Ministry of Interior

National Cybersecurity Center

National Risk Management Framework

Draft v 0.1
May 2023

Table of Contents

Introduction

The National Cyber Security Center (NCSC) of the Kingdom of Bahrain is delighted to present this Risk Management Framework document, as the authoritative reference for Risk Management concerning Information Security across the nation.

In an age where our world is more interconnected than ever, where technology fuels our daily lives and drives the engines of progress, safeguarding our organizations and Critical National Infrastructure (CNI) is paramount. This Framework breaks new ground, setting the stage for a resilient and secure future. Risk Management is crucial in that it helps organizations protect their assets, make informed decisions, safeguard their reputation, comply with regulations, capitalize on opportunities, ensure business continuity, and gain stakeholder confidence. It is a proactive and strategic approach that enables organizations to navigate uncertainties and achieve their objectives in an ever-changing environment.

This document is not purely a compilation of best practices but a testament to innovation in the field of cyber security. It brings forth a pioneering approach, leveraging the power of the Center for Internet Security (CIS) controls as part of a package of tools tailored to address the unique challenges faced by the Kingdom's CNI sectors and industry more broadly. It marks a turning point in managing cyber security risk, ensuring the protection of our nation's most vital assets. What sets this document apart is its unwavering focus on empowering industry professionals. It recognizes the indispensable role played in fortifying our infrastructure against evolving cyber threats. By harnessing this expertise, this Framework enables industry professionals to take charge of risk management, equipped with a state-of-the-art approach.

This Framework aims to unify the Nation's approach to risk management, supporting professionals as catalysts of change, equipped with tools that seamlessly integrate CIS controls into their risk management practices. The impact on these roles will be nothing short of transformative, elevating them to proactive guardians of our nation's cyber security.

This document outlines the principles, processes, and procedures for managing organizational risks. It provides a structured approach to identifying, assessing, mitigating, and monitoring risks across an organization's operations. This document serves as a guide for employees and stakeholders involved in risk management activities and ensures consistency and standardization in managing risk throughout the organization.

This Framework encourages a dynamic roadmap approach that translates principles into action, providing practical steps and tangible solutions. It equips practitioners with the tools necessary to assess risks and vulnerabilities, and best approach implementation of robust security measures, ensuring resilience in the face of an ever-evolving threat landscape.

It is through embracing innovation, in rising above the challenges that we secure the future of our nation. Together, let us embark on this transformative journey and create a cybersecurity landscape that will stand the test of time.

Purpose

This document provides a high-level reference, outlining the Risk Management Framework (RMF) that Bahrain NCSC recommends for use nationwide. This document references recognized international standards and outlines how NCSC leverages these for its Risk Management activities.

This document serves as best practice guidance to the full range of public and private entities within the Kingdom of Bahrain. By providing this guidance, NCSC aims to promote uniformity and commonality of the Information Security Mission across the Kingdom.

NCSC recognizes that information technology has become core to providing services and meeting mission goals. With this reliance on technology, organizations need to identify and manage risk with technology assets, processes, and tools. The National RMF is a systematic process that helps organizations identify, analyze, and prioritize potential risks to their assets, systems, and processes. The objective of the RMF is to ensure organizations have a clear understanding of their risk exposure, and to develop effective strategies for managing those risks. The RMF program aligns with the ISO/IEC 27005:2022 standard and provides ongoing support for organizations' risk management efforts.

This RMF is aligned with the NCSC's National Risk Assessment program, with the NCSC working in close partnership with CNI sector regulators. Through this partnership and by leveraging a toolset provided by NCSC, including this Framework document, risk assessments can be conducted in a consistent manner across the Kingdom, providing insight into the risk profile of each sector.

NCSC provides this document as a RMF to govern and organize Risk Management activities across the Kingdom of Bahrain.

Target Audience & Scope

NCSC commends the Risk Management Framework outlined in this document to each of the Sector Regulators, all government departments, public sector bodies, and private entities across the CNI space, and throughout the Kingdom, as the best practice guidelines for conducting Risk Management and Risk Assessment. This publication serves to inform and direct both public and private stakeholders across all sectors, with specific focus on those considered CNI. It is the intention that Risk Assessments from these CNI sectors contribute to analysis at the national level, from which national and sectoral maturity assessments can be made.

Introduction to Risk Management

What is Risk Management?

Risk management is the process of identifying, assessing, and prioritizing risks to minimize or mitigate their impact on an organization's objectives. It involves systematically analyzing potential risks, evaluating their likelihood and potential consequences, and implementing strategies to manage or respond to those risks effectively.

National Institute of Standards and Technology (NIST) can be considered an authoritative source and describes it as the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

The National Risk Management Framework (RMF) is based on international cyber security standards and is recommended for adoption by most organizations. Entities meeting certain criteria will be required to adopt the framework. Widespread adoption throughout CNI and beyond is highly encouraged.

Why conduct Risk Management?

The goal of Risk Management is for organizations to minimize their security risk through the planning, execution, administration and monitoring of security controls, in relation to threats. The threats are those that have been identified by an organization through assessment.

Implementing a RMF at a national level ensures uniformity of approach and a common language with which to describe, view and assess the Kingdom’s security interests. This common framework enables NCSC and sector regulators to develop focused initiatives and solutions to address gaps that may be identified.

International Risk Management Standards

International security standards are important as they; provide a framework for consistent security practices, ensure compliance with legal and regulatory requirements, enhance customer trust, promote continuous improvement, offer third-party assurance, and facilitate international collaboration and knowledge sharing. By following these standards, organizations can establish a strong security foundation and mitigate risks in an ever-changing threat landscape. The standards listed below are referenced or alluded to later in this document.

International Organization for Standardization 31000 (ISO 31000)

This standard from ISO, provides guidelines, principles, a framework and processes for managing risk. It is a high-level document dealing with Risk Management in the round, pitched for use by any organization operating in any sector. The standard seeks to provide the following benefits for organizations:

- **Return on Investment.** Ensures that security controls are deployed effectively and addresses those risks which require priority treatment due to the potential losses which could occur.
- **Budget Allocation.** Ensures that budget can be allocated effectively, according to prioritized risk calculations.
- **Appropriate Control Selection.** This includes optimization and effective resource utilization.

International Organization for Standardization 27005:2022 (ISO 27005:2022)

ISO 27005 is an information security-orientated standard closely related to ISO 31000. ISO 27005 is designed to support the implementation of information security based on a risk management approach. The contained guidelines include a subset of a broader range of security best practices laid out by ISO.

ISO 27005 is applicable to a very wide variety of organizations and sectors, including CNI. ISO 27005 proposes an iterative approach aimed at balancing time and effort with the efficiency of controls. The approach is aligned with the NCSC's RMF, focusing on the definitive phases.

The adoption of this framework throughout the Kingdom of Bahrain, underpinned by this standard, will promote the alignment of best practices and help identify, assess, evaluate, and ultimately treat information security vulnerabilities.

Related Controls Documents & Standards

The following are not Risk Management Standards; however, they are related to aspects of Risk Management and referenced or alluded to later in this document, so they are included here for completeness.

International Organization for Standardization 27002 (ISO 27002)

ISO 27002 forms a reference set of protection tools. It covers cyber security, information security and privacy protection controls and is based on generally accepted best practices. ISO 27002 provides comprehensive information security techniques and asset management controls for any organization that needs a new information security management program or wishes to improve its existing information security policies and practices.

Center for Internet Security (CIS) Controls v8

The CIS controls are a set of safeguards that provide mitigations against the most prevalent cyber threats. The intention behind them is to provide a comprehensive set of controls - a baseline against which organizations can measure where gaps appear in their own control sets. The controls set consists of 18 overarching measures and they map to the majority of the other international standards for implementing controls (for example, ISO 27002, NIST 800-53, Cyber Essentials, MITRE Attack v 8.2, PCI Payment Card Industry v4.0).

Risk Management Framework

The Risk Management Framework (RMF) consists of 3 key aspects - Governance, the Risk Management Method and the Framework Implementation. As governance concerns the overarching management of the Framework, including the creation of a strategy, the establishment of roles and responsibilities, and the defining of the organization's risk appetite. Governance is fundamental to the successful implementation of the framework.

The Risk Management Method concerns best practice for how Risk Management is carried out in an organization, compliant with local and international standards. The Method provides practical guidance for identifying, assessing, mitigating, monitoring, and communicating cyber security risk.

The Framework Implementation provides an iterative approach for implementing the Method defined in the previous step and describes how it can contribute to the National Risk Assessment initiative.

Senior Management should initiate risk management as they provide **governance** to the organization. Once governance is established, **risk management** activities should follow, the outcome of which will uncover which risks need to be treated. Finally, the overall approach should undergo refinement and enhancement as circumstances may necessitate a change in risk appetite or strategy. A high-level summary of the Framework is illustrated below:

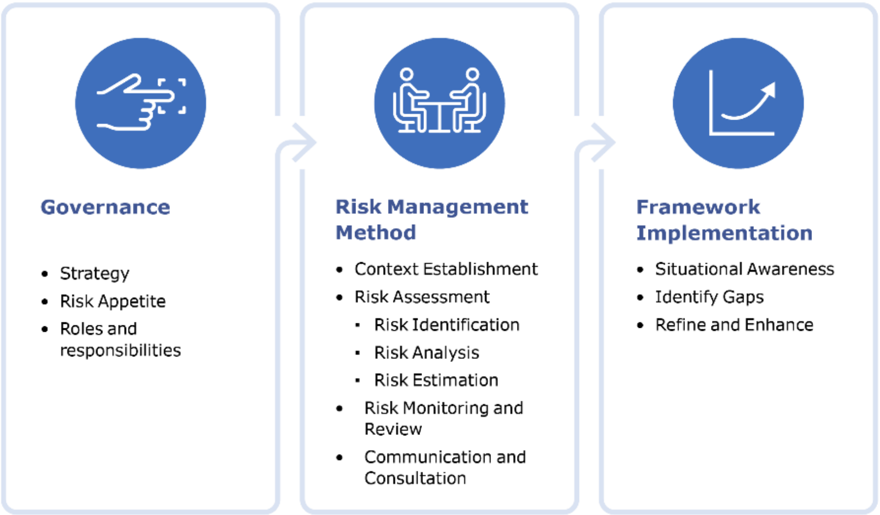


Figure 1: Risk Management Framework Overview

1. Governance

The success of individual entities owes much to their own internal organization. Governance, Risk management and Compliance (GRC) models provide an overview of how the risk management function aligns with high-level strategy makers and the internal auditors to give three symbiotic relationships, which work together to maintain effective conditions for risk management.

GRC integrates governance, risk management, and compliance functions, facilitates effective risk management and compliance with regulations, supports informed decision-making, enhances organizational efficiency, builds reputation and trust, and enables a proactive approach to change, whilst boosting stakeholder confidence. By adopting a comprehensive GRC approach, organizations can navigate complexities and mitigate risks.

Governance is provided by the Board of Directors, who create the high-level strategies and then receive visibility of the risk management function, through a steering committee, who manages the implementation of controls through operations personnel, and review existing risk management initiatives. Internal audits are supported through the provision of insight into compliance levels.

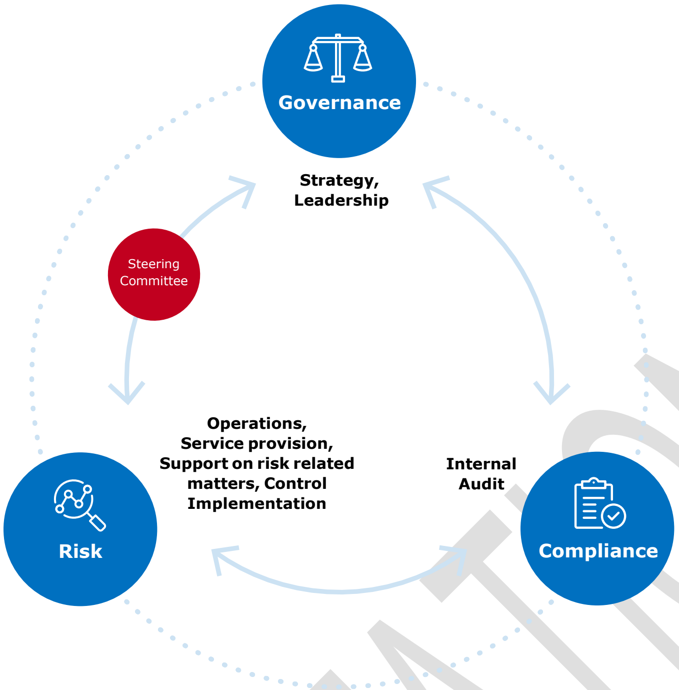

Governance
Strategy, Leadership
Steering Committee
Operations, Service provision, Support on risk related matters, Control Implementation
Internal Audit
Risk
Compliance

Figure 2: Governance, Risk and Compliance

1.1 Risk Management Strategy

Each organization should define its own Risk Management Strategy, in line with the National Cybersecurity Strategy, wherever possible. The Risk Management Strategy should support the overall strategic objectives of the organization. There are several factors which should be addressed to ensure a Risk Management Strategy is aligned to the organization’s mission and goals:

- Culture of the organization.
- Organization’s mission and long-term vision.
- Strategic goals of the organization.
- Organization’s composition (key stakeholders, workforce).
- How the organization operates (departments, key capabilities, internal procedures).

These factors are shown in Figure 3, below, with Risk Appetite discussed in the next section:

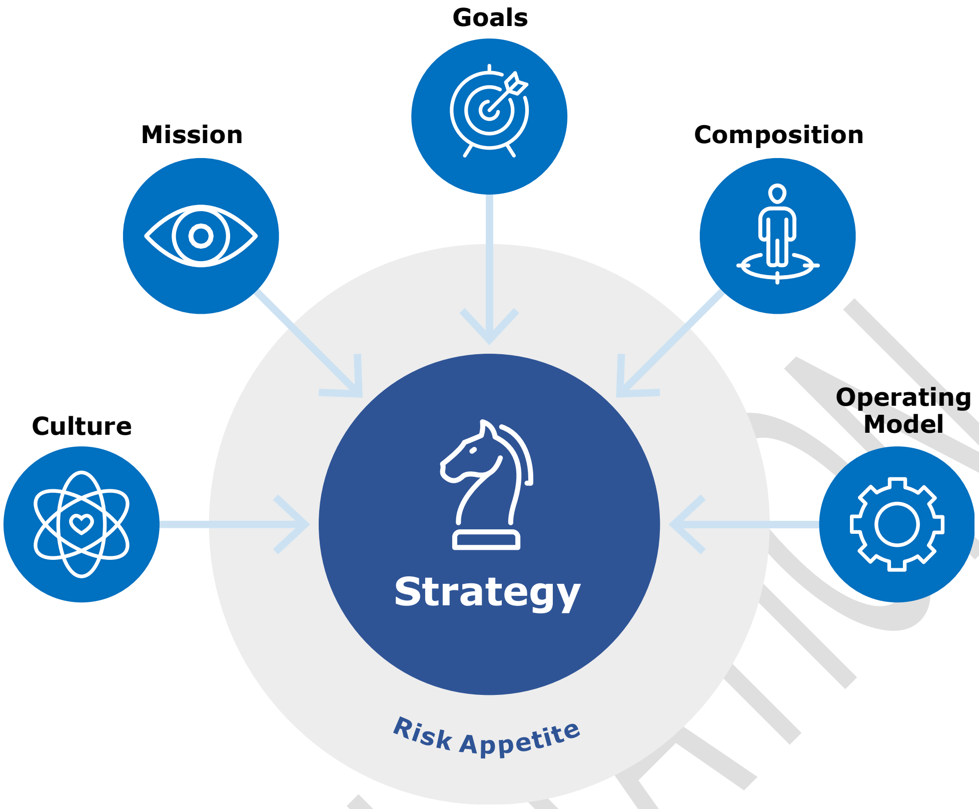


Figure 3: Factors Establishing a Risk Management Strategy

An example of such a strategy:

> *"The company will seek to identify all potential risks which could affect our software projects and services. These risks will be evaluated and assigned a risk score. High Priority risks will be analyzed in greater depth to understand their root causes and potential consequences. The company will develop a plan to minimize the impact of identified risks and may involve the use of preventative measures such as conducting additional testing or securing backup resources. Risks will be continually monitored, and mitigation strategies will be regularly assessed. When risks materialize, appropriate measures will be taken and could involve the activation of contingency plans. The company will maintain open communication channels with all stakeholders, and all risks will be documented together with their assessment and mitigation strategies."*

1.2 Risk Appetite

These factors above help provide an underlying context for the organization, and together help to formulate what the **risk appetite** may be. Risk Appetite is the organization's willingness to accept and manage risk in pursuit of its objectives. By defining risk appetite, organizations can align risk-taking decisions with their strategic goals, guide risk management efforts, allocate resources effectively, communicate with stakeholders, and promote a risk-aware culture. Risk appetite statements should be prepared and tailored to the specific organization, its industry, and its objectives. Some examples of this could include:

> *"We are willing to accept moderate fluctuations in financial performance to pursue strategic growth opportunities, but we will avoid risks that could jeopardize the long-term financial sustainability of the organization*" (Financial Sector Entity)
>
> *"Protecting the confidentiality, integrity, and availability of our information assets is a top priority. We have a low-risk appetite for security breaches and will invest in robust security measures to safeguard our sensitive data and maintain customer trust."* (IT Sector Entity)
>
> *"We are committed to ensuring the safe and reliable operation of our Industrial Control System. Our risk appetite is focused on maintaining the integrity, availability, and confidentiality of critical infrastructure. We have a low tolerance for risks that could result in safety incidents, system disruptions, or compromise the security of our ICS. We will invest in robust controls, proactive monitoring, and continuous improvement to mitigate risks and protect our operations and stakeholders from cyber threats, equipment failures, and human error. Our risk appetite aligns with industry best practices, regulatory requirements, and the expectations of our customers, employees, and regulatory authorities."* (ICS Sector Entity)

Organizations should also consider factors which can influence how much risk they are willing to accept such as organizational objectives, organizational opportunities, legal aspects, operational activities, technological constraints, financial constraints, supplier relationships and other human factors. Ultimately, an organization with a higher risk appetite can set a higher threshold of acceptance and can accept more risk than an organization with a lower risk appetite.

1.3 Roles and Responsibilities

The relevant roles for conducting risk management will vary from one organization to another and could be assigned to any specified team by the organization's top management. However, the responsibilities remain the same, and it is possible to identify typical roles upon whom these responsibilities might rest:

- **CRO (Chief Risk Officer)**. The CRO role may differ from one organization to another. The foremost responsibility of the CRO is to provide leadership and vision for the entire risk management function. The specific responsibilities of this position include:
  - heading the Risk Management Function;
  - chairing the Risk Management Committee;
  - reporting to senior management/board members on risk management;
  - reporting to shareholders on risk and capital management;
  - communicating risk management matters to other stakeholders including regulators.
- **CEO (Chief Executive Officer)**. The CRO will usually report to the CEO, but often where there is no CRO, the CEO (due to the responsibility they hold) becomes the CRO by default. In such situations, the CEO must manage the achievement of business outcomes alongside the risk management function.
- **Risk Management Committee**. The Committee is comprised of a variety of personnel across the organization. The Committee's function is to support the CRO. The Committee is responsible for:
  - deciding on levels of risk appetite and tolerance;
  - approving risk framework and policies;
  - allocating risk appetite & setting risk limits;
  - setting standards for risk assessment;
  - monitoring the overall risk profile;
  - identifying emerging risks;
  - proposing risk mitigation actions;

  - reviewing risk decisions.
  - The creation of the Risk Management Committee from across the organization allows for the basic requirements of relevant interested parties to be considered. The Committee is aware of existing security baselines that may already be being followed, along with internal policies, other sector-specific standards, and existing control sets.

- **Risk Owner**. The Risk Owner is the individual responsible for each major risk. The Risk Owner is internal to the business and is responsible for ensuring that risk management is taking place as risks are taken.
- **Control Owner**. The Control Owner is the individual responsible for ensuring that the control activity is in place and is operating correctly. The Control Owner does not necessarily perform the control activity, but they should have a level of oversight of its performance.
- **Internal Auditors**. These individuals can verify that there is effective and continual compliance with policies and standards, and tracking and handling of risk limit breaches.
- **Sector Regulator.** CNI sectors typically have regulatory bodies who, in partnership with the NCSC, ensure that risk assessments are conducted in line with the NCSC's guidelines, and obtain data on the outcomes of those risk assessments. In performing this function, regulators have insight into the risk profile of their sector and facilitate the aggregation of risk assessment maturity scores for further analysis with support from the NCSC.
- **Cyber Security Function.** This function maintains the cyber security controls in the system(s) supporting business activities. It should identify the potential threats to systems, understand and identify risk through cyber security risk scenarios, as well as identify threats and vulnerabilities.
- **Technology/Engineering Function.** This function supports business activities by ensuring that the underlying computer network infrastructure is functioning correctly, and that includes the administration of cyber security controls that are in place.

Note: Some of the roles listed above may overlap, be given different names, or may be combined into one, larger role.

2. Risk Management Methodology

The Risk Management Methodology incorporates and is closely aligned with ISO 27005, as previously discussed, and as shown in the Figure 4 below, the methodology is comprised of the following components:

1. ***Context Establishment.*** The gathering of relevant contextual information from across the organization.
2. ***Risk Assessment.*** The identification, analysis and calculation of risk across the organization, culminating in the evaluation of a Risk score or status.
3. ***Risk Treatment.*** The adopted response to the Risk Assessment, given what risks have been evaluated, and cognizant of the overall Risk Acceptance Criteria (derived from the Risk Appetite).
4. ***Risk Monitoring and Review.*** The continual evaluation of risk levels and appropriate responses, according to changing priorities, controls, assets and the threat landscape.
5. ***Communication and Consultation.*** The ongoing training and communication of risk in line with business priorities to enhance the awareness of the Risk Management function and promote participation and compliance.

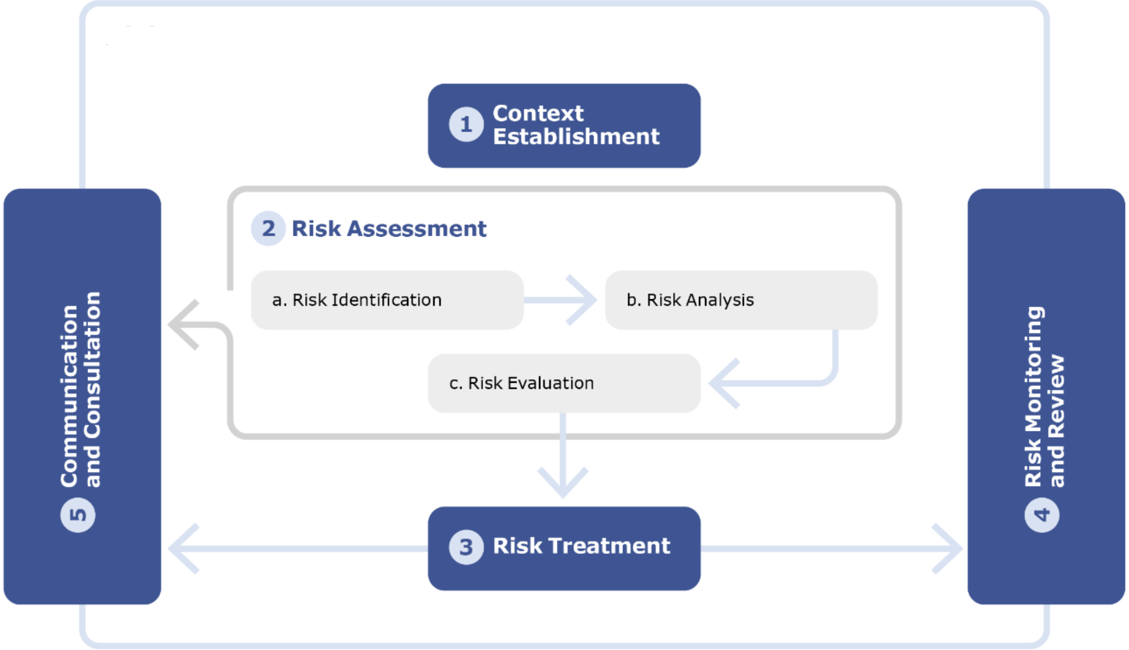


Figure 4: Risk Management Methodology Overview

The goal of risk management is to deliver each of these components in a cohesive manner. Specific details of these phases and the various component parts will now follow.

2.1 Context Establishment

Context establishment is the process of defining and understanding the specific environment, circumstances, and factors that surround all risks to the organization. It involves identifying and analyzing numerous elements that can influence the nature and impact of risks, such as organizational objectives, stakeholders, legal and regulatory requirements, and other internal and external factors.

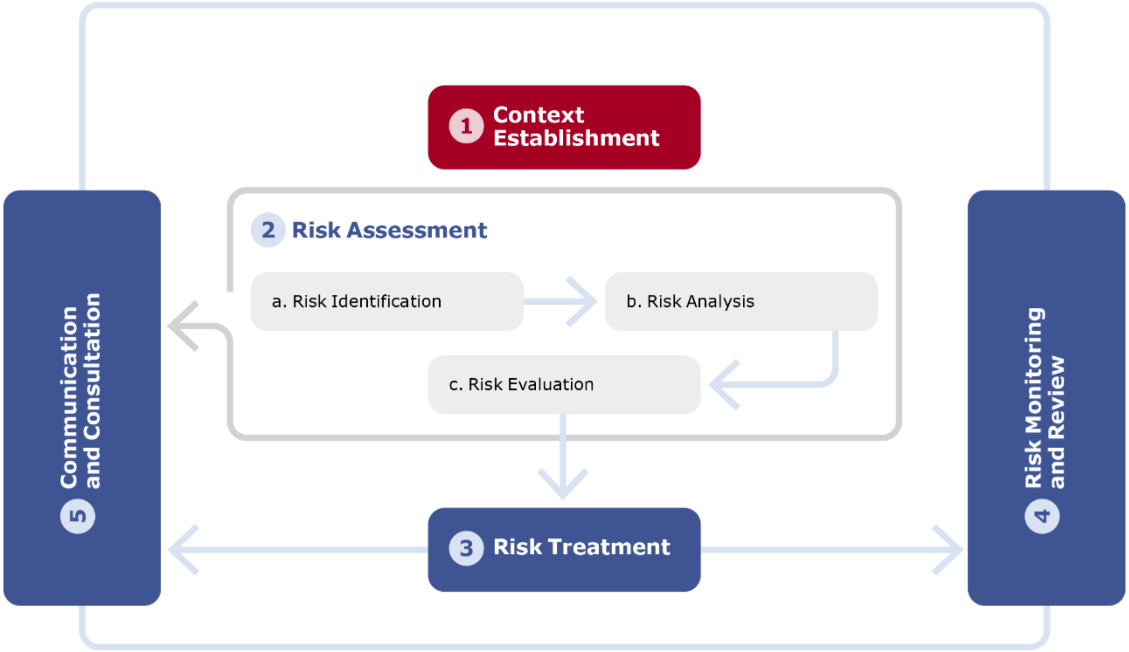


Figure 5: Context Establishment – A Closer Look

Context establishment is crucial in risk assessment, as it provides the necessary foundation and understanding to conduct an accurate and meaningful evaluation of risks. Building and expanding on the earlier Governance phase, context establishment is important for many reasons, and includes:

- **Risk Relevance.** Establishing the context helps determine the relevance of risks to the organization's objectives in the light of the organization's goals, strategies, and operational context. It provides alignment with the organization's priorities and facilitates effective risk management decision-making through a description of the organizational, technical, and operational environments in which risk assessments will take place. It includes information about the organization's structure, culture, business processes, information systems, and external factors that may impact assessment.
- **Scope Definition.** A Scope Statement is a clear and concise document outlining the boundaries and extent of the assessment, including the organizational units, processes, assets, and stakeholders to be considered. By defining the scope, risk assessors can ensure

that the assessment is comprehensive, targeted, and relevant to the specific context of the organization.

- **Risk Criteria.** Context establishment helps determine the risk criteria and parameters for the assessment. This includes defining the scales or metrics to assess the likelihood and impact of risks, as well as any other factors to be considered, such as legal, regulatory, or industry-specific requirements. The establishment of risk criteria ensures a consistent and standardized approach to evaluating risks, allowing for meaningful comparisons and prioritization.
- **Data Gathering.** A Data Collection Plan outlines how data will be collected during assessments Context establishment guides the collection of relevant data and information for the risk assessment. It helps identify the sources of information, such as internal documentation, industry benchmarks, historical data, or expert opinions.
- **Assumptions and Constraints.** Documented assumptions made during the context establishment phase, which may include limitations, dependencies, or restrictions on the risk assessment process. This helps to manage expectations and potential challenges.
- **Communication Plan**. A plan for communicating the progress, findings, and outcomes of the risk assessment to stakeholders. It outlines the frequency, channels, and formats for reporting, as well as the intended audience and purpose of each communication.

2.2 Risk Assessment Process

The risk assessment process is a systematic approach used to identify, analyze, and evaluate risks within an organization. It uses the established context as its foundation and involves several steps that help organizations understand potential threats, assess their likelihood and impact, and determine appropriate risk management strategies. It involves ***Risk Identification, Risk Analysis*** and ***Risk Evaluation*** *as shown in the figure below.*

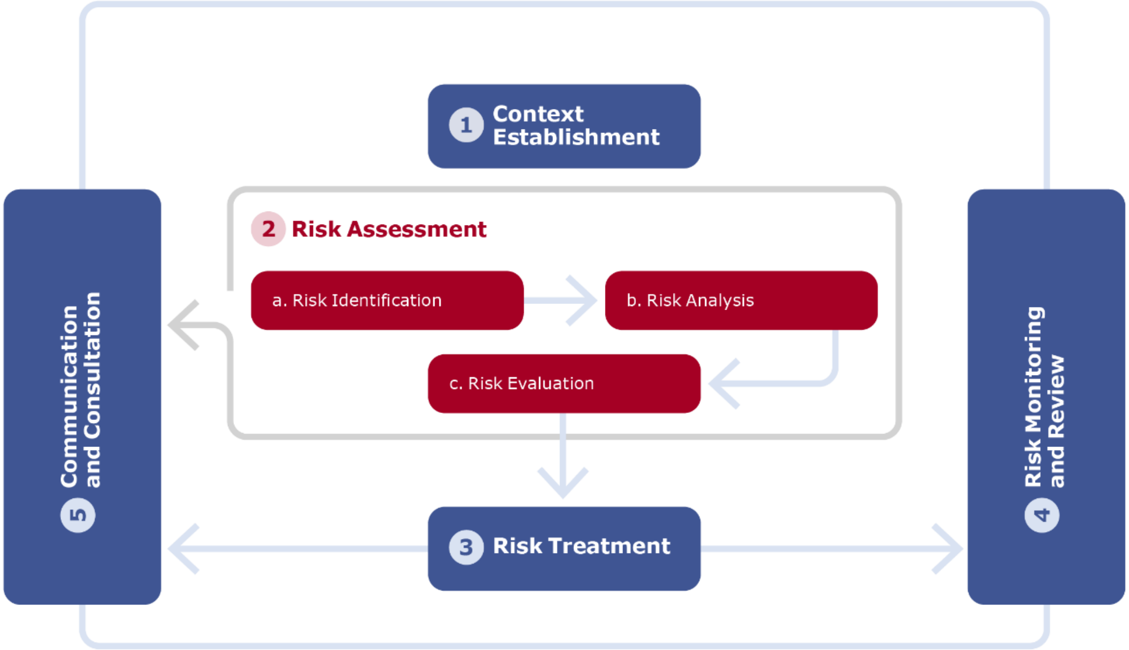


Figure 6: Risk Assessment – A Closer Look

2.2.1 Risk Identification

With context established, before beginning the process of analyzing risk it is essential to first identify risks by characterizing the organization's environmental conditions and perceived threats. Effective Risk Identification plays a critical role in enabling accurate risk analysis and from there, proactive decision-making and planning. The following items need to be established:

Identification of Assets. There should be a defined scope as to which assets are under consideration. It is helpful to categorize assets by their type, and generally most will fit into one of the following categories: devices, networks, users, software, and data.

Identification of Existing Controls. The practice of discovering if existing controls are utilized, and to what extent. For example, a control may be mentioned in policy documents, but its actual implementation may be absent. Controls should be in place, in response to one or more of the threats identified. Gap analysis may be used against a premade controls framework, such as ISO 27002 or CIS Controls.

CIS Control	CIS Description	ISO 27002	ISO 27002 Text	Asset Type	Control Type	Control
1.1	**Establish and maintain an accurate, detailed and up to date inventory of all Enterprise Assets**	5.9	An Inventory of information and other associated assets, including owners should be developed and maintained	Devices	Detect	Asset Inventory and Discovery system
10.1	**Deploy and maintain anti-malware software on all enterprise assets.**	8.1	Information stored on, processed by or accessible via user endpoint devices should be protected.	Devices	Protect	Endpoint Protection System

Table 1: Example of Control Identification using CIS Controls and ISO 27002

Identification of Threats. There are many approaches to identifying and categorizing threats, and organizations can select from these as they see fit. Organizations may consider, for example, the use of Microsoft's STRIDE threat modeling tool (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of Privilege).

Note: With Microsoft's model largely targeted at engineering projects, practitioners at Lockheed Martin introduced a 7th classification (LM - Lateral Movement) to make the model more applicable to network defense, as shown in the example below.

CIS Control	CIS Description	Asset Type	Control Type	Threat (STRIDE-LM)
1.1	**Establish and maintain an accurate, detailed and up-to-date inventory of all Enterprise Assets**	Devices	Detect	S
10.1	**Deploy and maintain anti-malware software on all enterprise assets.**	Devices	Protect	S, T, R, I, D, E, LM

Table 2: Example of Threat Identification using STRIDE-LM

An alternative to this is the provision within CIS-RAM's controls-based approach, for controls to link to specific threats. For example:

Control	Asset Type	Defends Against Ransomware	Defends Against Malware	Defends against privilege misuse	Defends against Targeted Intrusions	Defends Against Web Application hacking
Use DMARC on all emails	Applications	yes	yes	no	no	yes

Table 3: Example of Threat Modelling using the CIS-RAM Approach

Note: CIS controls and CIS-RAM are aligned with the National Risk Assessment program.

Threat identification plays an important role in determining which controls are in fact needed and/or relevant. For example, an air-gapped network does not require the same control set as a standard enterprise network, because the threat exposure is different, a significant degree of Risk Avoidance is already in place, and many of the possible controls are irrelevant.

It is important that these considerations are informed by the latest and most relevant reporting, available through Open-Source Intelligence (OSINT) or other sources. Enterprises may use historical threat occurrence data to generate likelihood figures (e.g., annual expectancy), and to define what the threats actually are.

Identification of Vulnerabilities. Vulnerabilities must be identified for each asset. Each type of asset within the scope should come into consideration. Vulnerabilities include known, technical vulnerabilities like CVEs (Common Vulnerability and Exposures), but must also include non-CVE vulnerabilities, such as misconfigurations, and design weaknesses.

Note: Vulnerabilities are tied to assets and controls and are not considered in relation to threats.

2.2.2 Risk Analysis

Risk Analysis is the outcome of assessing, across the identified assets, the **likelihood** of a risk occurring, together with its **consequences**. Risk Analysis takes the previous data gained from ***Risk Identification*** and performs ***Risk Estimation*** on that data. Organizations should consider how they will define likelihood, consequence, and risk level criteria.

2.2.2.1 Consequence (Impact)

These should define the significance of information security events to the organization. Furthermore, these should be developed and specified in terms of the extent of damage or loss, or harm to an organization or individual resulting from the loss of confidentiality, integrity and availability of information. Losses can take many forms as loss of life, loss of staff, adverse effect on plans, loss of business, loss of market advantage/reputation, breach of contract, breach of the law, negative impacts on the environment.

While many of these can be expressed in financial terms, others cannot, and the simple application of a linear scale may also not be appropriate. **Variations** on this theme may be in terms of**:**

- **Mission**. In other words, what impact is there to the benefit that your enterprise provides your customers, clients, constituents, or the public.
- **Operational Objectives.** What impact is there on the business or organizational goals.
- **Financial Objectives.** What are the unexpected cost outlays that your enterprise could or could not tolerate.
- **Obligations**. What harm could foreseeably come to others as a result of a cyber security incident.

Mission		
Consequence (Impact)	**Impact Score**	**General Description**
Negligible	1	The Mission is unaffected and remains intact.
Acceptable	2	The Mission has been compromised but does not require correction.
Unacceptable	3	The Mission has been compromised in a way that requires correction, but that correction can be achieved through the normal course of business.
High	4	The Mission has been compromised in a way that requires correction, and that correction can only be achieved through extraordinary efforts.
Catastrophic	5	The Mission has been compromised in such a way as it can now no longer be achieved.
Operational Objectives		
Consequence (Impact)	**Impact Score**	**General Description**
Negligible	1	The Operational Objectives, as defined, are not affected and the growth plan remains intact.
Acceptable	2	The Operational Objectives have been compromised but do not require correction.

		The Growth plan would be off target, but within variance.
Unacceptable	3	The Operational Objectives have been compromised in a way that requires correction, but that correction can be achieved through the normal course of business. The Growth plan would be out of variance but can be recovered within a fiscal year.
High	4	The Operational Objectives have been compromised in a way that requires correction, and that correction can only be achieved through extraordinary efforts. The Growth plan would be out of variance and may require multiple years to correct.
Catastrophic	5	The Operational Objectives can now no longer be achieved. The Business/organization is no longer able to grow.
Financial Objectives **(NOTE: actual monetary figures will need to be applied to each of the below definitions, and this will vary from one organization to another)**		
Consequence (Impact)	**Impact Score**	**General Description**
Negligible	1	The Financial Objectives, as defined, are not affected.
Acceptable	2	The Financial Objectives have been compromised but do not require correction.
Unacceptable	3	The Financial Objectives have been compromised in a way that requires correction, but that correction can be achieved through the normal course of business.
High	4	The Financial Objectives have been compromised in a way that requires correction, and that correction can only be achieved through extraordinary efforts.
Catastrophic	5	The Financial Objectives can now no longer be achieved.
Obligations		
Consequence (Impact)	**Impact Score**	**General Description**
Negligible	1	No harm could foreseeably result.
Acceptable	2	Any harm that could result would not require correction, repair, or compensation to make the harmed parties "whole."
Unacceptable	3	Correctible harm may occur to one or few others.
High	4	Correctible harm may occur to many others, or harm that can be partially corrected for a few others may occur.
Catastrophic	5	We would not be able to protect others from any degree of harm.

Table 4: NCSC Levels of Consequence (Impact)

2.2.2.2 Likelihood (Expectancy)

When considering Likelihood or “Expectancy” some controls may already be in place, and so this becomes an exercise in assessing what the likelihood is of the risk manifesting, given the extant controls. Consideration should also be given to the maturity of the controls presently in place, as this will affect the assessment of the Likelihood (Expectancy) score. Note how the following definitions are presented in this way.

Many factors help determine likelihood criteria, which can be expressed in probabilistic terms (the chances that something will occur within a given time frame) or frequentist terms (the average number of occurrences in a given time frame). Establishing a Likelihood criteria means working within the limits of anticipated event likelihood – these should be chosen according to the organization's context and the scope of its Information Security Management System.

Likelihood (Expectancy) over a specified time period, e.g., 1 year	Expectancy Score	Criteria
Remote	1	Existing safeguard would reliably prevent the threat.
Unlikely	2	Existing safeguard would prevent most of the occurrences of the threat.
As likely as not	3	Existing safeguard would prevent as many threat occurrences as it would not.
Likely	4	Existing safeguard would prevent few threat occurrences.
Certain	5	Existing safeguard would not prevent threat occurrences.

Table 5: NCSC Levels of Likelihood (Expectancy)

Risk Level Criteria. Organizations should define how they arrive at an overall Risk Level, given the likelihood and consequence criteria and the actual findings.

2.2.2.3 Risk Estimation

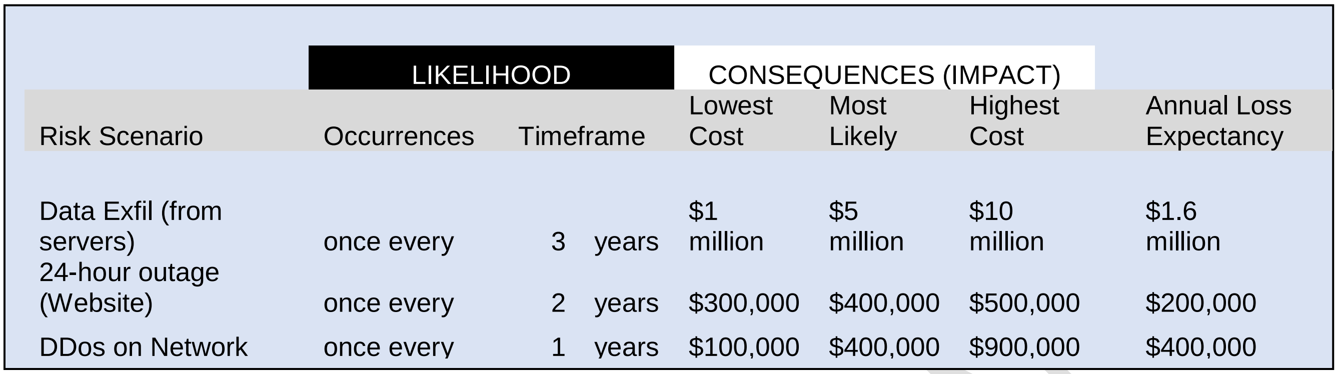
Risk Estimation is the process of assigning values to the probability and consequences of a risk. There are several approaches to this, qualitative, quantitative or a mixture of the two. A qualitative approach uses committee-style, opinion-based reasoning to identify the top risks given the potential impact to the asset concerned, and the likelihood of the threat manifesting. The use of a qualitative risk assessment matrix (Figure 12) is common and often takes place as a paperwork/tabletop exercise. The resultant calculation produces indicative figures rather than real, tangible cost values. The Impact and Expectancy scores can help to derive an overall Risk score which will map to the figure.

Likelihood (Expectancy)	Consequence (Impact)				
	Catastrophic	High	Unacceptable	Acceptable	Negligible
Certain	🟧	🟧	🟨	🟨	🟨
Likely	🟧	🟨	🟨	🟨	🟩
As Likely as not	🟨	🟨	🟨	🟩	🟩
Unlikely	🟨	🟨	🟩	🟩	🟩
Remote	🟩	🟩	🟩	🟩	🟩

🟧 High 🟨 Moderate 🟩 Low

Table 6: Example Qualitative Risk Assessment Matrix

A Quantitative Risk Assessment may follow on from those risks identified as prioritized after an initial qualitative estimation. This approach is efficient, by focusing efforts on the more significant risks. Quantitative risk estimations are often more complex and require more time to deliver. What is ultimately considered is the Business Impact. For a qualitative estimation, that is typically represented by a rating – Low, Medium, or High. For a quantitative estimation, it will be in terms of money or hours – a tangible figure.



	LIKELIHOOD			CONSEQUENCES (IMPACT)			
Risk Scenario	Occurrences	Timeframe		Lowest Cost	Most Likely	Highest Cost	Annual Loss Expectancy
Data Exfil (from servers)	once every	3	years	$1 million	$5 million	$10 million	$1.6 million
24-hour outage (Website)	once every	2	years	$300,000	$400,000	$500,000	$200,000
DDos on Network	once every	1	years	$100,000	$400,000	$900,000	$400,000

Figure 7: Example of a Quantitative Risk Assessment

2.2.2.4 Gap Analysis and Risk Calculation

The recommended Risk Assessment Method allows the aforementioned calculations to be housed inside a single tool. NCSC's National Risk Assessment Toolset and self-assessment questionnaire (hereon referred to simply as the Toolset) which is based on the CIS RAM Risk Assessment Method (CIS-RAM), has been selected for recommendation because it satisfies the following criteria:

- **Consistency**. Similar results should be obtained irrespective of who is performing the risk assessment.
- **Comparability.** Assessments performed for different risks should produce comparable results when using the same Risk Level Criteria.
- **Validity**. The results should reflect reality as closely as is practically possible.

The tool relieves risk assessors from much of the preliminary work of Threat Identification, Asset /Vulnerability Identification and Likelihood estimation. It is a controls-based approach to Risk Assessment which means that a number of realistic assumptions as to the 3 aforementioned factors, are built into the deployment (or otherwise) of the controls.

Each control is in effect a response to a threat vector being realized upon a certain type or class of Asset. As a result, descriptions of the threat vectors countered, the asset the control seeks to defend, along with the likelihood of that threat being realized based on the asset type and real-world statistical data, can be packaged alongside each control.

Control (Safeguard) Maturity. The Likelihood, or expectancy of a threat manifesting is largely influenced by the imposition of a control and the maturity of that control. Risk is **then** calculated **in the usual way** as the product of Likelihood (Expectancy) and Consequence (Impact).

Impact. Impact (Consequence) may generally be **financial** but is not limited to this and may incorporate aspects of all 4 previously identified variants of consequence (Mission, Operational Objectives, Financial Objectives, Obligations).

In summary, **Risk** is then calculated in a conventional way, however, the factors below contain several component parts which the Toolset and CIS-RAM automate the establishment of, in conjunction with each specific control. The **control/safeguard** in question determines the **asset type**, which determines an **expectancy value**, which is in turn mitigated by the **control/safeguard maturity**. This establishes the **Likelihood** which is multiplied against the assessed **Consequence (Impact)** value to get the **Risk Score**. This calculation is mapped out in the figure below.

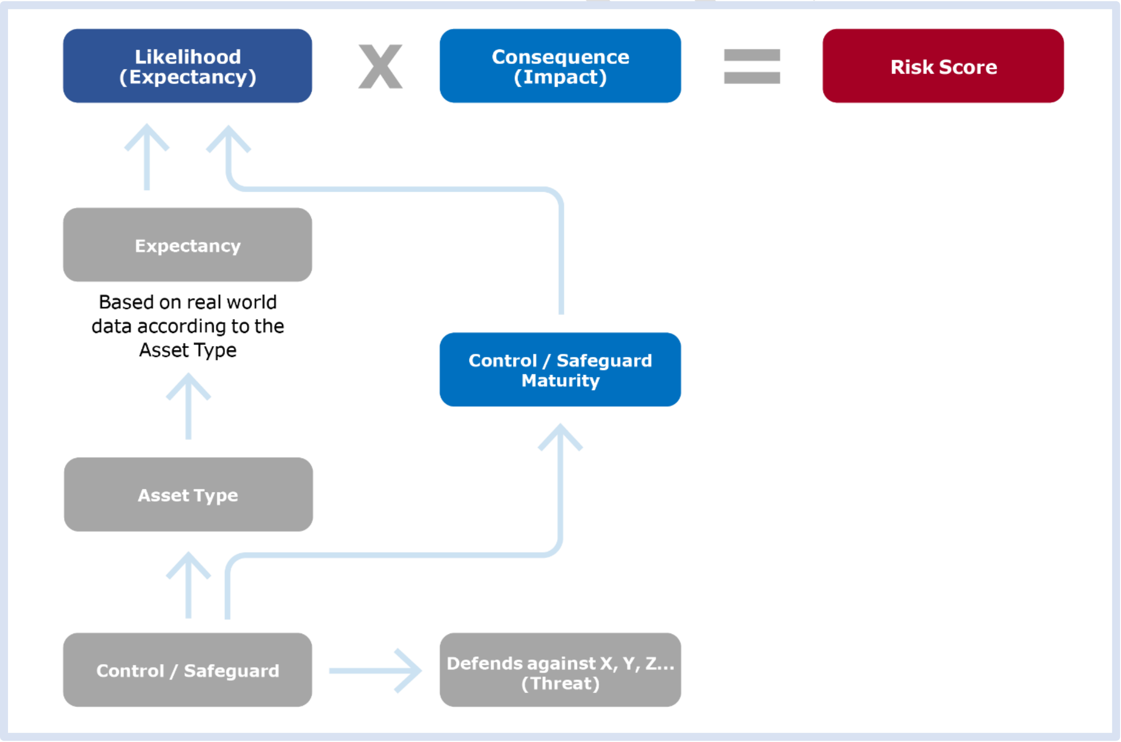

Likelihood (Expectancy)
X
Consequence (Impact)
=
Risk Score
Expectancy
Based on real world data according to the Asset Type
Control / Safeguard Maturity
Asset Type
Control / Safeguard
Defends against X, Y, Z... (Threat)

Figure 8: Calculation of Risk Score

The following approximation from the Toolset exemplifies this:

Determin Determin

Control	Asset Type	Safeguard Maturity (0-5)	Defends Against Ransomware	Defends Against Malware	Defends against privilege misuse	Defends against Targeted Intrusions	Defends Against Web Application hacking	Expectancy Score	Impa Scor
Use DMARC on all emails	Applications	2	Yes	yes	no	no	yes	3	3

Determin

Table 7: Toolset Implementation of Risk Calculation

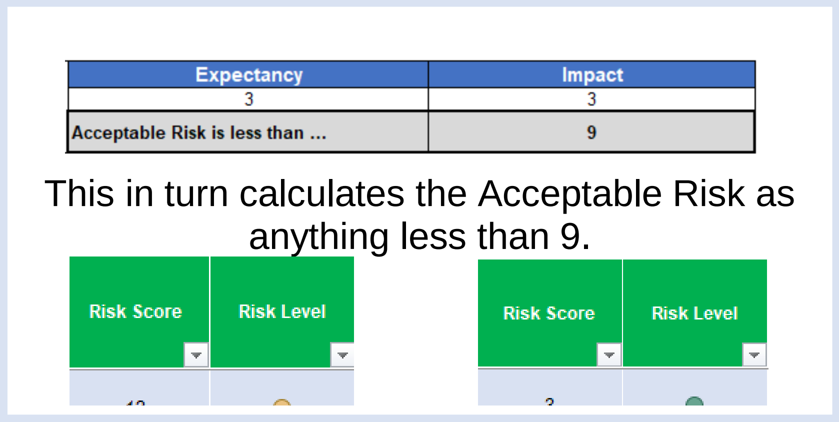
This process is automated because the only values which need to be supplied in order to get a valid **Risk Score** in compliance with the aforementioned Risk Assessment concepts are scores for safeguard maturity and impact.

2.2.2.5 Risk Evaluation

The level of risk for all relevant incident scenarios is calculated. During risk evaluation, risk levels are compared against risk acceptance criteria in order to determine which risks must undergo treatment. It is dependent on the case, but low risks are typically within the risk acceptance criteria, whereas anything higher may be determined to require treatment. In this case, Risk Acceptance Levels will already have been defined, in line with the overall Risk Appetite.

This level is simplified down to a single threshold value. Either the calculated Risk score (from the Expectancy x Impact calculation) exceeds this, or it does not. In the former case, additional mitigating controls will need to be considered in order to reduce the risk level to a more acceptable value.

For example, the Risk Assessment Tool allows for the entering of Risk Acceptance Criteria in terms of Impact and Expectancy (see earlier definitions).



Expectancy	Impact
3	3
Acceptable Risk is less than ...	9

This in turn calculates the Acceptable Risk as anything less than 9.

Risk Score	Risk Level
12	●

Risk Score	Risk Level
3	●

Figure 9: Tool Evaluated Risk Score In-Line with Acceptance Criteria

2.3 Risk Treatment

The Tool calculates the actual risk score from the safeguard in place and the potential impact, and the figures above demonstrate the attainment of acceptable and unacceptable, resultant risk scores. By treating risks, organizations can lower their risk profile and significantly reduce the likelihood of experiencing costly security incidents. The possible consequences of a realized risk can be mitigated, so that it falls within risk acceptance criteria and can be accepted (or “tolerated”).

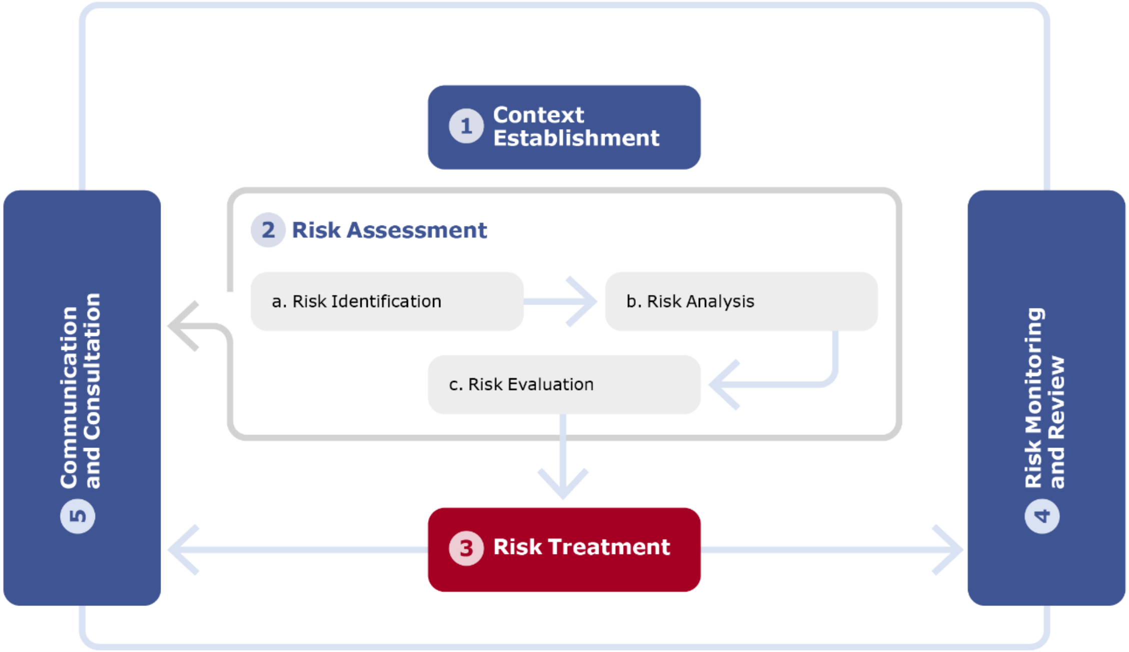


Figure 10: Risk Treatment – A Closer Look

Acceptance is one of four conventional treatments:

- ***Risk Acceptance.*** Risk Acceptance is dependent on the Risk Appetite of the organization. The risk is accepted because it is: below the organization’s risk appetite, it is not possible to implement any practical safeguard or control, or because the cost of implementing a safeguard significantly outweighs the value of the asset it is designed to protect.
- ***Risk Reduction (Mitigation).*** Measures are designed to lower the impact or the probability of occurrence of a risk in order to make it tolerable. Note: this option does not eliminate all of the risk, instead lowering it to an acceptable level.
- ***Risk Transference.*** Risk transfer involves shifting the impact or responsibility of a risk to another party. For example, purchasing insurance.
- ***Risk Avoidance*****.** This is where an entity takes actions to avoid the risk altogether, because the magnitude of the risk is so high, and any available mitigation strategy is either too expensive or infeasible.

Note: The Assessment Tool’s controls-centric approach limits use to the first two treatments – Risk Acceptance and Risk Reduction. With controls being used as the

starting point for the assessment, it would be inappropriate to "Transfer" or "Avoid" them in the way one might do so with respect to a risk.

2.3.1Residual Risk / Risk Acceptance Stage

Residual Risk is the remaining risk after a safeguard has been applied. It is this value which senior managers then use to make a decision based on the organization's Risk Appetite. The treatment plan must be agreed by senior management. During this step, heads of departments may question costs that they think are too high or consider accepting certain risks. These exceptions must be justified. The Toolset adds additional considerations relating to the cost of implementing the safeguard and allows room for discussion over whether the implementation of a safeguard imports additional risk.

2.4 Risk Monitoring and Review

Risks change frequently, and the RMF must adapt. It is vitally important that an up-to-date view of all risks is maintained. This is because the nature of the threat to individual assets can change; new assets can be added which bring with them their own risk-related connotations; existing assets may be updated or changed in their implementation as part of change-management; new security controls may be added, and old security controls may be removed.

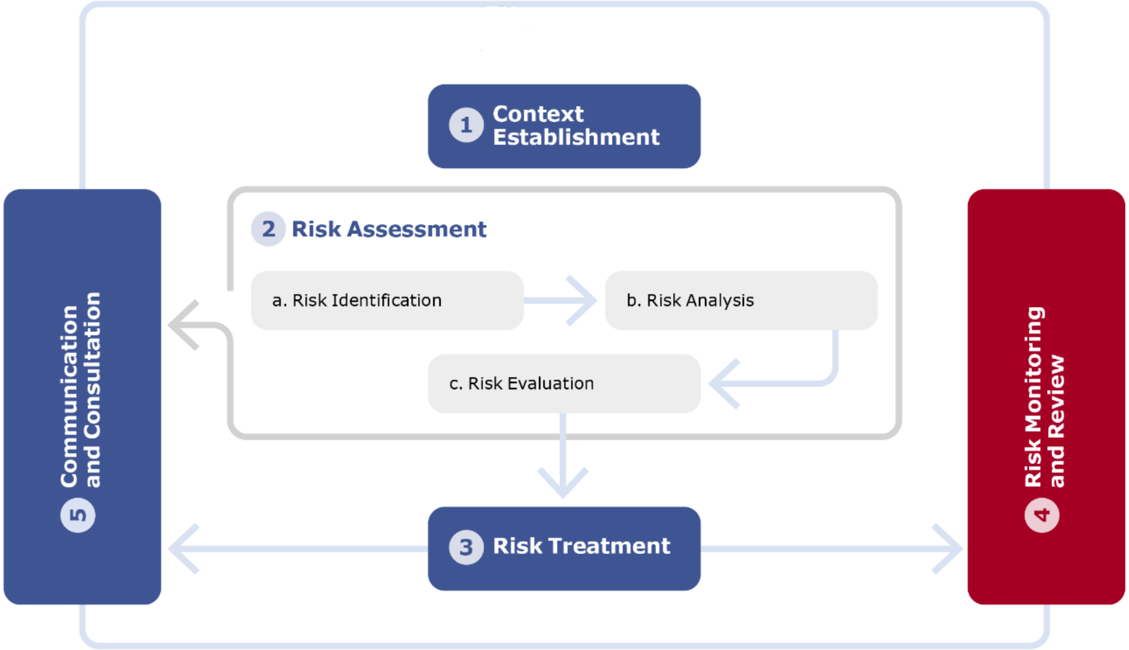


Figure 11: Risk Monitoring and Review – A Closer Look

2.4.1Risk Register

Risk review and monitoring is facilitated by the creation of a Risk Register, where the assets and their vulnerabilities are identified; Threats are identified and understood; the risk has been calculated; the risk acceptance level has been set; controls have been set to correspond to risk, where appropriate; residual risk values have been calculated; the risk has been either accepted or otherwise according to the acceptance criteria.

Risk Registers allow for the Risk Management Function to be monitored and reviewed effectively. It is not merely a case of doing it once and then never repeating. It is intrinsically iterative and aimed at continual improvement.

A very basic Risk Register might have the following column headings:

Risk Identification/Analysis/Evaluation

Risk Name	Risk Description	Asset Type	Safeguard Maturity Score	Expectancy Score	Impact Score (Mission)	Impact Score (Operational Objectives)	Impact Score (Financial Objectives)	Impact Score (Obligation

Table 8: Example of a Basic Risk Register

Note: The National Risk Assessment Program Toolset's assessment questionnaire forms the basis of a risk register, as does CIS-RAM. It is recommended that the organization's risk register be based on this, or else be constructed in a format that is compatible with the assessment questionnaire.

2.4.2Risk Treatment Plan

A Risk Treatment Plan takes the information from a Risk Register and seeks to apply a strategy for the chosen Treatment, according to a timeline for implementation. It is a way of charting what the organization is going to do with respect to the application of additional mitigations or controls and in response to the chosen treatment.

An example Risk Treatment plan may have the following column headings:

Risk Treatment

Risk Name	Treatment Strategy	Control Name	Control Description	Revised Implementation	Revised Risk Score	Cost of Revised Control	Implementatio Date

Table 9: Example of a Risk Treatment Plan

2.4.3Key Risk Indicators

A Key Risk Indicator (KRI) measures the probability that the likelihood of an event, combined with its consequences, will exceed the Risk Appetite of the organization. The establishment of KRIs can provide a number of key benefits. KRIs can give an organization advanced notice that a risk is about to be realized and provide insight into the failings of existing monitoring and use of controls. KRIs are highly specific to a given organization, as they are derived with important considerations in mind:

- An understanding of those corporate attributes and assets which are key to the organization’s success.
- knowledge of Risks, Threats, and Vulnerabilities specific to the organization, together with the organization’s ability to implement mitigations.
- An understanding of how risks are prioritized, specific to the organization.
- How metrics can be applied to identify when and how an identified risk becomes a serious threat to critical attributes of the organization.

KRIs should be approved by senior management and are developed in relation to an organization's people, processes, technology, facilities and other elements critical to its operations. KRIs also provide measurement points that, if exceeded, could disrupt operations.

Category	Risk	KRI
Business Interruption	**ISP failure**	Number/length of ISP outages.
	Vendor service interruption	Number of applications currently running in the organization without a Service Level Agreement (SLA).
	Data loss	Number of backup failures.
Reputational Damage	**Critical incidents not resolved**	Number of Critical Incidents. Time to resolve critical incidents.
	Anonymous data leaks	Number of active database admin accounts.
	Terminated employees accessing systems	Average time between termination of employment and closing of their accounts.
Information Breach	**Malware infection**	Number of outbound malware related connections per month.
	Phishing	Number of users who click on a link in internally generated phishing campaigns.

Table 10: Examples of KRIs

2.5 Communication and Consultation

Sharing and exchanging information about risk facilitates agreement between decision-makers and other stakeholders on how to manage risk. Communication plans should be established for normal and emergency operations. Risk communication should occur throughout the overall risk management operation. Communication facilitates good decision-making on the part of stakeholders and framework operators.

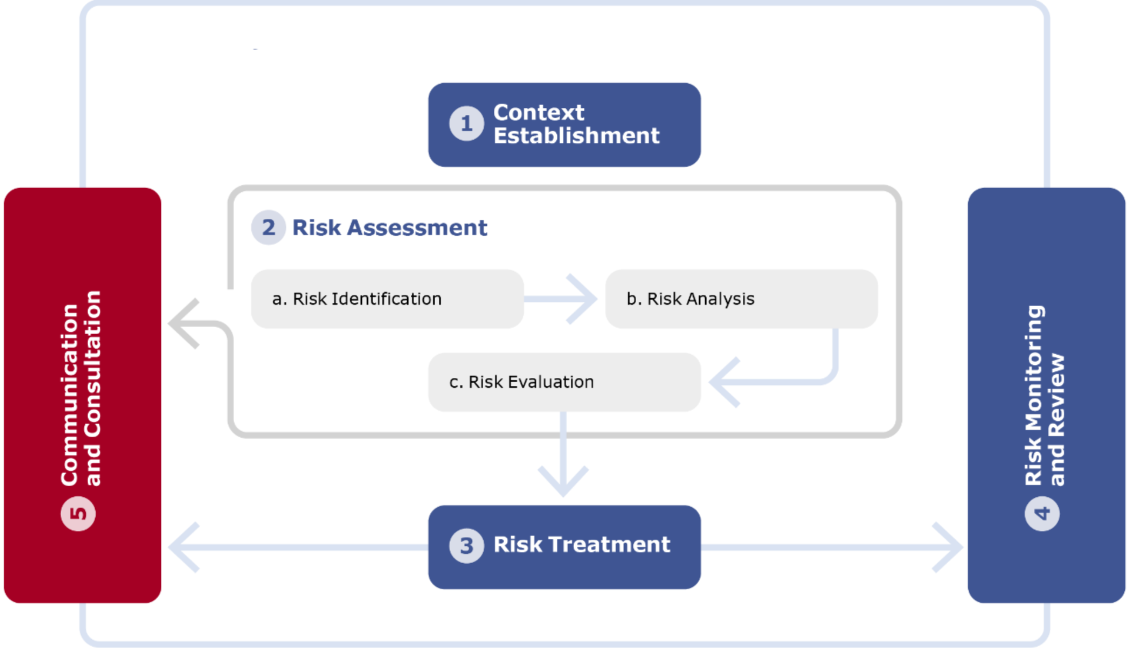


Figure 12: Communication and Consultation – A Closer Look

2.5.1 Training and Awareness

A risk management awareness program is an effective way to ensure that all employees fulfill their own obligations in terms of managing risk as they encounter it in the organization.

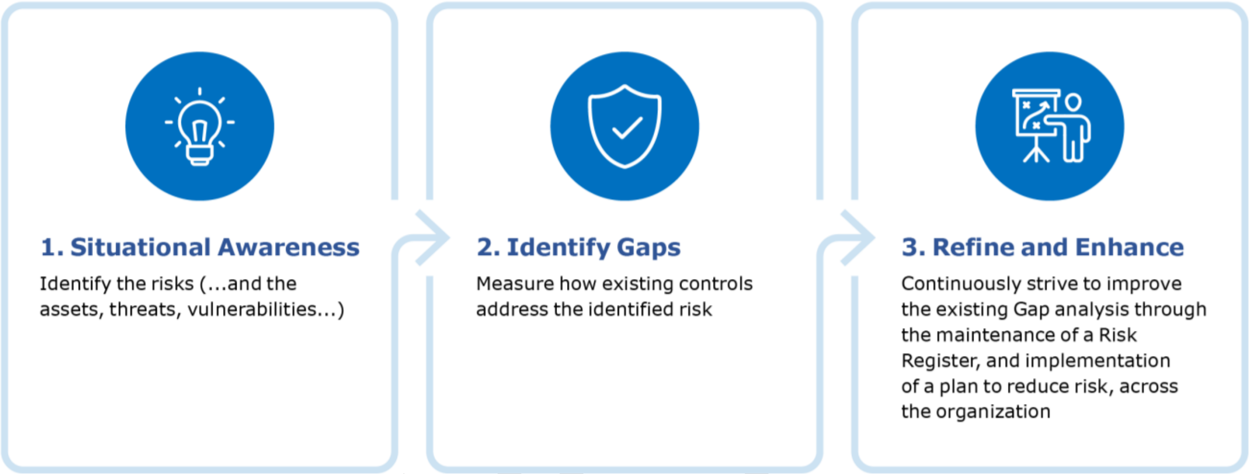
Participation. The risk management awareness program can engage with the rest of the workforce when planning risk management activities. A broad degree of participation from employees can communicate the importance of risk management by participating in workshops, brainstorming sessions or other meetings.

Communication. The Importance of identifying risk and complying with controls can be regularly communicated through specific information days and regular internal communications, whether that be through cloud communication platforms, email or intranet pages.

Training. Formal training in risk management or risk assessment can be carried out within the organization. It can be targeted at different levels, for example, induction, participation or management related training. Training can be delivered through in-person sessions, e-learning platforms or other digital mediums.

3. Framework Implementation

When organizations perform risk management in line with this document, they will either be doing it for the first time, or they will be building upon the foundation laid by a previous iteration. The figure below illustrates the desired progression for organizations, regardless of their current level of maturity.



1. Situational Awareness

Identify the risks (...and the assets, threats, vulnerabilities...)

2. Identify Gaps

Measure how existing controls address the identified risk

3. Refine and Enhance

Continuously strive to improve the existing Gap analysis through the maintenance of a Risk Register, and implementation of a plan to reduce risk, across the organization

Figure 13: Maturity Progression for Organizations and Entities

3.1 Implementation for the first time

Not every organization has implemented a Risk Management Framework before. In these cases, it is essential that Step 1 above is carried out comprehensively. Time investment at this stage is fundamental to the successful and efficient implementation of later stages of the process.

3.2 Updating and existing implementation

Where organizations have already carried out risk management functions before (i.e., some awareness of assets, threats, vulnerabilities, and risks; exist, and to a degree, some level of prioritization of risk has been applied), then it is likely that less effort will be required before moving to Step 2. For these organizations, it is a matter of matching existing controls against a recognized controls framework in order to identify gaps.

3.3 Refining and Enhancing

Risk management is a continual process and a perpetual endeavor to minimize risk as far as is practicable. Risk registers of a high level of maturity are only achieved through numerous iterations of the framework. Refinement and enhancement at this stage is more nuanced - fine-tuning, underpinned by significant investment in the prior stages.

National Risk Assessment

Roles, Responsibilities & Summary of Expectations

Each organization must nominate an individual whose responsibility it is to act as an external point of contact for risk. This may be the CEO, the CRO (Chief Risk Officer) where such a role exists, or another person to whom delegated responsibility has been granted, and who will act as the conduit through which elements of that entity's risk assessment results and maturity estimates may be passed through to the sector regulator and the NCSC. NCSC and sector regulators will maintain a list of all such appointments for each entity and may liaise with them on a regular basis.

Recording and Reporting Requirements

Risk assessment reporting should align with the risk assessment method. NCSC provides guidance notes for entities, describing the method for risk assessment to encourage standardization across each sector. Standardized assessment results can enable aggregation and analysis at the sector and national level.

Nominated liaisons will be the points of contact between the organizations, the sector regulators, and the NCSC.

Sector regulators with administrative authority are instrumental in ensuring regular communication occurs such that sector entities are fully engaged with the National Risk Assessment requirements, most notably in terms of the correctness of direction and guidance notes, and the notification of deadlines, timelines and submission particulars.

Threats and Vulnerabilities - Examples

Threats

Ransomware	Eavesdropping on Network
Phishing	Botnet
Insider Threat	Malware on USB
Data Leak	Malicious Website
Unauthorized Access to Network	Malicious Email Attachments
Unauthorized Access to Host	Password Guessing
Malware	User enumeration
Social Engineering	OSINT Collection
Exploitation of vulnerability	Adware
Banking Trojan	Data Exfiltration
DDoS	

Vulnerabilities

Improperly configured local permissions	Installation of open source software	Lack of inventory maintenance	Lack of backup procedures
Unpatched servers	Non-compliant hardware added to network	Lack of network segmentation	Many points of ingress/egress to the broader internet
Out of date software components	User accounts improperly provisioned	Lack of Multi Factor Authentication (MFA)	Unmanaged VPN access
Users who don’t complete compliance training	Improper termination of accounts	Out of date cryptography ciphers	Wi-Fi network shared medium
Firewall rules out of date	Default account passwords unchanged / password policy not enforced	Cloud storage left open and unprotected	Improper management of admin privileges
Operating System hardening not performed	Lack of network/system monitoring/alerting		

Glossary

Asset	Something either tangible (physical) or intangible which is owned by an organization and to which value can be attributed.
Chief Risk Officer (CRO)	The individual with overall responsibility for risk management within an organization and who chairs the Risk Committee.
Consequences	Can be assessed using abstract levels (Low, medium, high for example) or using monetary or other objective measures.
Inherent Risk	The amount of Risk attributable to a situation without the application of any controls
Likelihood	The probability that something will happen (usually in percentage terms, and evaluated over a fixed term)
National Risk Assessment (NRA)	A campaign led by the Bahrain Ministry of the Interior, to establish assessment outcomes at a national level, for Risk.
Open Source Intelligence (OSINT)	Intelligence derived from open sources, including but not limited to, the indexed web, journals, articles, reports, forums, social media activity, all publicly available.
Residual Risk	The amount of Risk attributable to a situation after controls have been applied.
Risk	A situation where there is a probability that a certain degree of harm or degradation will occur with respect to one or more assets.
Risk Acceptance	The formalized level at which a company or organization tolerates or treats risk.
Risk Appetite	The degree to which a company or organization is willing to accept that inherent risk can be tolerated.
Risk Assessment Program	A subset of activities within a Risk Management Framework, where Risks are identified, analyzed and evaluated, leading to a decision over how the risks are to be treated.

Risk Committee	A body in each organization established to oversee Risk management and Risk Assessment within.
Risk Management Framework (RMF)	The overarching approach to handling and managing Risk in an organization.
Risk Register	A continuous monitoring/review tool, maintained by an organization to provide an overview of how risks are being evaluated, re-evaluated and treated.
RMF	See Risk Management Framework.
Sector Regulator	Government appointed individual(s) with responsibility for ensuring that Government best practices and guidelines are adhered to by sector constituents.
Threat	An agent with the capacity to cause an adverse effect on an asset or assets.
Vulnerability	A weakness borne by an asset.

References

CIS Controls	https://www.cisecurity.org/controls
CIS-RAM	https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method
ISO 27001	https://www.iso.org/isoiec-27001-information-security.html
ISO 27002:2022	https://www.iso.org/standard/75652.html
ISO 27005:2022	https://www.iso.org/standard/80585.html
ISO 31000	https://www.iso.org/iso-31000-risk-management.html
Kingdom of Bahrain National Cyber Security Center (NCSC)	https://www.ncsc.gov.bh/en/index.html
MITRE ATTACK	https://attack.mitre.org/
NIST 800 Series	https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information
STRIDE Framework for Threat Identification	https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
STRIDE-LM	https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf

--End of Document --