or mission-critical information, operation, resources, supply flows, functions, supporting infrastructure providers or partnering organizations.
Moderate	21-75	5	The adversary analyzes publicly available information to target specific high-value organizations, programs, operations or information.
Low	6-20	2	The adversary uses publicly available information to target a class of high-value organizations, operation or information, in order to seek targets of opportunity within that class.
Very Low	0-5	0	The adversary may or may not target any specific organization or class of organizations.

The range of operational effects from non-adversarial threats can be assessed with semi-quantitative or qualitative approaches. Table 6: Non-adversarial capabilities presents an example of qualitative and semi-quantitative approaches for classifying the effects of those threats on organizational assets.

Table 6: Non-adversarial threat effects

Qualitative	Semi-Quantitative		Description
Very High	96-100	10	Error, failure, accident or act of nature sweeps almost all cyber assets of the operation and information systems.
High	76-95	8	Error, failure, accident or act of nature extensively affects most of the cyber resources of the operation and information systems, including many critical assets.
Moderate	21-75	5	Error, failure, accident or act of nature affects a significant portion of the cyber resources of the operation and information systems, including some critical assets.
Low	6-20	2	Error, failure, accident or act of nature affects limited non-critical cyber resources of the operation and information systems. Critical assets are not affected.
Very Low	0-5	0	Error, failure, accident or act of nature minimally affects a few or no cyber resources of operation or information systems. Critical assets are not affected.

D.2 Threat event

Table 7: Adversarial threat events presents examples of adversarial threat events on organizational and operational assets.

Table 7: Adversarial threat events

Threat event	Description
CRAFT ATTACK TOOLS	
Phishing attacks	Adversary counterfeits communications from a legitimate source to acquire sensitive information such as usernames and passwords. Typical attacks occur via email by directing users to websites that appear to be legitimate sites, while stealing the entered information.
Spoof certificates	Adversary counterfeits or compromises a certificate authority so that malware or redirected connections will appear legitimate.
False front supplier	Adversary creates false front suppliers with legitimate appearance in the critical life-cycle path that leads to inject corrupted/malicious cyber system components into the organizational supply chain.
INSERT MALICIOUS CAPABILITIES	
Known malware infection	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware into organizational information systems or possibly operational systems.
Modified malware infection	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP, removable media) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems or possibly operational systems.
Malware on control systems	Adversary installs malware (e.g., virus, worm, Trojan horse) that is specifically designed to take control of information/operational/control systems and/or exfiltrate sensitive information.
Insert counterfeit or tampered hardware into the supply chain	Adversary intercepts hardware from legitimate suppliers, modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organizational systems	Adversary replaces, through supply chain, subverted insider, or some combination thereof, critical information/operational system components with modified or corrupted components.
Install sniffers on organization-controlled networks	Adversary installs sniffing software onto organizational or operational networks.
Insert malicious scanning devices	Adversary uses commercial delivery services to place a device in the mailroom that can scan wireless communications accessible from within the mailroom in order to jam the wireless network and/or transmit information back to the adversary.
Insert subverted individuals into privileged positions	Adversary places individuals in privileged positions who are willing and able to carry out actions to cause harm to missions/business functions. Adversary may target privileged functions to gain access to sensitive information and/or control of systems.
EXPLOIT and COMPROMISE	
Exploit physical access of authorized staff	Adversary follows (“tailgates”) authorized individuals into secure/controlled locations with the goal of gaining access to facilities bypassing physical security checks.
Exploit poorly configured systems exposed to the Internet	Adversary gains access through the Internet to information systems that do not meet configuration requirements.

Threat event	Description
Control devices reprogrammed	Adversary makes unauthorized changes to programmed instructions in PLCs, RTUs, DCS, SCADA controllers, or alarm thresholds. Adversary may issue unauthorized commands to control equipment that can result in damage to equipment, premature shutdown of processes, causing environmental incident or even disabling control equipment.
Exploit recently discovered vulnerabilities	Adversary exploits recently discovered vulnerabilities in information/operational systems in order to compromise the system, before the organization has identified the vulnerability or before mitigation measures are in place.
Exploit vulnerabilities timed with operations tempo	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.
Compromise critical systems via physical access	Adversary obtains physical access to organizational information/operational systems and makes modifications.
Compromise devices used externally and reintroduced into internal environment	Adversary installs malware on devices while the systems/devices are external to organizations for purposes of infecting systems when reconnected.
Compromise design, manufacture, and/or distribution components	Adversary compromises the design, manufacture, or distribution of critical information/operational system components at selected suppliers.
Control logic manipulation	Adversary compromises and modifies control system software or configuration settings in order to produce unpredictable results.
Safety systems modified	Adversary manipulates safety systems operation to prevent them from operating when needed, or to damage the ICS by making them perform incorrect control actions.
ACTIVE ATTACKS	
Communications interception	Adversary takes advantage of communications with weak encryption to gains access to transmitted information.
Wireless jamming	Adversary interfere with wireless communications to impede or block communications.
Using unauthorized ports, protocols and services	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use, but still available.
Distributed denial of service (DDoS)	Adversary uses multiple compromised information systems external or internal to the organization for attacking a single target, thereby causing denial of service for system operators.
Targeted denial of service (DoS)	Adversary targets DoS attacks to critical information/operational systems, components, or supporting infrastructures, based on adversary knowledge of dependencies in between organizational assets.
Denial of control action	Adversary disrupts control systems operation by delaying or blocking the flow of information. This attack affects availability of the networks to control system operators, makes information transfer bottlenecks or denial of service by IT-resident services (such as DNS).
Physical attacks to facilities	Adversary conducts a physical attack to organizational facilities (e.g., set fire).
Physical attacks to supporting infrastructures	Adversary conducts a physical attack to the supporting infrastructures (e.g., break water pipe, cut power line).
Cyber-physical attacks to facilities	Adversary conducts a cyber-physical attack to organizational facilities (e.g., remotely change HVAC settings).
External network traffic modification	Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then sits between them and potentially changes traffic without notice. Such attacks are of concern for organizational use of community, hybrid and supplier. This attack is known as man-in-the-middle attack.

Threat event	Description
Internal network traffic modification	Adversary operating within the organizational infrastructure intercepts and corrupts data and control sessions. This attack is known as man-in-the-middle attack.
Spoofed system status Information	Adversary creates false information to send to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators. This can be done either by internal man-in-the-middle attack, infection of monitoring systems, etc.
Supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary compromises the operation of software, firmware and hardware that performs critical functions for organizations. This attack happened before deployment of the solution in production.

Natural Resources Canada

Apendix

E Vulnerabilities

In this appendix, some examples of vulnerability classification and constraints are presented based on [7] and [3].

Table 8: ICS vulnerabilities presents some examples of vulnerabilities in operational environment.

Table 8: ICS vulnerabilities

Vulnerability	Description
POLICY and PROCEDURES	
Inadequate security policy for the ICS	Lack or inadequacy of policies for control system security. Every control should be traceable to a policy for uniformity and accountability. The policies should cover all related and connected devices to ICS, including portable devices.
No formal ICS security training and awareness program	Without formal cybersecurity training and awareness policy, program, procedures and documentation, staff cannot be expected to maintain a cyber secure ICS environment. The cybersecurity awareness program keeps staff up to date on organizational cybersecurity policies and procedures, and operational threats, vulnerabilities, industry standards and recommended practices.
Absent or deficient ICS equipment implementation guidelines	Lack of proper implementation guidelines is the recipe for new vulnerabilities and disability to respond to events. Equipment implementation guidelines should be accessible, up-to-date, and integrated with cybersecurity incident response procedures.
Inadequate review of the ICS security controls	Lack of policies, procedures and schedules to review and determine the extent to which the security program and its constituent controls may cause lack of visibility about incorrect implementation, misalignment from operational goals and producing undesired outcome with respect to meeting ICS cybersecurity requirements. The control review policy should address the stages of review lifecycle, purpose, technical expertise, methodology and level of independence.
Lack of ICS contingency plan	The lack of a specific ICS contingency plan could lead to additional downtimes and production loss. A contingency plan should be prepared, approved, tested and available in the event of a major hardware or software failure and destruction of facilities or critical supplies.
Lack of configuration management policy	Lack of policy and procedures for ICS configuration change management can lead to unmanageable and inconsistent inventory of hardware, firmware and software. Moreover, it may create invisible consistent vulnerabilities.
Lack of adequate access control policy	Consistent access control enforcement across operational environment depends on a policy that includes roles, responsibilities and authorizations. Following organizational access control policy allows to have organizational wide consistent access control.
Lack of adequate authentication policy	Lack of authentication policy may result in unauthorized access from insufficient/incorrect authentication controls. Authentication policies for operational environment should define the time to use, location of use, strength and procedure to maintain the authentication mechanisms (e.g., passwords, smart cards). Authentication policies should be developed as part of an overall ICS security program, in line with organizational authentication policies, considering the capabilities of the ICS and its personnel to handle more complex passwords and other mechanisms.
Inadequate incident detection and response plan and procedures	Lack of proper policies, planning and procedures for incident detection and response can potentially cause production loss and down time. Incident detection and response plans and procedures are necessary for rapidly detecting incidents, minimizing loss and destruction, preserving evidence, mitigating weaknesses and restoring ICS services. Incident detection includes continuous monitoring of ICS environment for anomalies and automatic containment of detected incidents. Incident response plan includes prioritizing the handling of incidents, implementing effective methods of data collection, analysis, decision-making and reporting.
Non-redundancy of critical components	Lack of redundancy for critical components can increase down time caused by single point of failure.
IT/OT misalignment	Miscommunications, wrong expectations and misaligned approaches of IT and OT personnel in securing ICS can create a usable gap for adversaries to compromise the system. For example, having the wrong expectation of the backup process from each side may lead to have improper backup process.
ARCHITECTURE and DESIGN	

Vulnerability	Description
No security perimeter defined	Lack of clear definition of ICS security perimeter makes it impossible to ensure proper deployment of necessary security controls. This can lead to numerous security problems, including unauthorized access.
Control networks used for non-control traffic	Having no segregation between control and non-control traffic makes it more difficult to configure the network so that it meets control traffic requirements, as those requirements are different from non-control traffic, such as reliability. For example, non-control traffic could inadvertently consume resources that control traffic needs, causing disruptions in ICS functions.
Control network services not within the control network	Using IT services, such DNS and DHCP, by control networks may cause the ICS network to become dependent on the IT network, that may not have the reliability and availability requirements needed by the ICS.
Inadequate collection of event data history	Without proper and accurate data collection, it might be impossible to determine the cause of a security incident. As a result, incidents might keep happening unnoticeably and lead to additional damage or disruption.
CONFIGURATION and MAINTENANCE	
Hardware, firmware, and software not under configuration management	Lack of configuration change management procedures can lead to inconsistent and ineffective cybersecurity defense posture. A process for controlling modifications to hardware, firmware, software and documentation should be implemented to ensure the ICS environment is protected against improper modifications in the whole lifecycle of system implementation.
Legacy software	Having OT systems run on legacy software that lack strong security features, such as sufficient authentication and data authenticity/integrity verification, can allow attackers to gain access to systems.
Poor remote access controls	SCADA systems connected to unaudited dial-up lines or remote-access servers with poor remote access controls can cause unauthorized access to adversaries. Remote access capabilities must be adequately controlled to prevent unauthorized individuals from gaining access to the ICS.
Critical configurations are not stored or backed up	Poor backup and restoration process of critical configurations can cause long down times. Procedures should be available for backup and restoring ICS configuration settings in the event of accidental or adversary-initiated configuration changes to maintain system availability and prevent loss of data.
Lack of up-to-date Malware protection	Outdated malware protection software leaves the system open to new malware threats. Malware protection controls, such as antivirus software, must be kept current.
Denial of service (DoS)	ICS software could be vulnerable to DoS attacks, resulting in inaccessibility of system resources for authorized access. Certain controls need to be considered to prevent this attack, such as network isolation or DoS prevention services.
Inadequate authentication, privileges, and access control in software	Unauthorized access to configuration and programming software could cause security breach or provide the ability to corrupt a device.
PHYSICAL	
Unauthorized personnel have physical access to equipment	Improper physical access to ICS equipment can cause any of the following: ■ Physical theft of data and hardware ■ Physical damage or destruction of data and hardware ■ Unauthorized changes to the functional environment (e.g., unauthorized use of removable media, adding/removing equipment or devices) ■ Disconnection of physical data links ■ Undetectable interception of data (keystroke and other input logging) Physical access to ICS equipment should be restricted to only the necessary personnel and access rights need to be reviewed regularly, considering safety requirements, such as emergency shutdown.
Default configuration	Using out-of-box default or simple passwords and baseline configurations for devices and systems make it easy for attackers to compromise OT systems.
Lack of backup power	Without backup power to critical assets, a general loss of power will shut down the ICS and could lead to insecure default settings.

Vulnerability	Description
Loss of environmental control	Loss of environmental control (e.g., temperatures, humidity) could lead to equipment damage, capacity reduction, intermittent errors, constant reboot or permanent incapacity.
Unsecured physical ports	USB and PS/2 ports could allow unauthorized connection of thumb drives or key loggers, if those ports are active.
Insecure default settings	Security capabilities that were installed with products are useless if they are not enabled or at least identified as being disabled in a wholesome security perspective.
COMMUNICATION and NETWORK CONFIGURATION	
Data flow controls not employed	Invalidated data flow can cause exfiltration of information, command injection, parameters manipulation, etc. The types of data, systems and network connections need to be defined. Data flow controls, based on data characteristics, need to be restricted based on type of data, systems and connection.
Firewalls nonexistent or improperly configured	Improper configured firewalls could allow unnecessary data to pass between networks, such as control and corporate networks, allowing attacks and malware to spread between networks, making sensitive data susceptible to eavesdropping. This can provide individuals and adversaries with unauthorized access and control to critical systems.
Insecure industry-wide ICS protocols	Legacy SCADA controllers and ICS protocols often have few or no security capabilities, such as authentication and encryption, that can cause considerable vulnerabilities, such as sniffing to discover username and passwords. It is recommended to use the latest protocol versions with security features enabled.
Authentication of users, data or devices is substandard or nonexistent	Many ICS protocols have been designed without security considerations. Lack of authentication/isolation of the network where those protocols are used can potentially allow an adversary to replay, modify or spoof data or spoof devices such as sensors and user identities.
Lack of integrity checking for communications	There are no integrity checks built into most industrial control protocols, which can allow manipulation of communications undetected. Lower-layer protocols with integrity check (e.g., IPSec) can be used in ICS communications.
Inadequate authentication between wireless clients and access points	Weak authentication between wireless users and access points can lead to having users connected to adversary controlled rogue access points or have the adversary connected to ICS wireless networks. It is recommended to use strong mutual authentication between wireless clients and access points.
Inadequate data protection between wireless clients and access points	Lack of encryption or use of weak algorithms in data transmission protocols can allow the adversary to extract the communicated data. Using strong encryption in communications is recommended.
Web exposure	Traditional OT systems, such as HMIs and PLCs are increasingly being connected to the Internet. Those systems are highly vulnerable to attacks, such as cross-site scripting and SQL injection attacks.

Table 9: presents some examples of constraints in the organization and operational environment.

Table 9: Constraints

Constraint	Description
Time	■ A control should be implemented within a certain time. ■ Life span of a control can be during operation of a system, or not. ■ Acceptable period of time to be exposed to a particular risk.
Financial	■ Controls to protect a system should not be more expensive that the value of that system. ■ Budget for each task. ■ Executive decisions for the tasks that exceed acceptable budget constraints. ■ Priorities for operation of controls in the case of budget reduction.
Technical	■ Compatibility of software and hardware during the selection of controls. ■ Backward compatibility in implementation of controls to an existing process or system without effecting their productivity.
Operational	■ 24/7 operation with continuous backups.
Cultural	■ Staff should understand the need for the controls, otherwise the control may become ineffective over time. For example, bag search may be acceptable in some regions and inacceptable in some other regions.
Ethical	■ Ethical constraints can be different in various regions. For example, email scanning may be acceptable in some regions and unacceptable in others.
Environmental	■ Environmental factors can influence the selection of controls. For example, distance to a natural phenomenon such, as river, affects the selection of controls.
Safety	■ Safety regulations and culture can influence the selection of controls. For example, the culture or requirements of wearing safety gear can affect the consequence of a threat.
Communication	■ The level of communications between staff and having formal communication procedures can influence the selection and effectiveness of controls. For example, in a poorly communicated environment, incident response process would be challenging in the case of unavailability of some staff.

Natural Resources Canada

Apendix

F Impact

In this appendix, some examples of adverse impacts and risk scenarios for assessing the impact of incident scenarios are presented based on NIST SP 800-30 [2]. classification and constraints are presented based on [7] and [3].

Table 10 presents some examples of adverse impacts of incidents to organizations, operations, assets, individuals, other organizations, the community and the environment.

Table 10: Example of adverse impacts

Type	Impact
HARM TO ORGANIZATION	
Financial	Financial costs of the business or mission
Reputation	Damaging the trusted relationships with clients, service providers, public, etc.
Reputation	Damaging the image and potentially affecting future trusted relationships
Legal and regulatory	Regulatory penalties due to noncompliance with regulations or contractually binding agreements, e.g., sanctions or licence suspension
Financial	Financial costs due to noncompliance with regulations or contractually binding agreements
Legal and regulatory	Regulatory penalties due to noncompliance with related information privacy acts
Opportunity	Reduction in operation capacity that prevents performing future services
HARM TO OPERATIONS	
Service interruption	Interruption of performing current functions in sufficient time
Service interruption	Interruption of performing future functions in sufficient time
Service interruption	Affecting the ability to restore functions in future
Plant disruption	Affecting the confidence or correctness of current services
Plant disruption	Affecting the confidence or correctness of future services
Plant disruption	Affecting the ability to follow planned resource constraints during the operation of current functions
Plant disruption	Affecting the ability to follow planned resource constraints during the operation of future functions
Financial	Cost of repair or recovery
HARM TO ASSETS	
Service interruption/financial	Damage to or loss of physical facilities
Service interruption/financial	Damage to or loss of systems or networks
Service interruption/financial	Damage to or loss of equipment, parts or supplies
Service interruption/financial	Damage to or of loss of information assets
Financial	Loss of intellectual property
HARM TO INDIVIDUALS	
Health and safety	Injury, disease or loss of life
Health and safety	Physical or psychological mistreatment

Type	Impact
Financial/Reputation	Identity theft and disclosure of confidential information
Legal and regulatory/financial	Loss of personally identifiable information
Skill Loss	Loss or unavailability of special skills provided by employees or external resources
HARM TO OTHER ORGANIZATIONS	
Financial	Financial costs due to causing harm to another organization because of noncompliance with regulations or contractually binding agreements
Legal and regulatory	Regulatory penalties due to causing harm to another organization because of noncompliance with regulations or contractually binding agreements
Reputation/Legal	Damaging the trusted relationships with clients, service providers and public because affecting the operation of other organizations, e.g., by being part of a DDoS attack against an organization
Reputation	Damaging the image and potentially affecting future trusted relationships by affecting the operation of other organizations.
HARM TO THE COMMUNITY AND ENVIRONMENT	
Environmental	Damaging the environment or creating hazard by malfunction or human error
Financial/Legal/ Environmental/ Service interruption	Damage to or incapacitation of a critical infrastructure sector
Legal/Service interruption	Loss of government continuity of operations
Financial/Reputation	Damaging national reputation and potentially affecting future trusted relationships
Legal/Reputation	Regulatory penalties due to causing harm to trusted relationships with other governments or with nongovernmental entities
Opportunity/Service interruption	Damage to current or future ability to achieve national objectives by causing harm to national security

Some of the identified impacts can be grouped together based on organizational preferences. Typically, different impacts will be scaled and normalized into one table. Table 11 illustrates an example of a normalized impact table.

Table 11: Normalized impact table

Impact Type	Very Low	Low	Medium	High	Severe
Financial	<$10,000 cost	<$100,000 and >$10,000 cost	<$1,000,000 and >$100,000 cost	<$10,000,000 and >$100,000 cost	>$10,000,000 cost
Reputation	1-5 clients would have minor complaints	Local news being remembered for less than a year	Being in local news and communities from 1 to 5 years	Being in national or international headlines	Internationally recognized as the main cause of a disaster
Legal and regulatory	Getting regulatory warning	Minor fine or mandated to do further audit	Temporary suspension of a licence	Losing some licences	Permanent voiding of practice licence
Environmental	Controlled and contained hazard	Contained hazard that can be fixed in a few days	Local hazard that will last for a few months	Wide environmental damage that will last for years	Permanent environmental damage
Opportunity	Delaying new contracts	Dissatisfaction of some existing clients	Losing some contracts with value under $100,000.	Losing contracts with value between $100,000 and $1,000,000.	Losing all business line opportunities
Health and safety	Temporary and minor injuries	Repeated injuries	Numerous injuries or loss of organ	Casualties	Numerous casualties

For the risk management process, and more specifically risk assessment, there are many tools and methodologies available that can be used for certain parts of the process or the overall process. One of the famous methods to assess the impact of a specific threat event is demonstrated in the Bow Tie diagram. Figure 14 shows a risk scenario example in a Bow Tie diagram.

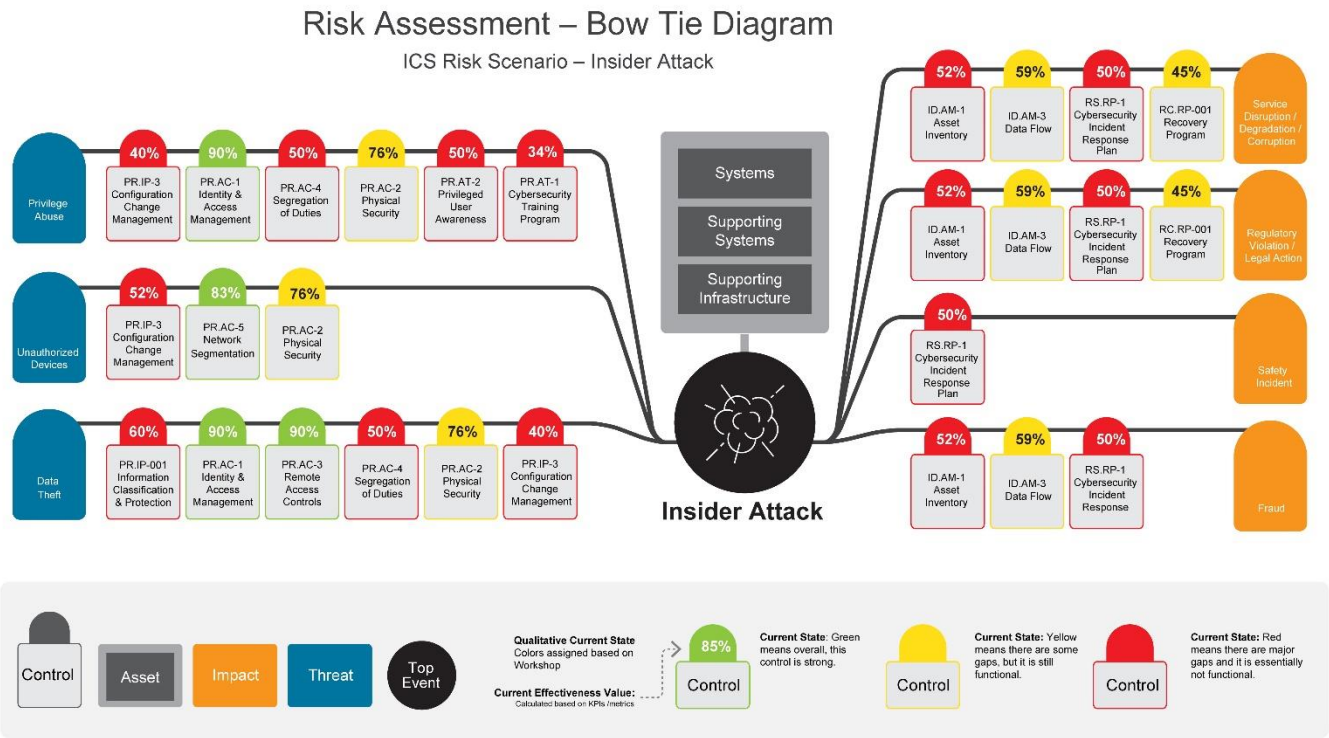


Figure 14: Risk scenario in Bow Tie diagram

In this example, three threats are considered on the left side in blue boxes. These threats can be avoided by the preventive controls in front of them. The effectiveness of those controls is calculated and marked, in percentage.

In the middle of the diagram, a cybersecurity event is identified that can happen if the preventive controls are not effective. The systems and supporting infrastructure that can be affected by this event is identified.

On the right side, four impacts are identified if the cybersecurity event happens. These impacts can be limited by containment controls before them. The effectiveness of those controls is calculated and marked.

Natural Resources Canada

Apendix G

Likelihood of occurrence

In this appendix, some examples of the likelihood of different events in the risk process based on NIST SP 800-30 [2].

Table 12: Likelihood of threat initiations by adversary

Qualitative	Semi-quantitative		Description
Very High	96-100	10	Adversary is **almost certainly** to initiate the attack
High	81-95	8	Adversary will **most likely** initiate the attack
Moderate	21-80	5	Adversary is **somewhat likely** to initiate the attack
Low	5-20	2	Adversary will **unlikely** initiate the attack
Very Low	0-4	0	Adversary is **almost certainly not** to initiate the attack

Table 13: Likelihood of non-adversarial threat occurrence

Qualitative	Semi-quantitative		Description
Very High	96-100	10	Unintentional threats occur **almost certainly**, or occur more than 100 times a year
High	81-95	8	Unintentional threats occur **most likely**, or occur between 10-100 times a year
Moderate	21-80	5	Unintentional threats occur **somewhat likely**, or occur between 1-10 times a year
Low	5-20	2	Unintentional threats occur **unlikely**, or occur fewer than once a year, but more than once every 10 years
Very Low	0-4	0	Unintentional threats **almost certainly not** to occur, or occur fewer than once every 10 years

Based on the posture of the implemented cybersecurity controls and existing vulnerabilities, the chance of success for specific adversarial attacks can be calculated in a success scale, such as Table 14.

Table 14: Likelihood of adversarial success

Qualitative	Semi-quantitative		Description
Very High	96-100	10	Adversary **almost certainly** succeeds in the attack.
High	81-95	8	Adversary **most likely** succeeds in the attack
Moderate	21-80	5	Adversary **somewhat likely** succeeds in the attack
Low	5-20	2	Adversary **unlikely** succeeds in the attack
Very Low	0-4	0	Adversary **almost certainly** fails in the attack.

Finally, the total likelihood of each threat event can be calculated. See Table 15 for an example.

Table 15: Total likelihood of threats

Threat event	Likelihood
ACTIVE ATTACKS	
Adversary takes advantage of communications with weak encryption to gain access to transmitted information.	8
Adversary interferes with wireless communications to impede or block communications.	9
Adversary conducts attacks using ports, protocols and services for ingress and egress that are not authorized for use, but still available.	7
Adversary uses multiple compromised information systems external or internal to the organization to attack a single target, thereby causing denial of service for system operators.	4
Adversary targets DoS attacks to critical information/operational systems, components or supporting infrastructures, based on adversary knowledge of dependencies in between organizational assets.	4
Adversary disrupts control systems operation by delaying or blocking the flow of information. This attack affects network availability to control system operators, creates information transfer bottlenecks or denial of service by IT-resident services (such as DNS).	5
Adversary conducts a physical attack to organizational facilities (e.g., sets fire).	6
Adversary conducts a physical attack to the supporting infrastructures (e.g., break water pipe, cut power line).	8
Adversary conducts a cyber-physical attack to organizational facilities (e.g., remotely change HVAC settings).	9
Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then sits in between them and potentially changes traffic without their notice. Such attacks are of concern for organizational use of community, hybrid and supplier. This attack is known as man-in-the-middle attack.	2
Adversary operating within the organizational infrastructure intercepts and corrupts data and control sessions. This attack is known as man-in-the-middle attack.	3
Adversary makes the false information to send to control system operators either to disguise unauthorized changes or to initiate inappropriate actions by system operators. This can be done either by internal man-in-the-middle attack, infection of monitoring systems, etc.	6
Adversary compromises the operation of software, firmware and hardware that performs critical functions for organizations. This attack happened before deployment of the solution in production.	5

Natural Resources Canada

Apendix H Risk

In this appendix, we provide description of a potential way to determine risk as combination of likelihood and impact based on NIST SP 800-30 [2].

In the first step, risk levels need to be defined. Table 16 provides an example of defining risk levels.

Table 16: Levels of risk

Qualitative	Semi-quantitative		Description
Very High	96-100	10	Threats event is expected to have **multiple severe** adverse effects
High	81-95	8	Threats event is expected to have **a severe** adverse effect
Moderate	21-80	5	Threats event is expected to have **a serious** adverse effect
Low	5-20	2	Threats event is expected to have **a limited** adverse effect
Very Low	0-4	0	Threats event is expected to have **negligible** adverse effect

In the next step, the combination of likelihood and impact is defined. Table 17 provides an example of a risk matrix.

Table 17: Risk matrix

	Impact				
Likelihood	**Very Low**	**Low**	**Medium**	**High**	**Severe**
Very High	5	7	8	9	10
High	4	6	7	8	9
Moderate	3	5	7	7	8
Low	2	4	5	6	7
Very Low	1	2	3	4	6

Finally, the details of each risk are assessed and listed. Table 18 provides a template example of the list of cybersecurity risks.

Table 18: Risk list template

1	2	3	4	5	6	7	8	9	10	11	12	13	14
Adversarial / non-Adversarial	**Threat**						**Likelihood**			**Vulnerabilities**		**Impact**	**Risk**
	Threat Event		Threat Source				Initiation Likelihood	Success Likelihood	Overall Likelihood	Vulnerability and conditions	Severity		
Yes / No	ID, Description	Relevance to scope	ID, Description	Capability	Intent	Target	Level, Number	Level, Number	Level, Number	ID, Description	Level	Level, Description	Level, Description

In another example, by focusing on the change that control measures can make to the risk posture, Table 19 shows the reduction either in the likelihood or impact of the cyber threat.

Table 19: Semi-quantitative risk assessment template

1	2	3	4	5	6	7	8	9	10
Activity	**Threat**	**Vulnerability**	**Likelihood**	**Impact**	**Risk**	**Control Measure**	**△ in Likelihood**	**△ in Impact**	**Residual Risk**
Operator operating within the exclusion zone	Monitoring system malfunction and cause injuries and damage	Outdated firmware with too much access exposure	M (<1x per yr)	H (disabling or fatal injury)	H (from risk matrix)	Regular firmware patch management procedure with auditory alarm trigger	L (<1x in 10 yrs)	H	M

BBA

Natural Resources Canada

Apendix

Risk assessment report template

In this appendix, the main topics that are recommended to be captured in a Cybersecurity risk assessment is presented.

1. Executive summary
    - Introduction, date and the background of the risk assessment
    - Purpose, context and scope of the risk assessment
    - Approach of conducting the risk assessment
    - High-level cyber risks to the organization and operational environment based on the perception of executives before conducting the risk assessment
    - Organizational Risk Matrix
    - Top cybersecurity risks to ICS environments in the industry
    - Identified crown jewel assets in the context of operational and organizational systems, along with examples of related cybersecurity risks, threats, consequences, related systems, and the controls to protect the crown jewel assets
    - Overall level of risk and number of risks for each level
2. Risk assessment body
    - Definition of normalized impact levels, including details of effect on the organization, business, mission, and operations
    - List of businesses, missions and major operation lines along with the number of risks for each of them in each risk category
    - Classification of risks based on severity of impact, class of impact and category of cyber risk, after input of business/mission and operation representatives
3. Appendices
    - List of References
    - List of assets associated with each risk to each operation line and mission, along with the affected OT/IT systems by the risk
    - Dependencies between assets in respect to each risk that shows the affection span of a risk if to happen
    - List of detailed assessment evidences that supports the results of assessment, such as details about risk factors, asset profile and dependencies, controls and their coverage, constraints, risk aggregations, and past cybersecurity incidents
    - List of teams, individuals and dates of interviews