



Workbook for NCIIPC based Transformation of Indian Organizations

Enhancing the Cybersecurity Posture for Critical
Information Infrastructures

Comprehending

1

Vivek Kant, Soham Mohanty

HF
SS Studios

The authors would like to acknowledge Thomas Raju for his support during the early stages of the project. The authors would like to acknowledge Gokul S for his support during the latter stages of the project. They would also like to express their gratitude to the participants, subject-matter experts (SMEs), and organizations that supported the development of this Toolkit.

© 2026 Vivek Kant.

All rights reserved. No part of this book may be reproduced in any form without permission from the author or publisher.

To request permission, contact Vivek Kant, vkant@iitk.ac.in

Published by

HFSS Studios

Department of Design

Indian Institute of Technology Kanpur

Kalyanpur, Kanpur 208 016, India

<https://home.iitk.ac.in/~vkant/>

ISBN Number : 978-93-6128-253-9

ISBN 978-93-6128-253-9



Navigating Through the Workbooks

Current Phase - Workbook 1: Comprehending

How to use this workbook along with others?

This workbook functions as part of a progressive series designed to guide organizations through various stages of cybersecurity maturity. Each workbook builds upon insights from the previous one, ensuring a structured and continuous improvement process. When used collectively, they create an integrated framework that helps organizations internalize NCIIPC principles, align teams around shared objectives, and sustain long-term cybersecurity growth.



Workbook 1 Comprehending

In the very first phase the key idea is to self assess and comprehend the essential status of the organization, in terms of the various domains and respective controls.



Workbook 2 Sensemaking

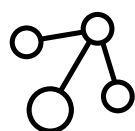


Workbook 3 Reformulating, Implementing

Table of Contents

Workbook for NCIIPC based transformation of Indian Organizations

Benefits of the Workbook	1
Introduction	2
Collaborative Change Management Process	4
NCIIPC.....	8
Domains and Controls.....	11
Domains, Controls and Risk Priority Score.....	15
Understanding the Risk Priority Score (RP).....	16
Scoring Criteria for Assessment.....	18
How to use the Worksheet.....	20
Governance.....	21
Risk Management.....	27
Asset Management.....	31
Identity and Access Management.....	38
Secure Design and Engineering.....	42
Vulnerability and Patch Management.....	47
Threat Intelligence.....	51
Security Incidence Management.....	55
Resilience Management.....	59
Physical and Environmental Security.....	65
Data Protection.....	69
Supply Chain Risk.....	73
Workforce Management.....	77
Change Management.....	81
Situational Awareness.....	85



Benefits of the Workbook

Enabling adoption of NCIIPC

Building a shared cybersecurity culture in organizations

This workbook represents a paradigm shift in how organizations approach cybersecurity maturity and adopt NCIIPC guidelines. Rather than relying solely on external audits or one-time assessments, it empowers organizations to build internal capacity, ownership, and accountability for protecting Critical Information Infrastructure (CII).

From Auditor Dependency to Employee Empowerment

With a typical cybersecurity assessments, organizations get to wait until one of these third-party auditors identify their gaps, leading them to be in a reactionary posture. Through this workbook, a bottom-up approach is facilitated in which CISOs and their teams can assess, score, and prioritize their selected controls in a structured, consistent, and meaningful way. Audit Preparation gives way to long-term process and control improvement

Self-Assessment for Self-Development

The checklists, scoring models, and maturity parameters of the workbook promote constant self-evaluation, allowing organizations to visualize their growth and maturity in real-time.

Internal Capacity Building

It serves as a training and enablement tool by establishing clear scoring criteria for each of the common controls (AML, MML, RL) and maintaining control-specific guidance, as well as activity templates. Cross-departmental teams can assess their participation in cybersecurity, monitor progress, and collaborate effectively.

Secure, Private, and Insightful

Minimizing unnecessary sharing of data with third parties or Auditors. Detailed reports are not exported. The workbook delivers internal dialogue and action. The insights gained through it empower leadership to make informed decisions without sacrificing operational insight or confidentiality.

A Stronger, Scalable Model for NCIIPC Adoption

In doing so, the workbook serves as a translation layer between national directives and actionable ground-level controls by operationalizing NCIIPC guidelines (in conjunction with global best practices) into a set of practical measures. It fosters adoption, removes mystery from implementation, and offers a repeatable model that organizations can own, improve, and scale.

This workbook is not just a tool — it is a strategic enabler for a more resilient, self-aware and future-ready cybersecurity ecosystem in India.

Introduction

NCIIPC transformation for organizations - 1

What is this Workbook about?

The aim of this workbook is to help you and your organization to achieve substantial clarity and ability to incorporate the controls of NCIIPC in cybersecurity practice in an easy and simple manner. A critical barrier in achieving an improved cybersecurity posture is the lack of integration of controls and the insights from audits into everyday practice of organizations.

In contrast to an externalist viewpoint of audits, through self assessment and pathways for improvement, this workbook empowers organizational actors to imbibe principles and practices of cybersecurity in their work practices at all levels of the organization.

The key idea is to develop organizational competency such that actors are able to comprehend the functioning of the larger wholes and interaction of parts in cybersecurity practices. The focus of the workbook is to enable the movement from a viewpoint of symptomatic fixes to enabling an anticipatory viewpoint on NCIIPC compatibility.

Why to use this Workbook?

The workbook is designed to be used in conjunction with NCIIPC guidelines.

The workbook addresses some unique challenges in the NCIIPC locus of cybersecurity practices:

- There is a need for tools to map the domains and control relationships to provide clarity between these two dimensions
- There is a need to understand how the relationships between domains and controls can be used to highlight areas of improvement
- There is a need to chart out courses of action , timelines and responsibilities to achieve improvement from the previous states of the cybersecurity posture.
- There is a need for planning tools that enable stakeholders to become powerful actors in improving the cybersecurity posture
- There is a need for planning tools that recognize the complexity of the cybersecurity domain, challenges of NCIIPC guidelines and the issues faced while actors interpret and adopt these in their organizations.

The workbook has been created with these above issues in mind while ensuring that NCIIPC guidelines can be successfully transformed into organizational practices, unique to each entity. Therefore, practitioners are encouraged to keep the NCIIPC document handy while using the exercises in the workbook to enhance the uniqueness and compatibility with their own organization.

The tools created in this work book bridge the gap between the complex nature of the various domains of cybersecurity, controls of NCIIPC and the adoption of these in various organizations through the use of design thinking and systems thinking tools. Such a conjoined approach allows the transformation of the organization with cybersecurity practices being developed as a human-centric enterprise. The organizational stakeholders are comprehended as powerful actors who can view the various domains and controls of cybersecurity from a vantage point of comprehensibility and adoptability.

Introduction

NCIIPC transformation for organizations - 2

Who can use this Workbook?

Specifically, the aim is to ensure organizational compliance with NCIIPC controls through collective self assessment. The emphasis on a collective focus is important as cybersecurity practice is shared across the organization. Improvement in cybersecurity posture is an organizational phenomenon. Therefore, the tools and pathways depicted in this workbook are aimed to be used in groups of people ranging from the functional role of front-line operators to CISOs.

Application of NCIIPC controls and principles can be best comprehended, implemented and sustained in a participatory mode of inquiry and execution. The aim is to accomplish the improvement of cybersecurity practices by means of organizational actors who display responsibility, accountability, transparency, diligence and initiative.

Collaborative Change Management Process

NCIIPC transformation for organizations - 1

3 Principles of the Change Management Process

1. Framing and Scaffolding

Framing involves discovery processes that create a common understanding of issues and scope of required changes. Scaffolding involves transformational processes where the actors are supported throughout their journey by the use of tools that help in comprehension, decision making and execution. Both framing and Scaffolding are taken together as foundational viewpoints to successfully enable an adoption of NCIIPC guidelines and controls.

2. Participation and Collaboration

A Participatory approach recognizes that the cybersecurity practices require an inclusive view of all the stakeholders in the organization. These various actors have to work cooperatively and collaborate on important issues to improve the cybersecurity posture. Both participation and collaboration are important constructs that enable the adoption of NCIIPC guidelines and controls, and improving the cybersecurity posture of organizations.

3. Charting Pathways for cybersecurity improvement

In many cases, based on extensive discussions with auditors, it is found that organizational actors may not be able to comprehend what is required for improvement. They may know what needs to be improved but may not comprehend how to get there. Therefore what is required is a pathway that organizational actors can use to craft their own journey towards improvement. The need to support self-efficacy through providing pathways is the foundational basis of this workbook.

Creating a collaborative change management process

1. Stakeholder Selection

The key challenge in any change management process is to get in the right set of people who are representative of the various stakeholder groups. These stakeholder groups would ideally span a spectrum of the operators to the higher management, such as the CISO, as well as display proper demographic variety.

In order for maximum benefit to be achieved, organizers could use the 5Is as a choice criterion:

- **Informed:** Are the representative members informed about the issues and the context?
- **Impacted:** Are they sufficiently impacted by the issues in cybersecurity? Are they vulnerable to the consequences of the cybersecurity improvement process?
- **Interested:** Are these members sufficiently interested in the change process?
- **Invested:** Are they personally involved and invested in the outcomes of the process?
- **Implementers:** Can they be given the responsibility of implementing the change? Will they show sufficient accountability and diligence in executing part or whole of the process?

Collaborative Change Management Process

NCIIPC transformation for organizations - 2

2. Collaboration Sessions

Collaborative sessions should be organized on a weekly basis. In cases of extreme urgency, such as that of immediate self assessment, they can also be organized a series of session spread over a week. In these sessions, all the participants will meet regularly and use the tools of the workbook to perform a self assessment, map out the possible change pathways and resources required for improvement in the cybersecurity posture. All members should be allowed to participate inclusively with proper value given to their insights. Each session can be moderated by its members on a rotational basis. These sessions should inform, elicit, and act on vital information with a view towards benefits to the whole organization in the short- and long-term. In summary, the aim is to self-assess and create pathways for improvement

3. Implementation Sessions

Implementation sessions are similar to collaborative sessions in its structure. However, they differ in terms of their functions. Unlike the collaborative session, where the aim is to identify and create pathways, the implementation sessions ensure that the insights identified in the collaboration sessions will be implemented in specific timeframes by responsible people adhering to a timeline, while ensuring the highlighting of the completion status, once the change is implemented.

4 Phases of the change management process

The entire workbook is divided into 4 phases that demonstrate the phases of the change management process:

Phase 1: Comprehending

In this phase the key idea is to self assess and comprehend the essential status of the organization. this is possible by using the templates and scoring mechanism provided in the scorecard to generate an Risk Priority (RP) score.

Phase 2: Sensemaking

In this second phase, the domains and respective controls are highlighted and their improvement areas are listed. These improvement areas serve as the basis for the subsequent steps.

Phase 3: Reformulating

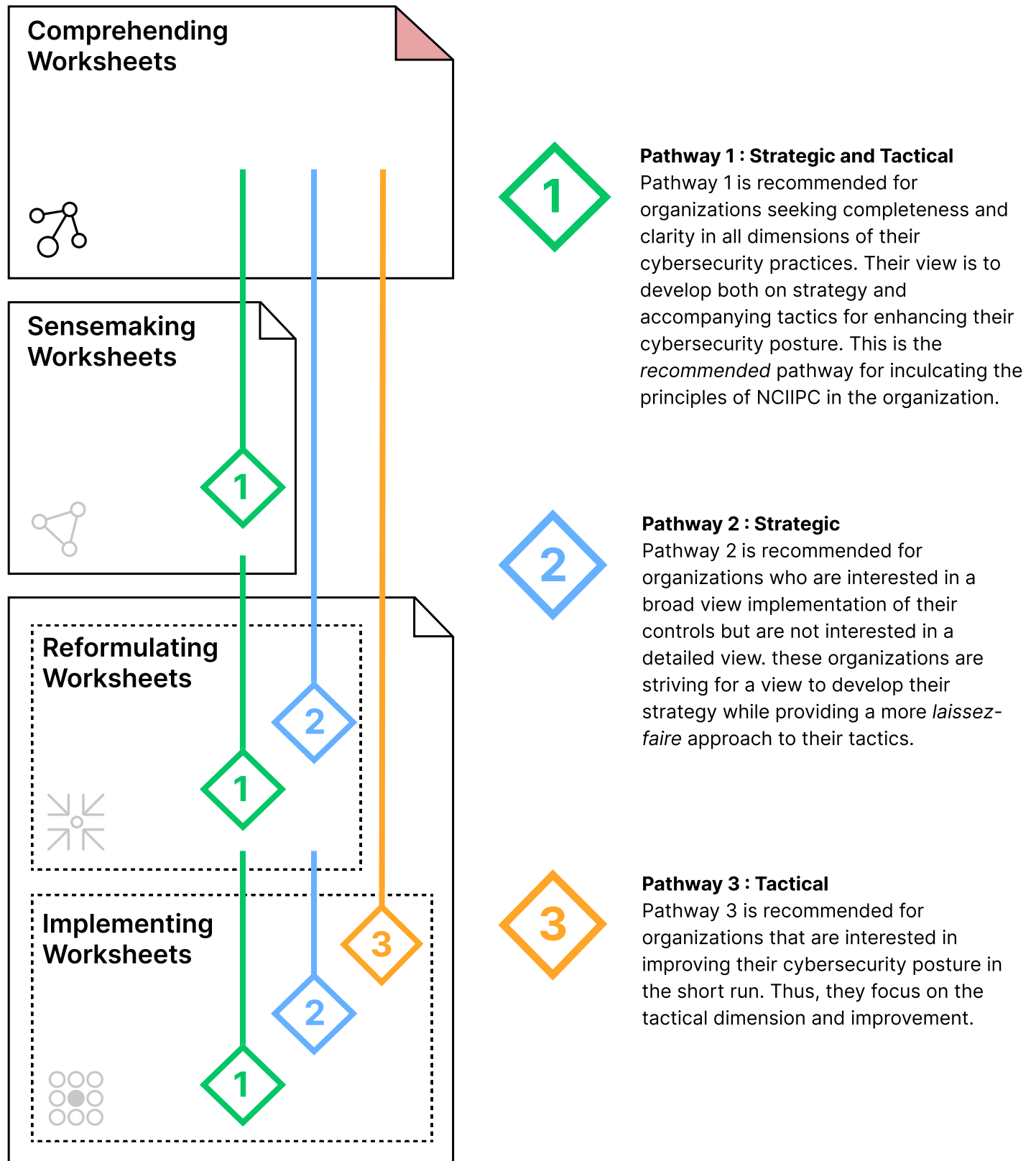
In this third phase, improvement pathways are created by delving into particular domains and controls in multiple ways. These can be made possible by the use of templates that provide clarity and insight into the particular areas.

Phase 4: Implementing

Finally, once the domains and controls have been identified, a timeline is charted and an implementation schedule set in place along with the assignment of responsibility and the date of completion. This enables, the implementation of a set of improvements which were identified in the first phase, detailed in the second phase, devised into detailed course of action in the third phase and finally implemented in the last phase.

Collaborative Change Management Process

NCIIPC transformation for organizations - 3a



Collaborative Change Management Process

NCIIPC transformation for organizations - 3b



Pathway 1: Strategic and Tactical

An organization that strives for completeness and clarity should follow this pathway.

Comprehending

This pathway begins with the filling of the scoresheet. These scoresheet provide an insight into the domain and associated controls.

Sensemaking

Stakeholders then move to the checklist of controls and complete this checklist in further detail. This detailed checklist filling provides a detailed understanding of the control limitations as well as areas that can be improved to enhance the cybersecurity posture.

Reformulating

The next step involves acting on the data produced from the exercise on the controls. In this third step, the stakeholders complete the sensemaking worksheets and try to grasp the future possibilities as well as areas for improvement in a strategic manner.

Implementing

Finally, based on insights of the sensemaking worksheets, the implementation is charted in greater detail.



Pathway 2: Strategic

An organization that strives for a broader granular view for the controls, yet wants to invest significant resources on a strategic outlook towards improving their cybersecurity posture.

Comprehending

This pathway begins with the scoresheet evaluation to gauge the current posture.

Reformulating

The next step involves acting on the data produced from the exercise on the controls. In this third step, the stakeholders complete the sensemaking worksheets and try to grasp the future possibilities as well as areas for improvement in a strategic manner.

Implementing

Finally, based on insights of the sensemaking worksheets, the implementation is charted in greater detail.



Pathway 3: Tactical

This pathway is best suited for organizations that focus on rapid implementation of the improvements in the controls for remedies in the short-run

Comprehending

This pathway begins with the filling of the scoresheet.

Implementing

Based on the insights of the scorecard details, the RP values are used to identify the timeline of the implementation. Next, the implementation is charted.

NCIIPC

A Brief Introduction - 1

About NCIIPC

The National Critical Information Infrastructure Protection Centre (NCIIPC) was established under Section 70A of the Information Technology (IT) Act, 2000 (amended in 2008). It was created as nodal body to protect critical information infrastructure (CII) against malicious cyber attacks. The National Technical Research Organization (NTRO) launched NCIIPC on January 2014 to safeguard India's critical information infrastructure assets. NCIIPC appeared as a strategic answer to India's increasing digital infrastructure dependence. The growing global threats to CII made NCIIPC essential to create a dedicated organization focused on cybersecurity protection.

NCIIPC was established to defend and secure operational assets and networks that serve vital national security, economic stability, public health, and essential service functions of India. Managing the threats of operational technologies involves moving beyond “information technology” and comprehensively taking into account the threat landscape of technology in general. As such, dealing with threats in the area of operational technology merits attention at par with Financial or Operational Risk Management.

NCIIPC guidelines identify CII as essential assets and networks whose disruption would severely harm vital national infrastructures.

The scope of NCIIPC extends across seven critical sectors:

- **Energy:** Safety measures defend critical energy assets like power grids, oil and gas delivery systems.
- **Banking, Financial Services, and Insurance (BFSI):** The sector needs protection for its financial systems and payment network infrastructure.
- **Telecommunications:** Our operations safeguard communication networks as well as the technologies connected to them.
- **Transport:** Our system defends digital assets across all transportation sectors including trains, planes, ships, and roads.
- **Government:** IT systems and public-service data need top-level security to function properly.
- **Strategic and Public Enterprises:** The nation protects sectors that manufacture defense hardware and space technology and control sensitive industrial operations.
- **Healthcare:** The public health system and medicine transportation routes need stronger backup measures and better protections.

As the threat landscape continues to evolve in large part because of growing digital interconnectivity and ever-more-sophisticated attack vectors technical safeguards need to be amplified by an organizational culture backed up by human involvement, accountability and collaboration. Besides being consistent with NCIIPC's general mission, this all-encompassing human-centric strategy might also ensure that any framework that it promotes would be sufficiently robust and flexible, and one that is structured for long-term effectiveness against continuously evolving cyberthreats.

NCIIPC

A Brief Introduction - 2

NCIIPC Controls and Compliance

Compliance frameworks are a set of structured guidelines, controls and practices that help organization in maintaining their cybersecurity practices with respect to regulatory, Industry, legal and business standards. They provide a systematic approach to navigating requirements and integrating them with the broader organizational goals. These frameworks have been created for both Informational Technology (e.g. NIST Cybersecurity Framework (CSF) 2.0, ISO 27001:2022, etc.) and Operational Technology (e.g. IEC62443, NIST 800 series, etc.).

In India NCIIPC is an Operational Technology compliance framework. NCIIPC has categorized thirty five controls as 5 control groups: planning controls (12 controls), implementation controls (6 controls), operational controls (11 controls), disaster recovery/ business (3 controls), reporting and accountability (3 controls). These controls are categorized based on their functional impact in the development/ deployment/operationalization cycle. While each control may not be required in all cases, it is expected that all CII would take a judicious decision regarding the applicability in terms of minimizing risk. The lack of compliance with the NCIIPC controls identify the areas of improvement for any organization.

As NCIIPC has to cover all aspects of cybersecurity for CII, the guidelines needs to be thorough, while understanding the detailed functioning of CII. Further, an additional consideration is that Compliance frameworks in general and also in the particular case of NCIIPC, can be further supplemented through an understanding of functional domains of Capability Maturity Models. This would enable the NCIIPC guidelines to providing a holistic coverage based on categories that are vital to the understanding and maturity in the functioning of organizations.

NCIIPC and Domains of CSCMM

Capability Maturity Models (CMMs) provide a standardized way to assess an organization's cybersecurity posture, identify capability gaps, and guide improvements in a structured and progressive manner. Over time, multiple cybersecurity maturity models have emerged to address sectoral, organizational, and national security requirements.

In the Indian context, the National Critical Information Infrastructure Protection Centre (NCIIPC) introduced the Cyber Security Capability Maturity Model (CSCMM) to enable a structured assessment of cybersecurity capabilities, particularly for critical information infrastructure organizations. CSCMM follows a maturity-based approach to evaluating how effectively cybersecurity practices are defined, implemented, managed, and continuously improved across an organization. The model supports progression from foundational security practices toward more mature, systematic, and resilient cybersecurity capabilities.

CSCMM adopts a domain based approach by organizing cybersecurity practices into distinct domains, allowing organizations to systematically evaluate their strengths and weaknesses and to plan targeted capability improvements. This domain-oriented structure also supports consistency across assessments and alignment with regulatory and compliance expectations.

Within CSCMM, cybersecurity capabilities are grouped across domains such as Governance, Risk Management, Asset Management and etc. Collectively, these domains address the critical dimensions of cybersecurity required to build and sustain organizational resilience.

In the current workbook, these fifteen categories are used as the starting point for analyzing cybersecurity domains and examining their alignment with the controls proposed by relevant compliance and regulatory frameworks.

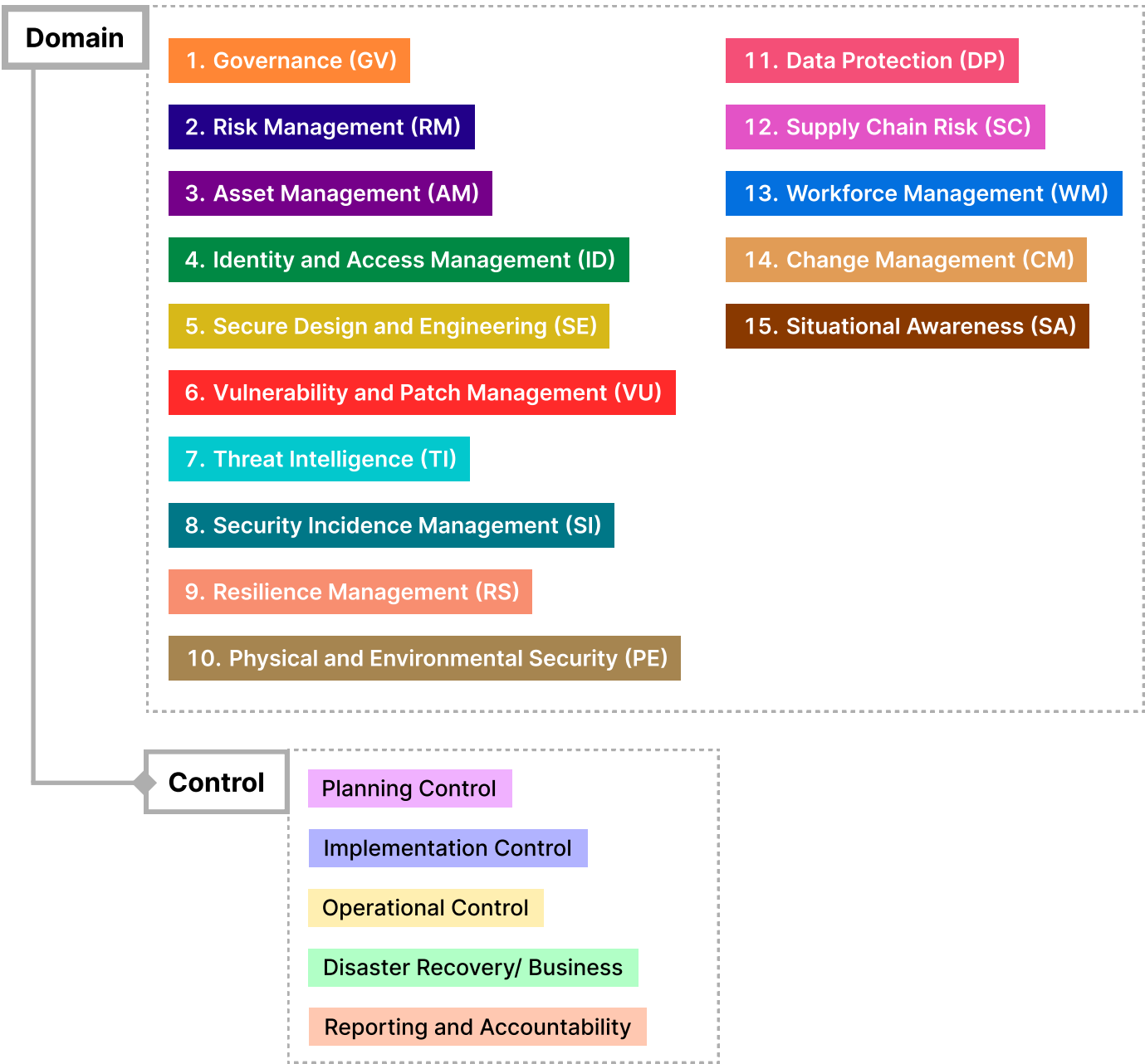
NCIIPC

A Brief Introduction - 3

Domains and Controls as an assessment matrix for NCIIPC compliance

The above subsections have listed the role of domains and controls as the basis for comprehending any sector. Any sectoral cybersecurity practices involves comprehending the organization in terms of its maturity of its capability. One manner of addressing the capability is to understand it in terms of two major dimensions of domains and controls. The domains refer to those categories that organizations employ to understand its functional cyber security practices. At the same time, the controls refer to categories used to for characterizing the development/ deployment/operationalization cycles in organizations.

Taken together domains and controls provide us a functional matrix that provides us the an insight into comprehending the organization in terms of its maturity of cyber security practices.



Domains and Controls

Quick Reference Sheet - 1

What is a Domain?

Cybersecurity practices are often grouped under a category identified as a Domain. A domain represents a collection of practices within a specific subject area such as risk management, identity and access management, or incident response that an organization employs to strengthen its overall cybersecurity posture. While many international frameworks define their own sets of cybersecurity domains, domains are not explicitly used to classify controls within NCIIPC. Therefore, based on an extensive study of widely accepted international classifications, 15 domains are used for the categorization and sensemaking of organizational cybersecurity maturity in this model

1. Governance (GV)

The organization should maintain a board-endorsed cybersecurity governance framework aligned with strategic objectives, ensuring effective oversight of policy, risk management, program execution, and legal and regulatory compliance across the business.

2. Risk Management (RM)

The organization should implement a continuous, standards-aligned risk management process to identify, assess, and mitigate risks to critical service assets, ensuring confidentiality, integrity, availability, safety, and compliance with enterprise, legal, and regulatory requirements.

3. Asset Management (AM)

The organization should maintain a defined and approved asset management process covering the full asset lifecycle, with an accurate inventory and controlled configuration baselines to ensure the security, integrity, and availability of all IT and OT assets.

4. Identity and Access Management (ID)

The organization should enforce strong identity and access management (IAM) practices to ensure only authenticated and authorized users or devices have access, supported by controlled provisioning, periodic reviews, and timely revocation to prevent unauthorized access.

5. Secure Design and Engineering (SE)

The organization should ensure that secure design and engineering practices are aligned with enterprise architecture and industry best practices, and are embedded into planning and change processes to deliver resilient, cost-effective systems capable of detecting, resisting, responding to, and recovering from cyber threats.

6. Vulnerability and Patch Management (VU)

The organization should maintain a defined and approved vulnerability and patch management process to systematically identify, assess, and remediate security weaknesses across IT assets, reducing the attack surface and minimizing the likelihood and impact of exploitation.

7. Threat Intelligence (TI)

The organization should maintain a formally approved threat intelligence management process that uses credible sources to deliver timely, actionable insights, informing risk understanding and guiding proactive measures to strengthen the cybersecurity posture.

Domains and Controls

Quick Reference Sheet - 2

8. Security Incident Management (SI)

The organization should maintain a clearly defined and approved incident response process covering detection through post-incident review, with the capability to analyze logs, detect anomalies, and respond promptly to incidents affecting critical assets and infrastructure.

9. Resilience Management (RS)

The organization should ensure cyber resilience by maintaining tested and documented backup, incident response, and disaster recovery processes that protect data integrity and availability, enabling rapid detection, response, and recovery with minimal impact on business continuity.

10. Physical and Environmental Security (PE)

The organization should ensure integrated physical, health, safety, and environmental security controls are in place, supported by risk assessments and incident response mechanisms that protect critical systems, safeguard personnel and the environment, and enhance overall operational resilience.

11. Data Protection (DP)

The organization should ensure effective data protection controls to safeguard sensitive data, including PII, in compliance with the Digital Personal Data Protection Act and privacy principles, while maintaining confidentiality, integrity, and availability across the data lifecycle.

12. Supply Chain Risk (SC)

The organization should implement a well-defined supply chain risk management framework to identify, assess, and mitigate cyber risks from third parties, ensuring continuity through clear accountability, appropriate security controls, and continuous monitoring of outsourced systems and ICT assets.

13. Workforce Management (WM)

The organization should maintain a capable and well-structured cybersecurity workforce with clearly defined roles, appropriate skills and training, regular performance evaluation, and ongoing awareness programs to effectively safeguard organizational assets.

14. Change Management (CM)

The organization should maintain a clearly defined and approved change management process to control and monitor changes to cyber assets, ensuring stakeholder authorization, compliance, and effectiveness while preserving service reliability and scalability.

15. Situational Awareness (SA)

The organization should maintain a well-defined and implemented situational awareness process to continuously monitor, detect, and analyze cyber threats, integrated with incident management to support timely response and informed decision-making.

Domains and Controls

Quick Reference Sheet - 3

What is a Control?

NCIIPC has categorized thirty five controls based on their functional impact in the development/ deployment/ operationalization cycle. While each control may not be required per se, it is expected that all CII would take a conscious decision regarding the applicability or otherwise of every control as a conscious process of minimizing risk. In this contest, it is imperative that CII security move out of the realm of “IT” or “Cyber Security”, and into a threat meriting Board level attention at par with Financial or Operational Risk Management.

Planning Control

PC1 PC2 PC3 PC4 PC5 PC6 PC7 PC8 PC9 PC10 PC11 PC12

These set of controls are required to be assessed at the conceptualization and design stage to ensure that security is taken as a key design parameter for all new CII.

Implementation Control

IC1 IC2 IC3 IC4 IC5 IC6

These controls are required for translating the design/conceptualisation planning so as to ensure adequate and accurate translation of the security designs into actual system security configurations. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.

Operational Control

OC1 OC2 OC3 OC4 OC5 OC6 OC7 OC8 OC9 OC10 OC11

To ensure that security postures are maintained in the operational environment. These controls also come into play in case of retrofitting existing, unprotected/poorly protected CII.

Disaster Recovery/ Business

DR1 DR2 DR3

These controls are essential to ensure minimum downtime, as well as to ensure that the restoration process factors in, and overcomes the initial vulnerabilities, or alternatively isolates infrastructure compromised by attackers, to ensure graceful degradation / minimum maintenance of Service provided by the CII.

Reporting and Accountability

RA1 RA2 RA3

These controls ensure that adequate accountability and oversight is exercised by Senior management, as well as reposting to concerned Government agencies where required. This family of Controls also includes compliance controls.

Domains and Controls

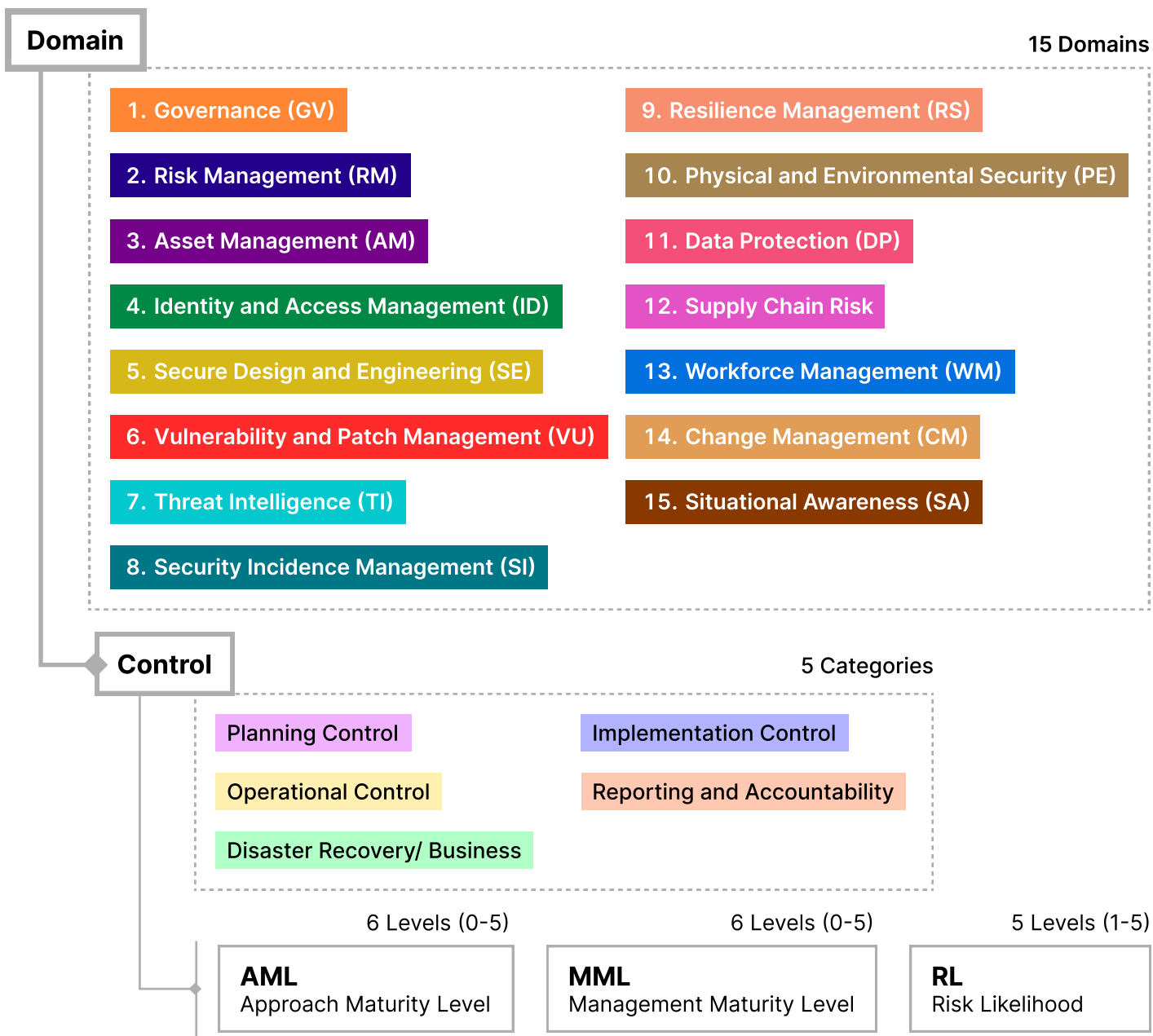
Quick Reference Sheet - 4

Domain	Control										
1. Governance (GV)	PC1	PC2	PC3	PC4	PC10	PC11	IC1	RA1	RA2	RA3	
2. Risk Management (RM)	PC1	PC2	PC6	PC8	OC4	OC5	DR1	RA2	RA3		
3. Asset Management (AM)							PC1	IC1	OC6	OC9	
4. Identity and Access Management (ID)								IC2	IC3	OC10	
5. Secure Design and Engineering (SE)		PC5	PC7	PC8	PC9	IC4	IC6	OC7	OC8	DR3	
6. Vulnerability and Patch Management (VU)						PC6	IC6	OC5	OC7	RA2	
7. Threat Intelligence (TI)								PC2	OC11	RA1	
8. Security Incidence Management (SI)								PC3	OC2	OC11	
9. Resilience Management (RS)			PC2	PC8	PC12	IC5	OC2	DR1	DR2	DR3	
10. Physical and Environmental Security (PE)									PC12	IC5	
11. Data Protection (DP)								OC1	OC4	OC8	OC9
12. Supply Chain Risk (SC)								PC10	IC6	OC8	
13. Workforce Management (WM)								PC3	PC11	OC3	
14. Change Management (CM)								PC5	PC7	PC9	DR3
15. Situational Awareness (SA)						PC2	OC2	OC11	RA1	RA2	

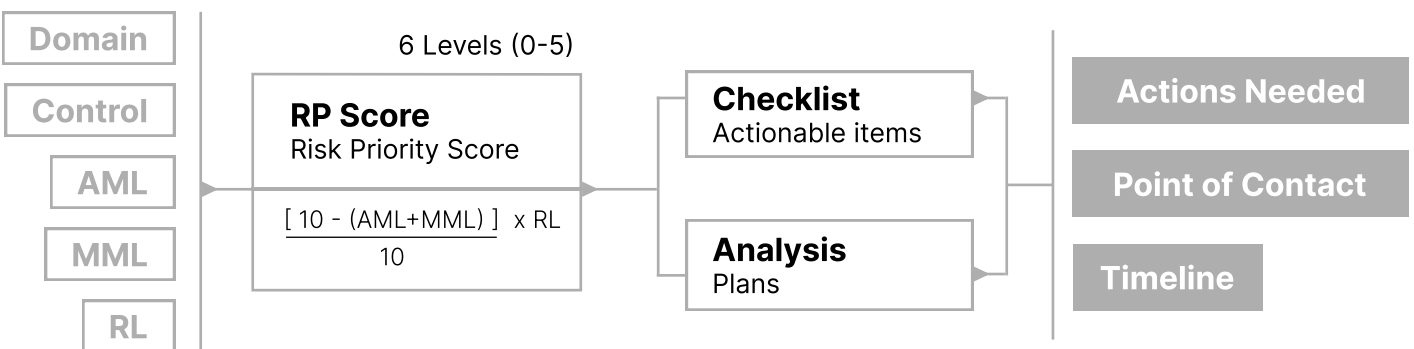
Domains, Controls and Risk Priority Score

Overview

Framework Architecture



Framework Usage



Perceived Risk Priority Score (RP)

Methods and Measures - 1

Purpose of the Formula

The Perceived Risk Priority formula is intended as a structured means for participants to express and compare their perceived exposure to risk within their organizational contexts. The resulting score is not designed to gauge an objective probability or a formal quantitative measure of risk. Rather, it functions as a relative, self-assessed indicator that enables organizations to situate risks on a common evaluative scale. This orientation is consistent with general risk-management guidance such as ISO 31000, which emphasizes systematic and repeatable assessment processes while deliberately allowing for a mix of qualitative and quantitative tools depending on organizational context. The standard does not prescribe numerical scoring or a specific computational approach, but it supports structured mechanisms that promote comparability, clarity and informed prioritization.

Conceptual Basis

The conceptual foundation of the formula aligns with widely recognized risk-management framings in which risk is understood as a function of event likelihood and the factors shaping potential consequences. This general formulation is common in professional practice. For example, compliance risk assessments frequently conceptualize risk as the interaction of likelihood and impact. Structured numerical approaches adopt similar logic by combining ordinal assessments of severity, occurrence and detection to produce prioritized scores that are explicitly relative rather than probabilistic. These approaches illustrate how numerical scoring systems can support consistency and comparability across assessments without claiming statistical precision. In the current workbook, the likelihood score (RL) is used to represent participants' perceived inherent risk.

A key premise of the formula is that the perceived maturity of an organization's risk-management approach influences how much risk is believed by participants to remain after considering existing controls. This premise is supported by literature on risk maturity models, which describe maturity as reflecting governance structures, processes, culture and the integration of risk practices. Typically, organizations at higher maturity levels possess more reliable and embedded mechanisms for managing uncertainty. The maturity components used in this study: Approach Maturity Level (AML) and Management Maturity Level (MML) are therefore treated as subjective indicators of process and governance capability.

Structure of the formula

The algebraic structure of the formula draws on residual-risk logic, a well-established concept in risk-management practice in which perceived residual risk is understood as the perceived level of exposure that remains after controls are applied. In simplified form, perceived maturity is normalized by combining AML and MML into a single index:

$$M = (AML + MML) / 10$$

(M= Perceived Maturity, AML= Approach Maturity Level, MML= Management Maturity Level)

The complementary proportion, $1 - M$, represents the perceived exposure remaining after accounting for maturity. Perceived Risk Priority is therefore expressed as $RP = RL \times (1 - M)$

After normalizing this value based on the combined range of AML and MML we arrive at the following formula:

$$\text{perceived* Risk Priority Score (RP)} = \frac{[10 - (AML+MML)]}{10} \times RL$$

****The RP score is based on self perception of an organization and does not seek to quantify control effectiveness or gauge the objective measure of risk.***

Perceived Risk Priority Score (RP)

Methods and Measures - 2

$$\text{Risk Priority Score (RP)} = \frac{[10 - (\text{AML} + \text{MML})] \times \text{RL}}{10}$$

AML = Approach Maturity Level (scale of 0–5)

MML = Management Maturity Level (scale of 0–5)

RL = Perceived Risk Likelihood (scale of 1–5)

Interpreting the Scores

This formulation does not seek to quantify control effectiveness or gauge the objective measure of risk. Instead, it provides an interpretive mechanism that reflects how participants believe maturity should influence their residual exposure, enabling risks to be compared on a levelled and internally consistent basis. The behavior of the formula is structured to be intuitive. The relationship is as follows: When maturity is minimal, perceived Risk Priority equals perceived likelihood, and as maturity increases, Risk Priority decreases proportionally.

Overall, the perceived Risk Priority formula is conceptually grounded in established principles of risk assessment and risk maturity while remaining intentionally simplified. Its formulaic structure reflects assumptions chosen to prioritize transparency, comparability and ease of interpretation rather than empirical calibration. In this sense, the formula functions as a transparent tool for supporting structured reasoning about perceived relationships between likelihood, maturity and residual exposure across varied organizational contexts for enabling self- assessment.

The RP score is relative and should be interpreted only within the context of your organization's own controls. It is a tool to compare across controls, not across organizations. Using RP scores to benchmark against other organizations is discouraged, as the scoring inputs particularly AML and MML are organization-specific and subjective.

***A higher perceived RP score does not mean “more risky” in an absolute sense
- it means “less mature and more exposed” in your organization’s context.***

How does acting on the RP Score support your organization?

- Prioritize actions based on risk-adjusted maturity gaps
- Align cybersecurity requirements with important and highly exploitable weaknesses
- Facilitate focused discussions during internal reviews and leadership briefings
- Track progress over time by observing how RP scores evolve as maturity improves
- Organizations can better understand which planning or implementation controls deserve urgent remediation, helping cybersecurity leaders move from targeted action to broad strategy using the reformulation section

Scoring Criteria for Assessment

Procedures

Scoring

The Risk Priority Score (RP) is designed to help organizations identify which cybersecurity controls require the most immediate attention. It offers a structured way for CISOs and their teams to prioritize planning and implementation efforts by factoring in both maturity levels and risk exposure.

Risk Priority Score (RP)=

[10 - (AML+MML)]

10

x RL

- AML = Approach Maturity Level (scale of 0–5)
- MML = Management Maturity Level (scale of 0–5)
- RL = Perceived Risk Likelihood (scale of 1–5)

Approach Maturity Levels(AML): 0–5 Scale

How to use the Approach Maturity Levels(AML) Scale

AML indicates the completeness, thoroughness, or level of development of an activity in a control. This scale is used to understand the posture of your organization according to the respective aspects of the control. the AML values can be calculated as follows:

1. Understand the control using the control descriptions on each control page
2. Read through the AML Scale of 0 to 5 and identify the level of maturity in terms of approach in your organization in the aspects of the control
3. Input the value into the respective boxes in the Assessment chart of the Domains for further calculations

AML-0 Nonexistent	No activities, processes, or practices exist to address the control. There is no recognition of the need for implementation
AML-1 Initial	The control is applied in an ad-hoc and reactive manner. There is minimal structure, and the focus is on addressing immediate risks without a formalized plan
AML-2 Managed	Basic processes are in place to address the control, but they are informal and inconsistently applied across the organization
AML-3 Defined	The control processes are documented, standardized, and consistently followed across all relevant areas. Repeatability is ensured
AML-4 Measured	The effectiveness of the control is measured and evaluated using metrics. Data is collected to improve processes and refine implementation
AML-5 Optimized	Processes are continuously improved based on feedback, metrics, and evolving best practices. Advanced tools and techniques are leveraged for maximum effectiveness

Management Maturity Levels(MML): 0–5 Scale

How to use the Management Maturity Levels(MML) Scale

MML indicates the extent to which a practice or activity is ingrained in an organization's operations (or institutionalized). The more deeply ingrained an activity, the more likely it is that the organization will continue to perform the practice over time. This scale is used to understand the posture of the organization with respect to controls. The MML values can be calculated as follows:

1. Understand the control using the control descriptions on each Domain section of the workbook
2. Read through the MML Scale of 0 to 5 and identify the level of maturity in terms of approach in your organization in the aspects of the control
3. Input the value into the respective boxes in the Assessment chart of the Domains for further calculations

MML-0 Nonexistent	No management oversight, policies, or governance mechanisms exist for the control. The control is not considered within the organization's risk management framework
MML-1 Initial	Management is minimally involved and provides limited oversight. Support is reactive and often driven by external pressures rather than internal planning
MML-2 Managed	Basic policies and management oversight are in place, but they are informal, inconsistently applied across the organization
MML-3 Defined	Management establishes formal policies, assigns responsibilities, and provides structured oversight to ensure consistent execution of the control
MML-4 Measured	Management actively monitors and evaluates the control's performance. Regular reviews, audits, and metrics are used to assess and guide effectiveness
MML-5 Optimized	Management demonstrates a proactive and strategic approach to the control. Continuous improvement and alignment with organizational objectives are prioritized

Risk Likelihood(RL): 1–5 Scale

How to use the Risk Likelihood(RL) Scale

RL scale identifies risk aspects of each control in various domains(eg: Program Management, Situational Awareness, etc.). The RL can be identified as follows:

Identify the related elements in your organization with respect to the control

Understand and evaluate the likelihood of the risk of the selected control

Assign an RL using the adjacent chart

Input the value into the respective boxes in the Assessment chart of the Domains for further calculations

RL-1	Rare	May occur only in exceptional circumstances
RL-2	Unlikely	Could occur, but probably will not
RL-3	Possible	Might occur at some time
RL-4	Likely	Will probably occur in most circumstances
RL-5	Certain	Is expected to occur in most circumstances

How to use the worksheets

Guide

Domain Assessment

Domain Name

IC5

Description
Physical & Environmental Security and protect facilities, equipment, and media from natural, environmental, and human threats.

Context
Protect facilities and critical equipment against unauthorized physical access, environmental hazards, and power anomalies. Implement layered site controls (guards, CCTV, biometrics), fire detection/suppression, redundant HVAC and UPS systems, and secure storage for sensitive media. Physical breaches can neutralize even the strongest cyber protections in seconds.

AML
Documented procedures require a mandatory physical security checklist to be completed during facility deployment, ensuring the presence and operational readiness of all basic controls.

MML
Check for a documented physical security plan, access logs, surveillance retention, environmental redundancies, and periodic drills with management review.

RL
Consider the risk that physical intrusion or environmental failure could disrupt or destroy CII assets.

2

4

3

This is because...

OC5

Description
Penetration Testing and proactively test CII defenses to uncover exploitable weaknesses.

Context
Conduct regular risk-based pentests covering IT, OT, and social engineering to uncover exploitable weaknesses before adversaries do. Third-party testers must follow strict scope and non-disruption clauses. Findings feed a remediation plan that is re-verified through re-testing.

AML
Determine if at least annual vulnerability scans or ad-hoc pentests are performed.

MML
Confirm scope is risk-based, findings tracked to closure, and re-tests verify remediation.

RL
Gauge risk that untested vulnerabilities will be exploited before discovery.

4

2

3

This is because...

Notes / Justification

Assess: Control and Identity management

1 First step is to fill the Domain Assessment page. In this page, you will be scoring the identified controls under the domain based on the AML, MML and RL scoring.

These sections display the identified Control (IC5, OC5) and its contextual description based on the Domain. This includes the Description (what the control is), the Context (why it matters to CII), and the Scoring Criteria (the core metrics, AML, MML, RL). The color strip determines which Control Group it belongs to (e.g., Planning, Implementation, Operational).

This is where you will input your scores. Score each control based on Approach Maturity Level (AML), Management Maturity Level (MML), and Risk Likelihood (RL). These scores are obtained from the scoring rubric available in the accompanying Guide (Pages 16 and 17). Score these with respect to your understanding/team's understanding. You can also write Notes/Justification for understanding the context of the scoring.

Domain Scorecard

Domain Name

Scorecard

1. This is a summary assessment page.
2. The formulae given below would be used to calculate the Risk Priority(RP) Score using the values from the Assessment page.
3. Place the RP score for each predefined controls in this page.
4. Assessment page.
5. Place the RP score for each predefined controls in this page.

Risk Priority(RP) = $\frac{[10 - (AML + MML)]}{10} \times RL$

Lower the score, lower the priority
Higher the score, higher the priority

RP	Average RP	Action needed	Point of Contact	Timeline
PC1	2.1	Action Task	Abhijeet	2 weeks
PC3	1.6			
PC6	4			
PC7	3.7			

IC5

OC5

Notes

Assess: Control and Identity management

2 Second step is to fill the Domain Scorecard page. Calculate the RP score using formula and fill the table with respective information

This is the formula to calculate the RP scores for individual controls. The values of the Approach Maturity Level (AML), Management Maturity Level (MML) and Risk Likelihood (RL) should be taken from the Assessment page of the respective Domains and calculate.

This is the section that will have the RP scores for all the controls and the associated Average RP scores for the Control groups. Use the Notes section in the page to calculate the scores and write it here.

Based on the RP scores, assign the immediate actions needed, POC and a timeline to achieve the outcome. (Heuristic for RP score: Higher the RP score, Higher the priority and vice versa). A detailed method for analysis on what factors to consider or how to take actions are mentioned later in the workbook. Refer to the next page to get more detailed understanding.

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Governance (Phase 2).

1 Governance

1 Governance

Worksheet Assessment

PC1	Description Identification and categorization of Critical Information Infrastructure (CII) based on functionality, criticality, dependencies, sensitivity, and potential impact. Context Correct identification of CII ensures cybersecurity, resilience, and response efforts focus on assets whose failure would cause significant organizational or national impact.	AML CII assets are identified and categorized using documented, organization-wide criteria covering criticality, dependencies, sensitivity, and impact, and the process is applied consistently.	
		MML Management reviews, approves, and assigns accountability for CII classification and ensures periodic validation.	
		RL Misclassification significantly increases likelihood of severe operational disruption and cascading failures affecting critical services.	
		Notes / Justification	
PC2	Description Identification and management of interdependencies between Critical Information Infrastructure, internal systems, external organizations, and supporting services. Context Unmanaged interdependencies can amplify cyber incidents and trigger cascading failures across multiple critical services and stakeholders.	AML Interdependencies between critical systems, suppliers, and external services are identified, documented, and maintained using a structured and repeatable approach.	
		MML Management oversees dependency analysis, assigns ownership, and ensures interdependencies are considered in governance, risk, and resilience decisions.	
		RL Poorly managed interdependencies increase likelihood of cascading failures, prolonged outages, and loss of critical services.	
		Notes / Justification	
PC3	Description Establishment of an Information Security Department (ISD) structure with clearly defined roles, responsibilities, authorities, and reporting lines. Context A clearly defined ISD structure enables accountability, coordinated decision-making, and effective execution of cybersecurity responsibilities across the organization.	AML Information security roles, responsibilities, authorities, and reporting lines are formally defined, documented, and communicated across relevant functions.	
		MML Management approves the ISD structure, assigns authority, and periodically reviews role effectiveness and coverage.	
		RL Weak or unclear ISD structure increases likelihood of accountability gaps and ineffective security response during incidents.	
		Notes / Justification	

1 Governance

Worksheet Assessment

PC4	Description Establishment and maintenance of an information security policy defining organizational intent, objectives, principles, and high-level rules for protecting information and critical systems. Context The security policy provides formal direction from leadership and ensures consistent security practices aligned with organizational objectives, risk posture, and regulatory expectations.	AML A documented information security policy exists, is approved, communicated organization-wide, and defines objectives, scope, and expectations for protecting information and critical systems. MML Management reviews, updates, approves, and enforces the policy periodically to ensure alignment with business objectives, risk posture and regulatory obligations RL Weak or outdated policy increases likelihood of inconsistent security practices, control gaps, non-compliance, and ineffective incident response. Notes / Justification	
PC10	Description Governance of cybersecurity risks arising from third-party vendors, suppliers, service providers, and outsourced operations supporting critical services. Context Supply chain weaknesses can introduce significant cyber risk and allow indirect compromise of critical systems through third-party dependencies.	AML Supply chain security requirements are defined, documented, and applied to relevant third parties, including vendors, service providers, & outsourced operations across the supplier lifecycle. MML Management oversees supplier risk assessments, approves assurance requirements, monitors compliance, reviews third-party performance impacting critical services, & remediation actions. RL Weak supply chain governance increases likelihood of third-party compromise, service disruption, and indirect attacks on critical infrastructure. Notes / Justification	
PC11	Description Oversight of cybersecurity certifications, regulatory obligations, and compliance with applicable standards, mandates, and legal requirements. Context Effective certification and compliance oversight provides assurance to regulators, stakeholders, and national authorities regarding cybersecurity posture and accountability.	AML Applicable cybersecurity certification & compliance requirements are identified, documented, tracked, & mapped to organizational obligations, applicable laws, & regulatory expectations. MML Management monitors compliance status, reviews audit results, ensures corrective actions, & reports overall compliance posture to leadership and timely remediation. RL Poor compliance oversight increases likelihood of regulatory violations, penalties, reputational damage, & loss of stakeholder trust & confidence. Notes / Justification	

1 Governance

Worksheet Assessment

IC1	Description Assignment of ownership and accountability for Critical Information Infrastructure assets to ensure responsibility for protection, maintenance, and security decision-making. Context Clear asset ownership ensures accountability for safeguarding critical systems and prevents gaps in security responsibility caused by unclear or shared ownership.	AML Ownership for all critical assets is formally defined, documented, and communicated across relevant organizational units and supporting functions.	
		MML Management assigns accountable asset owners, reviews ownership effectiveness periodically, and ensures responsibilities align with governance and risk management processes.	
		RL Unclear asset ownership increases likelihood of unmanaged risks, delayed decisions, and ineffective response to security incidents.	
		Notes / Justification	
RA1	Description Establishment of mechanisms to report cybersecurity incidents, compliance status, and mandated information to government and regulatory authorities. Context Timely and accurate reporting supports national situational awareness and enables coordinated response to cyber incidents affecting critical infrastructure.	AML Regulatory and government reporting requirements are identified, documented, and supported through defined reporting procedures and communication channels.	
		MML Management reviews reporting accuracy, timeliness, approvals, and compliance with mandated national and sectoral obligations.	
		RL Failure to report accurately increases likelihood of regulatory action, national response gaps, and delayed mitigation of widespread cyber incidents.	
		Notes / Justification	
RA2	Description Conduct of internal or external audits and assurance activities to evaluate cybersecurity control effectiveness and compliance obligations. Context Audits provide independent visibility into security posture, identify weaknesses, and support continuous improvement of governance and controls.	AML Audits are conducted using defined criteria to assess cybersecurity controls, governance practices, and compliance requirements across the organization.	
		MML Management reviews audit findings, prioritizes issues, assigns corrective actions, and tracks remediation progress to closure.	
		RL Absence of effective audits increases likelihood of undetected weaknesses, accumulated risk, and systemic security failures.	
		Notes / Justification	

RA3	Description Enforcement of cybersecurity compliance requirements and implementation of corrective actions to address identified non-compliances. Context Effective enforcement ensures that security requirements are followed consistently and deficiencies are corrected before escalating into incidents or regulatory breaches.	AML Non-compliances are identified, recorded, analyzed, and corrective actions are defined, implemented, and tracked within agreed timelines.	
		MML Management enforces compliance requirements, monitors corrective action progress, verifies effectiveness, and ensures lessons learned are applied organization-wide.	
		RL Weak enforcement increases likelihood of repeated violations, escalating cyber risk, regulatory penalties, and erosion of organizational security discipline.	
		Notes / Justification	

1 Governance

Worksheet Scorecard

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
 - The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP score of each Control Group in a domain for Reformulating Worksheet 1
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

$$\text{Risk Priority(RP)} = \frac{[10 - (\text{AML} + \text{MML})]}{10} \times \text{RL}$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC1					
PC2					
PC3					
PC4					
PC10					
PC11					
IC1					
RA1					
RA2					
RA3					

Governance

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Risk Management checklist (Phase 2).

2 Risk Management

PC1	Description Identification and assessment of cybersecurity risks affecting Critical Information Infrastructure (CII) based on impact, likelihood, and dependencies. Context Effective risk identification and assessment ensure that threats to critical systems are understood, prioritized, and managed before they result in significant disruption.	AML Risks to critical information infrastructure are identified and documented using defined criteria based on impact, likelihood, and dependencies across systems and supporting environments.	
		MML Management reviews risk assessments, approves risk ratings, assigns owners, and ensures integration with enterprise risk governance and periodic reporting.	
		RL Unmanaged risks increase likelihood of incidents causing severe operational disruption and national impact to essential services.	
		Notes / Justification	
PC2	Description Assessment and management of risks arising from interdependencies between critical systems, external services, and shared infrastructure. Context Interdependency-related risks can amplify incidents and cause cascading failures across multiple critical services if not properly assessed and managed.	AML Risk assessments consider interdependencies between critical systems, external services, and shared infrastructure during analysis to capture cascading impact scenarios.	
		MML Management ensures dependency-related risks are reviewed, prioritized, and addressed within risk treatment planning and governance oversight processes.	
		RL Unrecognized dependencies are likely to cause cascading failures, extended outages, and amplified impact across multiple critical services during cyber incidents and disruptions.	
		Notes / Justification	
PC6	Description Identification and assessment of cybersecurity risks arising from vulnerabilities and threats affecting systems, applications, and infrastructure. Context Understanding vulnerability and threat-related risks enables proactive mitigation and reduces the likelihood of exploitation impacting critical operations.	AML Vulnerabilities and threats are identified, analyzed, and documented as part of structured risk assessment activities covering systems, applications, infrastructure, and enterprise-wide scope.	
		MML Management reviews vulnerability and threat risks, prioritizes remediation, and allocates resources based on risk severity and business impact.	
		RL Unaddressed vulnerabilities significantly increase likelihood of exploitation leading to service disruption, data compromise, and operational impact across critical environments.	
		Notes / Justification	

PC8	Description Implementation of redundancy measures to mitigate risks affecting availability and continuity of Critical Information Infrastructure. Context Redundancy reduces the likelihood of single points of failure and supports continuity of critical services during cyber incidents or operational disruptions.	AML Redundancy requirements for critical systems are identified, documented, and implemented based on risk assessment outcomes and availability needs.	
		MML Management approves redundancy strategies, reviews effectiveness periodically, and ensures alignment with continuity and resilience objectives.	
		RL Absence of redundancy significantly increases likelihood of service outages and prolonged disruption during failures or cyber incidents.	
		Notes / Justification	
OC4	Description Identification and management of risks related to loss, leakage, or unauthorized disclosure of sensitive or critical data. Context Data loss can result in operational disruption, regulatory penalties, reputational damage, and national security concerns for critical services.	AML Risks related to data loss and leakage are identified, assessed, and documented across systems handling sensitive or critical information.	
		MML Management reviews data loss risks, approves mitigation measures, and monitors effectiveness through periodic assessments and reporting.	
		RL Unmanaged data loss risks increase likelihood of regulatory violations, reputational harm, and compromise of critical operations.	
		Notes / Justification	
OC5	Description Assessment of cybersecurity risks through penetration testing to identify exploitable weaknesses in systems and infrastructure. Context Penetration testing provides insight into real-world exploitability of vulnerabilities, enabling informed risk prioritization and remediation.	AML Penetration testing is conducted periodically to identify exploitable vulnerabilities and document associated risk exposure across critical systems.	
		MML Management reviews test results, prioritizes remediation actions, and tracks closure of identified risks.	
		RL Absence of penetration testing increases likelihood of unknown vulnerabilities being exploited, leading to significant security incidents.	
		Notes / Justification	

DR1	Description Identification and management of risks related to inadequate contingency planning for disruption of Critical Information Infrastructure Context Lack of effective contingency planning can amplify the impact of cyber incidents, system failures, or external disruptions on critical services.	AML Risks related to contingency planning gaps are identified, assessed, and documented for critical systems and supporting processes.	
		MML Management reviews contingency risks, approves mitigation strategies, and ensures alignment with business continuity and resilience planning.	
		RL Weak contingency planning significantly increases likelihood of prolonged outages, ineffective response, and failure to restore critical services.	
		Notes / Justification	
RA2	Description Identification of cybersecurity risks through internal and external audit findings and assurance activities. Context Audits provide structured insight into control weaknesses, process gaps, and systemic risks that may not be visible through routine operations.	AML Audit findings are analyzed to identify cybersecurity risks and document potential control weaknesses affecting critical systems.	
		MML Management reviews audit-identified risks, prioritizes remediation, and integrates findings into enterprise risk management processes.	
		RL Failure to address audit-identified risks increases likelihood of repeated weaknesses and escalating security incidents.	
		Notes / Justification	
RA3	Description Reduction of cybersecurity risks through compliance with applicable laws, regulations, standards, and mandatory requirements. Context Compliance failures can expose organizations to legal penalties, operational disruption, and increased cyber risk.	AML Compliance-related risks are identified, assessed, and documented based on applicable regulatory and legal requirements.	
		MML Management monitors compliance risks, approves mitigation actions, and ensures ongoing adherence through oversight mechanisms.	
		RL Non-compliance significantly increases likelihood of regulatory penalties, operational disruption, and heightened cybersecurity exposure.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
 - The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

$$\text{Risk Priority(RP)} = \frac{[10 - (\text{AML} + \text{MML})]}{10} \times \text{RL}$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC1					
PC2					
PC6					
PC8					
OC4					
OC5					
DR1					
RA2					
RA3					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Asset Management checklist (Phase 2).

3 Asset Management

PC1	Description Identification and scoping of information assets, including systems, applications, and infrastructure, based on their criticality to organizational and national operations. Context Accurate asset scoping ensures that cybersecurity controls and monitoring efforts are focused on assets whose compromise would cause significant operational or national impact.	AML Information assets are identified, documented, and classified based on defined criticality, sensitivity, and dependency criteria across the organization.	
		MML Management reviews asset scope, approves criticality classifications, assigns ownership, and ensures updates during organizational or technology changes.	
		RL Poor asset scoping significantly increases likelihood of critical systems being under-protected or overlooked during security incidents.	
Notes / Justification			
IC1	Description Maintenance of an accurate inventory of information assets with clearly assigned ownership and accountability. Context A reliable asset inventory enables effective security management, risk assessment, and incident response by ensuring visibility and accountability for all assets.	AML A centralized inventory of information assets is maintained, documenting ownership, location, purpose, and classification for critical systems.	
		MML Management ensures asset inventories are reviewed periodically, ownership remains valid, and discrepancies are resolved.	
		RL Incomplete or outdated inventories increase likelihood of unmanaged assets, control gaps, and delayed response during incidents.	
Notes / Justification			
OC6	Description Monitoring of operational information assets to maintain visibility into asset status, usage, and security-relevant changes. Context Continuous monitoring of assets supports early detection of anomalies, unauthorized changes, and conditions that could impact security or availability.	AML Operational assets are monitored to track status, configuration changes, and security-relevant events using defined monitoring mechanisms.	
		MML Management reviews monitoring outputs, ensures coverage of critical assets, and addresses identified gaps or anomalies.	
		RL Lack of asset monitoring increases likelihood of undetected changes, misuse, and delayed identification of security incidents.	
Notes / Justification			

OC9	Description Secure disposal and decommissioning of information assets to prevent unauthorized access, data leakage, or residual risk after asset end-of-life. Context Improper disposal of assets can expose sensitive data and create security gaps. Secure decommissioning ensures confidentiality and integrity are preserved throughout the asset lifecycle.	AML Asset disposal processes are defined and applied to securely remove data and decommission systems at end-of-life.	
		MML Management oversees disposal activities, approves methods, and ensures compliance with security and regulatory requirements.	
		RL Insecure disposal significantly increases likelihood of data leakage, unauthorized access, and regulatory non-compliance.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
 - The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

Risk Priority(RP) =
$$\frac{[10 - (AML+MML)]}{10} \times RL$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC1					
IC1					
OC6					
OC9					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Identity and Access Management checklist (Phase 2).

4 Identity and Access Management

4 Identity and Access Management

Worksheet Assessment

IC2	Description Implementation of role-based access control to ensure users have access only to information and systems necessary for their job responsibilities. Context RBAC reduces the risk of unauthorized access by aligning permissions with defined roles, supporting least privilege and separation of duties across critical systems.	AML Roles and access privileges are defined, documented, and assigned based on job functions, with access granted according to least privilege principles.	
		MML Management approves role definitions, reviews access assignments periodically, and ensures segregation of duties is enforced.	
		RL Weak role-based access control increases likelihood of unauthorized access, privilege misuse, and compromise of critical systems.	
		Notes / Justification	
IC3	Description Implementation of authentication mechanisms to verify user identities before granting access to information systems and resources. Context Strong authentication ensures only legitimate users gain access to systems, reducing risks from credential compromise, impersonation, and unauthorized access.	AML Authentication mechanisms are defined and implemented to verify user identities before access is granted to systems and applications.	
		MML Management reviews authentication controls, approves standards, and ensures alignment with risk and criticality of accessed systems.	
		RL Weak authentication significantly increases likelihood of account compromise and unauthorized access to sensitive systems.	
		Notes / Justification	
OC10	Description Control of access to internal networks and intranet resources to prevent unauthorized use and lateral movement within the organization. Context Restricting internal network access limits attacker movement and reduces the impact of compromised accounts or systems.	AML Access to internal networks and intranet resources is restricted based on defined access rules and user authorization.	
		MML Management ensures internal access controls are reviewed, monitored, and aligned with security policies and risk levels.	
		RL Poor internal access control increases likelihood of lateral movement and widespread compromise following initial access..	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment chart

The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain

2. Plan the Actions needed with respect to the RP Score. The checklist of actions can be found in the subsequent pages. The relevant checklist page is labelled based on the control identifier(Eg: PC6, etc.)

3. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control

4. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

Risk Priority(RP) = $\frac{[10 - (AML+MML)]}{10}$ x RL

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
IC2					
IC3					
OC10					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Secure Design and Engineering checklist (Phase 2).

5 Secure Design and Engineering

PC5	Description Integration of cybersecurity requirements into system design, development, and engineering processes to ensure security is built in from the outset. Context Security integrated during design reduces structural weaknesses and prevents costly retroactive fixes, ensuring systems are resilient and aligned with organizational risk expectations.	AML Security requirements are defined and integrated into system design and engineering activities using documented secure design principles and standards.	
		MML Management ensures secure engineering practices are approved, applied consistently, and reviewed across projects and system changes.	
		RL Absence of secure integration significantly increases likelihood of design flaws and systemic vulnerabilities in critical systems.	
		Notes / Justification	
PC7	Description Definition and application of security architecture principles and design standards governing systems, networks, and infrastructure. Context A consistent security architecture ensures systems are designed with appropriate controls, reducing complexity, misconfigurations, and inconsistent security implementations.	AML Security architecture principles and design standards are defined, documented, and applied during system and infrastructure design activities.	
		MML Management reviews architecture compliance and ensures deviations are assessed and approved through governance processes.	
		RL Weak or inconsistent architecture increases likelihood of misconfigurations and exploitable systemic weaknesses.	
		Notes / Justification	
PC8	Description Design and implementation of secure redundancy mechanisms to support availability and resilience of critical systems. Context Redundancy designed with security considerations prevents single points of failure while ensuring failover mechanisms do not introduce new vulnerabilities.	AML Secure redundancy requirements are defined and implemented during infrastructure design based on availability and resilience needs.	
		MML Management approves redundancy designs and reviews effectiveness during testing and operational use.	
		RL Poorly designed redundancy increases likelihood of outages or insecure failover during incidents.	
		Notes / Justification	

PC9	Description Secure integration and management of legacy systems within modern environments to reduce inherited vulnerabilities and operational risk. Context Legacy systems often lack modern security controls. Secure integration ensures older technologies do not weaken overall system security or introduce unmanaged exposure.	AML Security risks associated with legacy systems are identified, documented, and addressed during integration using defined compensating controls.	
		MML Management reviews legacy integration risks, approves mitigation strategies, and ensures alignment with security architecture standards.	
		RL Poor legacy integration increases likelihood of exploitable weaknesses and compromise of connected critical systems.	
		Notes / Justification	
IC4	Description Design and implementation of secure perimeter controls to protect systems and networks from unauthorized external access. Context Well-defined security boundaries limit attack surfaces and prevent unauthorized entry into critical environments and sensitive systems.	AML Network and system boundaries are defined and protected using security controls designed during architecture and engineering stages.	
		MML Management ensures perimeter designs are reviewed, approved, and tested for effectiveness against evolving threat scenarios.	
		RL Weak perimeter design significantly increases likelihood of unauthorized access and external attacks on critical infrastructure.	
		Notes / Justification	
IC6	Description Integration of security testing activities into system design, development, and engineering processes. Context Early security testing identifies weaknesses before deployment, reducing remediation costs and preventing vulnerabilities from entering production environments.	AML Security testing activities are defined and conducted during design, development, and engineering phases to identify vulnerabilities early.	
		MML Management ensures testing requirements are enforced and results are reviewed before system deployment or changes.	
		RL Absence of security testing increases likelihood of deploying vulnerable systems into production environments.	
		Notes / Justification	

OC7	Description Implementation of secure configuration and protection mechanisms for devices supporting critical systems and infrastructure. Context Secure device configurations reduce attack surfaces and prevent exploitation arising from default settings, misconfigurations, or unmanaged endpoints.	AML Secure configuration baselines for devices are defined, documented, and applied during deployment and operation.	
		MML Management reviews configuration standards, ensures enforcement, and monitors deviations for corrective action.	
		RL Weak device configuration increases likelihood of exploitation, lateral movement, and compromise of critical systems.	
		Notes / Justification	
OC8	Description Design and implementation of security controls for cloud-based systems, services, and infrastructure supporting critical operations. Context Cloud environments introduce shared responsibility and dynamic risks that require security controls to be engineered directly into cloud architecture and services.	AML Cloud security requirements are defined and integrated into cloud architecture, configurations, and service deployments.	
		MML Management oversees cloud security design, reviews control effectiveness, and ensures alignment with risk and regulatory requirements.	
		RL Poor cloud security engineering increases likelihood of data exposure, misconfigurations, and compromise of cloud-hosted critical services.	
		Notes / Justification	
DR3	Description Design of resilient system architectures to ensure continuity, fault tolerance, and rapid recovery of critical services. Context Resilient architectures reduce impact of failures and cyber incidents by enabling systems to withstand, adapt, and recover from disruptions.	AML Resilience requirements are incorporated into system architecture design, including fault tolerance, failover, and recovery mechanisms.	
		MML Management approves resilient design decisions and reviews performance during testing and real incidents.	
		RL Lack of resilient architecture increases likelihood of prolonged outages and inability to recover critical services.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
 - The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

$$\text{Risk Priority(RP)} = \frac{[10 - (\text{AML} + \text{MML})]}{10} \times \text{RL}$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC5					
PC7					
PC8					
PC9					
IC4					
IC6					
OC7					
OC8					
DR3					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Vulnerability and Patch Management checklist (Phase 2).

6 Vulnerability and Patch Management

6 Vulnerability and Patch Management

Worksheet Assessment

PC6	Description Identification and assessment of vulnerabilities affecting systems, applications, and infrastructure supporting critical services. Context Timely identification of vulnerabilities enables organizations to understand exposure and prioritize remediation before weaknesses are exploited.	AML Vulnerabilities are identified, analyzed, and documented using defined methods across systems, applications, and infrastructure.	
		MML Management reviews vulnerability assessments, prioritizes risks, and ensures remediation actions align with criticality and impact.	
		RL Unidentified vulnerabilities significantly increase likelihood of exploitation, service disruption, and compromise of critical assets.	
		Notes / Justification	
IC6	Description Use of security testing techniques to discover vulnerabilities in systems, applications, and infrastructure. Context Security testing complements vulnerability scanning by identifying weaknesses that automated tools or routine checks may miss.	AML Security testing activities are conducted to identify vulnerabilities and document findings across critical systems and applications.	
		MML Management ensures testing results are reviewed, remediation is prioritized, and repeat issues are tracked.	
		RL Absence of security testing increases likelihood of unknown vulnerabilities persisting and being exploited.	
		Notes / Justification	
OC5	Description Assessment of vulnerability exposure through penetration testing to evaluate real-world exploitability of identified weaknesses. Context Penetration testing provides insight into attacker perspectives and validates whether vulnerabilities can be practically exploited.	AML Penetration testing is conducted periodically to identify exploitable vulnerabilities and document associated risk exposure.	
		MML Management reviews test results, approves remediation priorities, and tracks closure of findings.	
		RL Lack of penetration testing increases likelihood of exploitable vulnerabilities remaining undetected until incidents occur.	
		Notes / Justification	

OC7	Description Management of security patches and configuration updates to remediate vulnerabilities across systems, applications, and infrastructure.	AML Patching and configuration updates are identified, tested, documented, and deployed based on vulnerability severity and asset criticality.	
		MML Management reviews patching performance, approves timelines, and ensures remediation aligns with operational and risk priorities.	
		RL Delayed or inconsistent patching significantly increases likelihood of exploitation using known vulnerabilities.	
		Notes / Justification	
RA2	Description Identification of vulnerabilities and control weaknesses through audit and assurance activities.	AML Audit findings are analyzed to identify vulnerability management gaps and document associated risks across critical systems.	
		MML Management reviews audit-identified issues, prioritizes corrective actions, and tracks remediation to closure.	
		RL Failure to address audit-identified weaknesses increases likelihood of recurring vulnerabilities and security incidents.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page

The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain

2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook

3. Plan the Actions needed with respect to the RP Score

4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control

5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

Risk Priority(RP) = $\frac{[10 - (AML+MML)]}{10}$ x RL

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC6					
IC6					
OC5					
OC7					
RA2					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AML, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Threat Intelligence checklist (Phase 2).

7 Threat Intelligence

PC2	Description Identification and use of threat intelligence derived from interdependencies between critical systems, partners, suppliers, and external ecosystems. Context Interdependencies expose organizations to shared threats. Understanding threat intelligence across connected entities improves anticipation of risks and coordinated defensive actions.	AML Threat intelligence related to interdependencies is identified, collected, and documented from internal sources, partners, and trusted external channels.	
		MML Management reviews dependency-based threat intelligence and ensures it informs risk assessment and defensive planning.	
		RL Lack of interdependency-focused intelligence increases likelihood of blind spots and cascading cyber incidents.	
		Notes / Justification	
OC11	Description Identification and analysis of advanced threats, including advanced persistent threats (APTs), targeting critical systems and infrastructure Context Advanced threats are often targeted and persistent. Intelligence on attacker techniques and campaigns enables proactive detection and response.	AML Intelligence on advanced threats and APT activities is collected, analyzed, and documented using internal detection and trusted external intelligence sources.	
		MML Management ensures advanced threat intelligence is reviewed, prioritized, and integrated into monitoring and response strategies.	
		RL Absence of advanced threat intelligence increases likelihood of prolonged undetected compromise	
		Notes / Justification	
RA1	Description Participation in government-led and sectoral threat intelligence sharing mechanisms. Context Threat sharing enhances collective defense by providing early warning of emerging threats affecting critical sectors and national infrastructure.	AML Government and sectoral threat intelligence sources are identified and regularly consumed to support situational awareness.	
		MML Management oversees participation in threat-sharing initiatives and ensures intelligence is disseminated internally.	
		RL Failure to leverage shared intelligence increases likelihood of delayed detection and response to widespread threats.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
 - The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

$$\text{Risk Priority(RP)} = \frac{[10 - (\text{AML} + \text{MML})]}{10} \times \text{RL}$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC2					
OC11					
RA1					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Security Incidence Management checklist (Phase 2).

Security Incidence Management

PC3	Description Establishment of governance structures, roles, and responsibilities for managing information security incidents across the organization. Context Clear incident governance ensures coordinated decision-making, accountability, and effective management of security incidents impacting critical systems and services.	AML Incident management roles, responsibilities, escalation paths, and governance processes are defined, documented, and communicated.	
		MML Management oversees incident governance, reviews major incidents, and ensures accountability for response effectiveness.	
		RL Weak incident governance increases likelihood of delayed response, confusion, and ineffective incident handling.	
		Notes / Justification	
OC2	Description Detection, analysis, response, and recovery activities for information security incidents affecting systems and infrastructure. Context Timely detection and effective response limit the impact of security incidents and reduce damage to critical services, data, and operations.	AML Security incidents are detected, analyzed, contained, and responded to using defined procedures and response workflows.	
		MML Management ensures incident response capabilities are resourced, tested, and reviewed after incidents.	
		RL Ineffective incident response significantly increases likelihood of prolonged disruption, data loss, and escalation of cyber incidents.	
		Notes / Justification	
OC11	Description Handling of security incidents involving advanced threats, including coordinated or persistent attack campaigns. Context Advanced incidents require specialized handling to eradicate threats, prevent reinfection, and protect critical systems from sustained compromise.	AML Procedures are defined to handle advanced threat incidents, including containment, eradication, and coordinated response activities.	
		MML Management reviews advanced incident handling outcomes and ensures lessons learned improve response capability.	
		RL Poor handling of advanced incidents increases likelihood of persistent compromise and repeated attacks.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page

The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain

2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook

3. Plan the Actions needed with respect to the RP Score

4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control

5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

Risk Priority(RP) = $\frac{[10 - (AML+MML)]}{10}$ x RL

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC3					
OC2					
OC11					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Resilience Management checklist (Phase 2).

9 Resilience Management

PC2	Description Identification and management of interdependencies between critical systems, services, suppliers, and supporting infrastructure. Context Interdependencies can cause failures in one area to cascade across multiple critical services, amplifying disruption.	AML Interdependencies between critical systems and external dependencies are identified and documented for resilience planning.	
		MML Management reviews interdependencies, assigns ownership, and ensures they inform continuity and recovery decisions.	
		RL Poorly understood interdependencies increase likelihood of cascading failures and widespread service disruption during incidents.	
		Notes / Justification	
PC8	Description Implementation of redundancy to reduce single points of failure in critical systems and infrastructure. Context Redundancy improves service continuity by ensuring alternate components are available during failures.	AML Redundancy requirements for critical systems are defined, implemented, and documented based on service criticality.	
		MML Management approves redundancy strategies and reviews their effectiveness periodically.	
		RL Insufficient redundancy increases likelihood of service outages when primary components fail.	
		Notes / Justification	
PC12	Description Physical safeguards supporting resilience and continuity of facilities and infrastructure. Context Physical incidents can disrupt operations; resilience-focused physical controls help maintain service availability.	AML Physical resilience controls are identified and implemented to protect critical facilities and infrastructure.	
		MML Management reviews physical safeguards and ensures alignment with resilience objectives.	
		RL Weak physical controls increase likelihood of operational disruption during physical or environmental incidents.	
		Notes / Justification	

IC5	Description Ensuring availability of critical services during cyber, physical, or operational disruptions.	AML Availability requirements for critical services are defined, documented, and supported through resilience measures.	
		MML Management reviews availability performance, approves targets, and ensures alignment with continuity objectives.	
		RL Inadequate availability planning increases likelihood of service downtime and failure to meet recovery expectations during incidents.	
		Notes / Justification	
OC2	Description Use of incident response capabilities to contain incidents and support stabilization and recovery of critical services.	AML Incident response procedures support containment, stabilization, and recovery of critical services during disruptive events.	
		MML Management reviews incident outcomes and ensures response capabilities support resilience and recovery objectives.	
		RL Ineffective response handling increases likelihood of prolonged outages, escalation, and delayed restoration of critical services.	
		Notes / Justification	
DR1	Description Development and maintenance of contingency and continuity plans for restoring critical services after disruption.	AML Contingency and continuity plans are defined, documented, and maintained for critical systems and processes.	
		MML Management reviews, approves, and ensures periodic testing and updating of continuity plans.	
		RL Absence of effective contingency planning increases likelihood of prolonged service disruption and recovery failure.	
		Notes / Justification	

DR2	Description Provisioning and maintenance of disaster recovery sites to restore critical systems and services after major disruptions.	AML Disaster recovery sites are defined, documented, and maintained based on recovery objectives for critical services.	
		MML Management approves recovery site strategies, reviews readiness, and ensures periodic testing of recovery capabilities.	
		RL Absence of effective recovery sites increases likelihood of prolonged outages and inability to restore critical services after incidents.	
		Notes / Justification	
DR3	Description Design and implementation of architectures that support rapid recovery and continuity of critical services following disruption.	AML Recovery and continuity requirements are integrated into system and service architecture design.	
		MML Management reviews recovery performance, approves architectural improvements, and ensures lessons learned are incorporated.	
		RL Weak recovery architecture increases likelihood of repeated failures and slow restoration of critical services.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
 - The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

$$\text{Risk Priority(RP)} = \frac{[10 - (AML + MML)]}{10} \times RL$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC2					
PC8					
PC12					
IC5					
OC2					
DR1					
DR2					
DR3					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Physical and Environmental Security checklist (Phase 2).

10 Physical and Environmental Security

10 Physical and Environmental Security

Worksheet Assessment

PC12	Description Implementation of physical and environmental safeguards to protect facilities and infrastructure supporting critical systems. Context Physical and environmental incidents such as unauthorized access, fire, or power failure can directly disrupt critical services if not adequately controlled.	AML Physical and environmental security requirements are identified and implemented to protect critical facilities and infrastructure.	
		MML Management reviews physical safeguards, approves controls, and ensures alignment with environmental and operational risks.	
		RL Weak physical or environmental controls increase likelihood of facility disruption and loss of critical service availability.	
		Notes / Justification	
IC5	Description Ensuring physical availability of infrastructure and facilities required to deliver critical services. Context Critical services depend on physical assets such as data centers, power, and connectivity. Their availability directly impacts service continuity.	AML Physical availability requirements for critical services are defined, documented, and supported through appropriate safeguards.	
		MML Management reviews availability performance and ensures alignment with continuity and resilience objectives.	
		RL Inadequate physical availability planning increases likelihood of service outages during environmental or physical disruptions.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
- The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

Risk Priority(RP) =
$$\frac{[10 - (AML+MML)]}{10} \times RL$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC12					
IC5					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Resilience Management checklist (Phase 2).

11 Data Protection

OC1	Description Protection of sensitive and critical data using cryptographic mechanisms such as encryption and hashing.	AML Cryptographic controls are defined and implemented to protect sensitive and critical data across systems and storage locations.	
		MML Management approves cryptographic standards, reviews implementation effectiveness, and ensures compliance with regulatory requirements.	
		RL Weak cryptographic protection increases likelihood of data exposure, integrity compromise, and regulatory violations.	
		Notes / Justification	
OC4	Description Implementation of controls to prevent unauthorized leakage, transfer, or loss of sensitive and critical data.	AML Data loss risks are identified and mitigated using preventive and detective controls across data handling processes.	
		MML Management reviews data loss incidents, approves mitigation measures, and monitors effectiveness of controls.	
		RL Inadequate data loss prevention increases likelihood of sensitive data leakage and compliance violations.	
		Notes / Justification	
OC8	Description Protection of sensitive and critical data stored or processed in cloud environments.	AML Data protection requirements for cloud environments are defined and implemented through secure configurations and controls.	
		MML Management oversees cloud data protection practices and ensures alignment with risk and regulatory expectations.	
		RL Weak cloud data protection increases likelihood of data exposure, misconfiguration incidents, and loss of sensitive information.	
		Notes / Justification	

OC9	Description Secure disposal of data and media to prevent unauthorized recovery of sensitive or critical information. Context Improper data disposal can expose sensitive information even after systems are decommissioned or media is retired.	AML Data disposal methods are defined and implemented to securely erase or destroy sensitive data and media.	
		MML Management approves disposal procedures, reviews compliance, and ensures evidence of secure disposal is maintained.	
		RL Insecure data disposal increases likelihood of data leakage, regulatory violations, and unauthorized information recovery.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
 - The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

Risk Priority(RP) = $\frac{[10 - (AML+MML)]}{10}$ x RL

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
OC1					
OC4					
OC8					
OC9					

Data Protection

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Supply Chain Risk checklist (Phase 2).

12 Supply Chain Risk

PC10	Description Governance of cybersecurity risks arising from third-party vendors, suppliers, service providers, and outsourced operations. Context Supply chain entities can introduce indirect cyber risks. Governance ensures third-party relationships do not undermine security and resilience of critical services.	AML Supply chain security requirements are defined, documented, and applied across vendor onboarding and contract management processes.	
		MML Management reviews supplier risks, approves assurance requirements, and monitors compliance throughout vendor relationships.	
		RL Weak supply chain governance increases likelihood of third-party compromise affecting critical systems and services.	
		Notes / Justification	
IC6	Description Security testing and assurance activities applied to suppliers, products, and services to identify supply chain vulnerabilities. Context Testing and assurance reduce risk of compromised components, insecure integrations, or malicious insertions through the supply chain.	AML Security testing or assurance activities are conducted for suppliers, products, or services supporting critical operations.	
		MML Management reviews assurance results, addresses identified risks, and ensures remediation actions are implemented.	
		RL Absence of supply chain assurance increases likelihood of compromised components entering critical environments.	
		Notes / Justification	
OC8	Description Management of cybersecurity risks associated with cloud providers and third-party service platforms supporting critical operations. Context Cloud and managed services extend organizational boundaries, requiring clear controls to manage shared responsibility and external dependencies.	AML Security requirements for cloud and third-party services are defined and implemented through contractual and technical controls.	
		MML Management oversees third-party service risk and ensures alignment with organizational risk tolerance.	
		RL Weak third-party service controls increase likelihood of data exposure and service disruption.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
 - The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

$$\text{Risk Priority(RP)} = \frac{[10 - (\text{AML} + \text{MML})]}{10} \times \text{RL}$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC10					
IC6					
OC8					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Workforce Management checklist (Phase 2).

13 Workforce Management

PC3	Description Definition of workforce structure, roles, and responsibilities relevant to cybersecurity and protection of critical systems. Context Clear role definition ensures accountability, prevents gaps in responsibility, and supports coordinated execution of security-related duties across the organization.	AML Workforce roles and responsibilities related to cybersecurity are defined, documented, and communicated across relevant functions.	
		MML Management approves role assignments, reviews adequacy periodically, and ensures responsibilities align with security objectives.	
		RL Unclear workforce roles increase likelihood of accountability gaps and ineffective execution of security responsibilities.	
		Notes / Justification	
PC11	Description Ensuring personnel involved in cybersecurity and critical operations possess appropriate qualifications, certifications, and competence. Context Competent personnel are essential for effective security implementation, compliance, and response to evolving cyber threats.	AML Competence requirements are defined, and relevant certifications or qualifications are identified for security-related roles.	
		MML Management ensures personnel competence is reviewed, gaps are addressed, and certifications remain current.	
		RL Inadequate workforce competence increases likelihood of errors, misconfigurations, and ineffective security controls.	
		Notes / Justification	
OC3	Description Provision of cybersecurity training and awareness programs for personnel supporting critical systems and operations. Context Training and awareness reduce human-related risks by ensuring personnel understand security responsibilities and recognize threats.	AML Cybersecurity training and awareness activities are conducted for personnel based on role and risk exposure.	
		MML Management reviews training effectiveness and ensures participation across the workforce.	
		RL Insufficient training increases likelihood of human error, social engineering success, and security incidents.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page

The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain

2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook

3. Plan the Actions needed with respect to the RP Score

4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control

5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

$$\text{Risk Priority(RP)} = \frac{[10 - (\text{AML} + \text{MML})]}{10} \times \text{RL}$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC3					
PC11					
OC3					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Change Management checklist (Phase 2).

14 Change Management

14 Change Management

Worksheet Assessment

PC5	Description Integration of cybersecurity requirements into change management processes for systems, applications, and infrastructure supporting critical services. Context Uncontrolled or poorly planned changes can introduce vulnerabilities, disrupt operations, or weaken security controls in critical environments.	AML Security requirements are identified and incorporated into change management processes for systems and infrastructure changes.	
		MML Management reviews and approves changes, ensuring security impacts are assessed and addressed.	
		RL Weak change integration increases likelihood of introducing vulnerabilities and operational disruptions during system changes.	
		Notes / Justification	
PC7	Description Control of configuration and architectural changes to ensure security and stability of critical systems. Context Changes to configurations or architectures can significantly affect security posture. Structured control ensures consistency and prevents unintended exposure.	AML Configuration and architectural changes are documented, reviewed, and implemented using defined change control procedures.	
		MML Management ensures configuration changes are authorized, tracked, and periodically reviewed.	
		RL Poor configuration change control increases likelihood of misconfigurations and exploitable security weaknesses.	
		Notes / Justification	
PC9	Description Governance of changes involving legacy systems to manage inherited risks and maintain operational stability. Context Legacy systems often lack modern controls. Changes to such systems require additional oversight to prevent unintended security or availability impacts.	AML Changes involving legacy systems are identified, assessed, and implemented using compensating controls where required.	
		MML Management reviews legacy system changes and ensures risks are mitigated before approval.	
		RL Uncontrolled legacy changes increase likelihood of system instability and security compromise.	
		Notes / Justification	

DR3	Description Use of situational awareness to understand system health, recovery status, and resilience posture during and after disruptive events Context Situational awareness must extend beyond detection to include visibility into recovery progress and system stability, enabling informed decisions during prolonged or complex incidents.	AML Recovery status, system health, and resilience indicators are monitored to maintain awareness during incidents and restoration activities.	
		MML Management reviews resilience-related situational insights and uses them to guide recovery decisions.	
		RL Lack of recovery-focused awareness increases likelihood of delayed restoration and repeated service disruption.	
		Notes / Justification	

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page
 - The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain
2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook
3. Plan the Actions needed with respect to the RP Score
4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control
5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

$$\text{Risk Priority(RP)} = \frac{[10 - (\text{AML} + \text{MML})]}{10} \times \text{RL}$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC6					
PC7					
PC9					
DR3					

Notes

Instructions

1. Each control has an assessment section
2. Read the Description and Context for the control, based on your organization's perceived current state and
 - i. Assign an appropriate value for AML (Approach Maturity Level)
 - ii. Assign an appropriate value for MML (Management Maturity level)
 - iii. Assign an appropriate value for RL (Risk Likelihood)

***For more context on AMI, MML & RL refer to Scoring Criteria for Assessment Pg. 18 & 19**

3. Provide Notes/ Justification for future reference wherever required
4. After scoring each control, refer to the scorecard for the next step.
5. After completing this section, refer to Workbook 2: Sensemaking for the Situational Awareness checklist (Phase 2).

15 Situational Awareness

PC2	Description Understanding interdependencies between critical systems, services, and external entities to maintain awareness of evolving operational and cyber conditions. Context Awareness of interdependencies enables organizations to anticipate cascading effects and maintain visibility during rapidly changing threat or disruption scenarios.	AML Interdependencies are identified and monitored to support situational awareness during normal operations and incidents.	
		MML Management reviews dependency-related insights and ensures they inform operational awareness and decision-making.	
		RL Poor interdependency awareness increases likelihood of blind spots and delayed response during cascading incidents.	
		Notes / Justification	
OC2	Description Monitoring of security and operational events to maintain real-time awareness of conditions affecting critical systems. Context Continuous monitoring enables early detection of anomalies, incidents, and emerging threats, supporting timely response and informed decisions.	AML Security and operational events are monitored to detect anomalies affecting critical systems and services.	
		MML Management ensures monitoring outputs are reviewed and used to maintain operational awareness.	
		RL Lack of effective monitoring increases likelihood of delayed detection and escalation of security incidents.	
		Notes / Justification	
OC11	Description Monitoring and analysis of advanced threats and persistent attack activity to maintain awareness of sophisticated adversary behavior. Context Advanced threats often evade basic controls. Focused monitoring improves awareness of stealthy or long-term attack campaigns.	AML Advanced threat indicators are monitored and analyzed to maintain awareness of persistent or targeted attacks.	
		MML Management ensures advanced threat awareness informs defensive posture and response priorities.	
		RL Absence of advanced threat awareness increases likelihood of prolonged undetected compromise.	
		Notes / Justification	

RA1	Description Reporting and sharing of cybersecurity threats, incidents, and situational updates with relevant authorities and stakeholders. Context Timely threat reporting enhances collective situational awareness, enabling coordinated response and early warning across organizations and sectors.	AML	Threat and incident information is reported and shared through defined internal and external communication channels	
		MML	Management reviews reporting practices and ensures timely, accurate dissemination of situational information.	
		RL	Poor threat reporting reduces shared awareness and increases likelihood of delayed or uncoordinated response.	
		Notes / Justification		
RA2	Description Use of audits and assessments to improve awareness of security posture, gaps, and emerging risks affecting critical systems. Context Audits provide structured insight into weaknesses and trends, strengthening situational awareness beyond real-time monitoring.	AML	Audit and assessment results are analyzed to identify trends and gaps affecting situational awareness.	
		MML	Management reviews audit insights and ensures findings inform awareness, monitoring priorities, and decision-making.	
		RL	Failure to use audit insights increases likelihood of blind spots and repeated undetected weaknesses.	
		Notes / Justification		

1. Calculate the Risk Priority(RP) Score using the values from the Assessment page

The Risk Priority(RP) Score represents the immediacy of actions required to satisfy the requisites of a control in accordance with its domain

2. Calculate Average RP Score of each Control group in a domain to later use in the Reformulating workbook

3. Plan the Actions needed with respect to the RP Score

4. Identify Point of Contact(person/team) in-charge of ensuring compliance of each control

5. Set an appropriate Timeline to ensure that compliance objective of the respective control is achieved

$$\text{Risk Priority(RP)} = \frac{[10 - (\text{AML} + \text{MML})]}{10} \times \text{RL}$$

Lower the score, lower the priority
Higher the score, higher the priority

	RP	Average RP	Action needed	Point of Contact	Timeline
PC2					
OC2					
OC11					
RA1					
RA2					

Situational Awareness

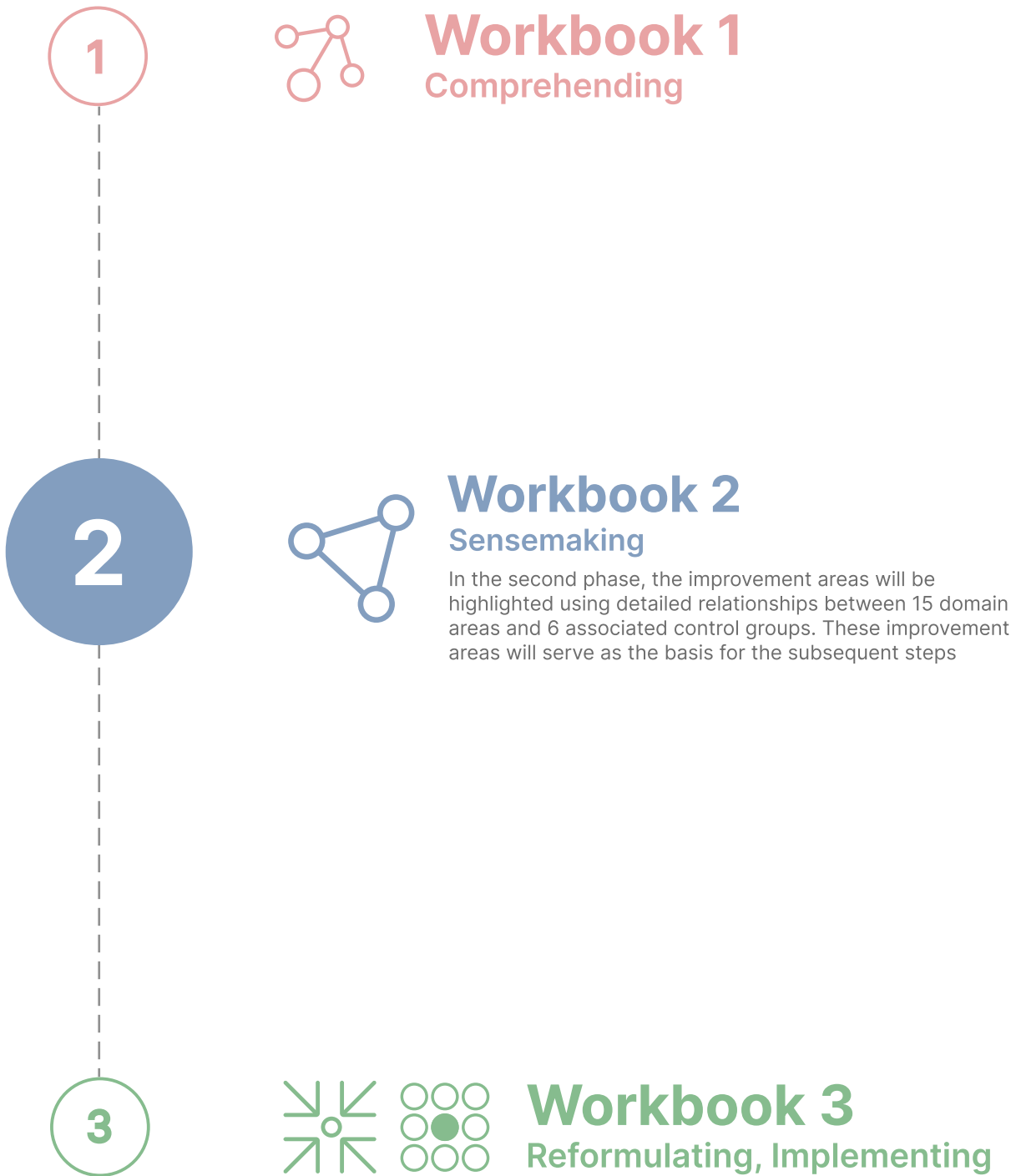
Notes

Navigating Through the Workbooks

Next Phase - Workbook 2: Sensemaking

How to use the next workbook based on the current one ?

The insights and outcomes gathered in this workbook form the foundation for the next phase of the journey. By carrying forward the findings from the Comprehending phase, organizations can ensure continuity, informed decision-making, and a smoother transition toward implementing NCIIPC-aligned cybersecurity practices.



Workbook for NCIIPC based transformation of Indian Organizations



The workbook is designed as a supplement to the *NCIIPC Guidelines For Protection Of National Critical Information Infrastructures*. It is designed to aid cybersecurity practitioners to successfully integrate the principles and guidelines of NCIIPC into their organizational practices in a systematic manner.

As a foundational element within India's cybersecurity practices, the NCIIPC guidelines is aimed to enhance protection of vital national assets. The actual results of these guidelines depend on their successful implementation across sectors possessing different resource capabilities, technical abilities and maturity levels. This workbook uses analytical tools to examine the existing cybersecurity posture of organizations using frameworks and methodologies which enhance guideline comprehension and reveal opportunities for performance improvement. Further, it adopts a broader human-centric lens—not limited to the direct involvement of individuals but extending to the tools and methods that allow organizations to analyze, adapt, and implement NCIIPC guidelines effectively in a participatory and phased manner.

The workbook derives from the principles of human-centered design thinking and systems thinking to support the adoption of NCIIPC guidelines using a 4-phase transformation process: *Comprehending, Sensemaking, Reformulating, Implementing*. These 4 phases and the associated analytical tools, systematically guide the practitioners in identifying the gaps in the organization's cybersecurity posture and aids them in formulating solutions in a participatory manner, while taking into account the viewpoints of the various stakeholders. In other words, the *NCIIPC based systemic transition* is an organizational achievement brought forth by *participation* and *collaboration* in light of the enhancements in the cybersecurity posture.

Phase 1: Comprehending

In the very first phase the key idea is to self assess and comprehend the essential status of the organization, in terms of the various domains and respective controls.

Phase 2: Sensemaking

In the second phase, the improvement areas are highlighted using detailed relationships between 15 domain areas and 6 associated control groups. These improvement areas serve as the basis for the subsequent steps.

Phase 3: Reformulating

In the third phase, improvement pathways are created in order to fill the gaps identified in the previous two phases. This phase uses templates and tools to enable the practitioners to chart out a set of actions for the improvement of the organization's cybersecurity posture.

Phase 4: Implementing

In the fourth phase, detailed course of action in the third phase get implemented in the organization. This aids the changemakers by providing them with tools to aid in the change implementation process based on priority and impact. thus enabling a smoother transition towards the integration of NCIIPC based guidelines and principles in the organization.

Vivek Kant
Soham Mohanty

HF
SS Studios

ISBN 978-93-6126-253-9



9 789361 282539