



Workbook for NCIIPC based Transformation of Indian Organizations

Enhancing the Cybersecurity Posture for Critical
Information Infrastructures

Sensemaking

2

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 2: Sensemaking

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

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.

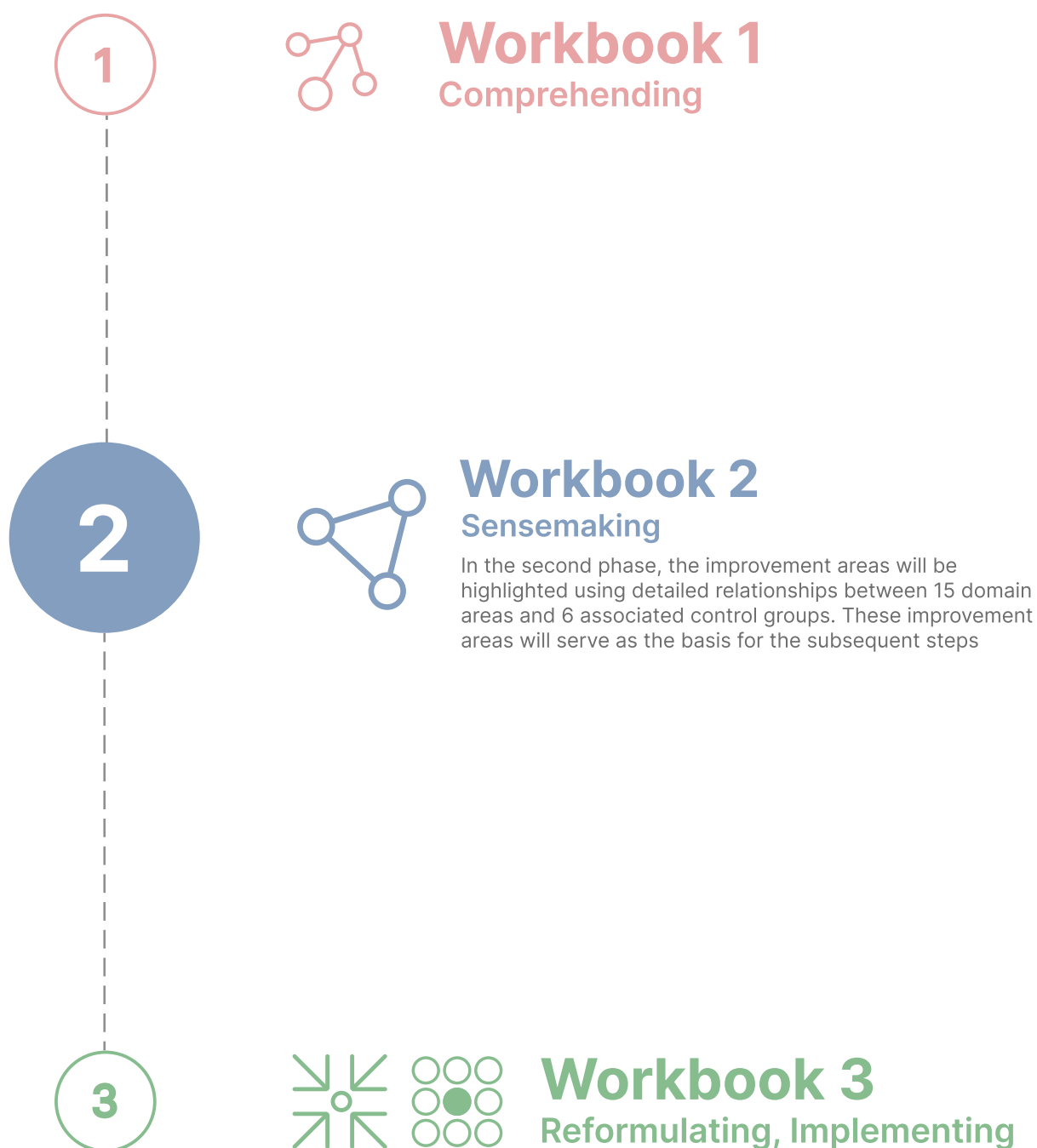
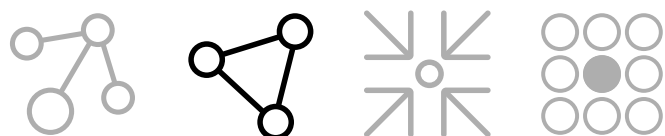


Table of Contents

Workbook for NCIIPC based transformation of Indian Organizations

Benefits of the Workbook	1
Introduction	2
Collaborative Change Management Process	4
How to use the worksheets	8
Governance.....	9
Risk Management.....	21
Asset Management.....	31
Identity and Access Management.....	37
Secure Design and Engineering.....	41
Vulnerability and Patch Management.....	51
Threat Intelligence.....	57
Security Incidence Management.....	61
Resilience Management.....	65
Physical and Environmental Security.....	77
Data Protection.....	81
Supply Chain Risk.....	87
Workforce Management.....	100
Change Management.....	104
Situational Awareness.....	110



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

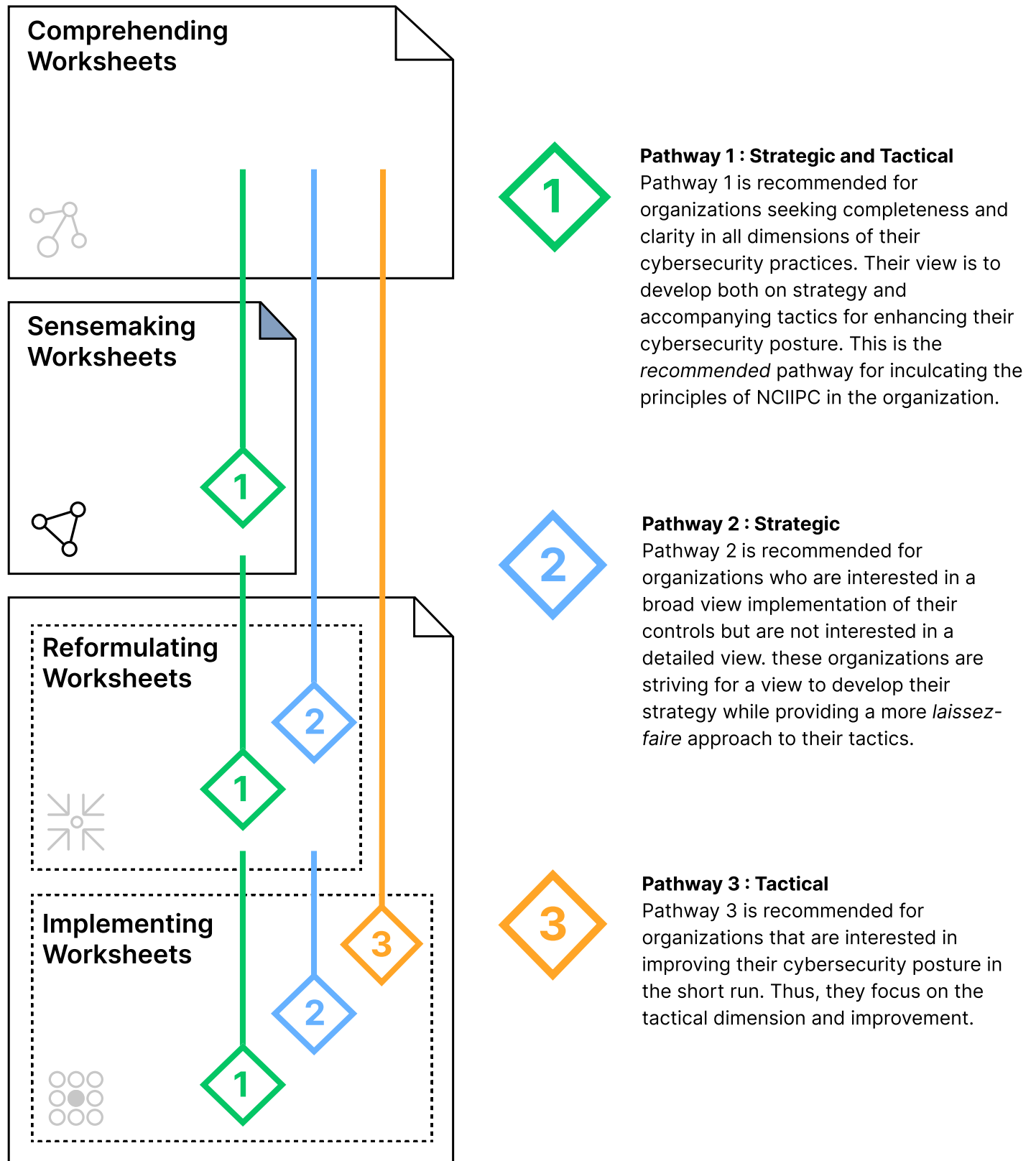
In this third phase, improvement pathways are created by delving into particular domains and controls in multiple ways. These can be made possible by the use of templates that provide clarity and insight into the particular areas.

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.

How to use the worksheets

Guide

X Domain Name

PC1

RP Range	Checklist
0 - <1	
1 - <2	
2 - <3	
3 - <4	
4 - <5	

For PC1 also refer to...

Notes

1

Find your RP score's range and follow the suggestions ,mentioned in the individual Control checklist pages

This is the section that has the RP range. Get your RP Score from the Scorecard page and follow the suggestions based on the range it falls in.

These are the curated suggestions for the particular control based on the RP Score's range. Tick the checkboxes of the suggestions you have implemented. For urgent implementation focus on your RP Range's suggestions. In order to achieve a comprehensive implementation of security practices, try to follow every suggestion this page

Because the suggestions are based on the context of the control under a particular domain, a few controls fall under multiple domain, for extensive implementation of a control, please refer to this section.

X Domain Name

PC1

RP Range	Checklist
0 - <1	
1 - <2	
2 - <3	
3 - <4	
4 - <5	

Notes

2

The objective is to achieve a comprehensive implementation of security practices. Therefore, practitioners are strongly advised to adhere to every suggestion on this page, regardless of the calculated RP score.

Implementation Sequence: It is advised that practitioners proceed with the checklist from the highest RP range to the lowest RP range. This sequence prioritizes fixing the areas with the worst scores (4-<5) and the highest risk exposure first.

Due to potential differences in self-perception and evaluation, the calculated Risk Priority (RP) Score for a specific control may occasionally fall outside the suggested RP range on the checklist. In all cases, please prioritize implementing the required actions based on the calculated RP score for accurate risk mitigation. Following all suggestions ensures that your organization adopts the complete set of best practices for the target control.

Instructions

1. Retrieve the calculated RP score from workbook 1 (Governance).
2. Locate the appropriate control within the Governance domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

1 Governance

RP Score

Checklist to follow

Planning Controls

Governance

0 - <1	☐ Maintain a formally approved CII identification framework that is regularly reviewed and aligned with national NCIIPC guidance. ☐ Ensure the CII inventory is continuously updated and mapped to business processes, services, and supporting information assets. ☐ Conduct periodic cross-functional governance reviews (IT, OT, business, risk) to validate that all critical services and dependencies are correctly classified as CII. ☐ Maintain executive-level dashboards that provide clear visibility into the current CII landscape, ownership, and associated risk posture.
1 - <2	☐ Improve the existing CII identification methodology to include clear criteria for impact on national security, economy, public safety, and public confidence. ☐ Establish structured governance forums where CII owners, risk teams, and senior leadership review additions or changes to the CII list at least annually. ☐ Conduct regular reconciliation between the CII inventory, asset registers, and risk registers to ensure consistency and completeness. ☐ Enhance documentation of decision rationales for why specific systems, networks, or data flows are classified (or not classified) as CII.
2 - <3	☐ Perform a comprehensive review of current CII identification practices to identify gaps in coverage, especially across subsidiaries, vendors, and joint ventures. ☐ Implement a formal process to map vertical and horizontal dependencies (upstream/downstream services) when determining CII status. ☐ Develop standardized templates and guidance for business units to propose and justify CII designation for their critical assets. ☐ Increase engagement with national guidance (NCIIPC advisories, workshops) to refine and mature the organization's CII identification approach.
3 - <4	☐ Deploy a governance-led CII identification programme to systematically discover, document, and classify critical assets across all business lines. ☐ Assign named CII owners and establish clear accountability for maintaining accurate information about each CII asset and its dependencies. ☐ Formalize escalation and approval workflows for newly discovered critical systems so that they are rapidly assessed and, where appropriate, designated as CII. ☐ Increase management oversight on projects, changes, and new deployments to ensure CII identification is embedded as a mandatory step in project governance.
4 - <5	☐ Urgent intervention required! Initiate an immediate, organization-wide CII discovery and classification exercise to identify all systems whose failure could have debilitating impact. ☐ Establish a temporary governance task force, led by senior management, to oversee rapid CII identification and ensure alignment with regulatory expectations. ☐ Implement mandatory reporting from all departments on critical services and supporting technology, consolidating information into a central CII register. ☐ Enforce a moratorium on major changes to potentially critical systems until they are assessed for CII relevance and associated governance controls are defined.

Also refer to
2.Risk Management PC1
3.Asset Management PC1

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formal governance process to document all vertical and horizontal interdependencies across business units, systems, and service providers. ☐ Ensure interdependency maps are routinely updated to reflect changes in organizational structure, technology, and service delivery models. ☐ Conduct periodic cross-functional workshops to validate that all upstream and downstream dependencies are accurately captured. ☐ Maintain governance dashboards that provide clear visibility into critical interconnections affecting service continuity and risk posture.
1 - <2	☐ Improve existing interdependency documentation to include impact pathways, failure propagation scenarios, and service reliance chains. ☐ Establish structured communication channels between interconnected departments to ensure timely updates on operational or technological changes. ☐ Conduct regular governance-level reviews of interdependency risks to ensure decisions reflect current operational realities. ☐ Enhance documentation to include justification for assigning criticality to specific dependencies or removing them from the critical chain.
2 - <3	☐ Perform a comprehensive review of current interdependency mapping practices to identify gaps, redundancies, and outdated information. ☐ Implement a formal methodology for analysing internal and external dependencies, including third-party and cross-sector linkages. ☐ Develop standard templates and guidance for business units to submit interdependency changes and impact assessments. ☐ Increase engagement with national bodies and peer organizations to benchmark interdependency management practices.
3 - <4	☐ Deploy a governance-led programme to systematically identify, validate, and track interdependencies across all CII-relevant assets and processes. ☐ Assign named dependency owners responsible for maintaining accurate and up-to-date information on specific critical interconnections. ☐ Formalize escalation workflows for reporting newly discovered or emerging interdependency risks to senior management. ☐ Increase governance oversight on transformation projects to ensure interdependency considerations are built into design and approval stages.
4 - <5	☐ Urgent intervention required! Initiate an immediate organization-wide reassessment of interdependencies to confirm the accuracy of critical service links. ☐ Establish a cross-functional task force to validate interdependency maps and align them with national security and regulatory expectations. ☐ Implement mandatory reporting procedures requiring all departments to declare changes that may introduce, modify, or remove interdependencies. ☐ Enforce a governance directive halting major system or process changes until critical interdependencies are reassessed and approved.

Also refer to
 2.Risk Management PC2
 7.Threat Intelligence PC2
 9.Resilience Management PC2
 15.Situational Awareness PC2

Notes

RP Score

Checklist to follow

Planning Controls

Governance

0 - <1	☐ Maintain a formally established Information Security Department (ISD) with clearly documented roles, responsibilities, and reporting lines. ☐ Ensure the ISD structure is regularly reviewed to align with organizational changes, emerging technologies, and evolving threat landscapes. ☐ Conduct periodic governance reviews to validate that ISD functions- monitoring, incident response, compliance, and risk are adequately staffed and resourced. ☐ Maintain management dashboards that provide clear visibility into ISD performance, key risks, incident trends, and compliance status.
1 - <2	☐ Improve the ISD organizational model to ensure a balanced blend of technical, governance, and operational capabilities within the team. ☐ Establish structured communication channels between ISD, business units, and senior leadership to ensure timely dissemination of security intelligence and requirements. ☐ Conduct regular coordination meetings between ISD and OT/SCADA teams to ensure protection of both IT and operational environments. ☐ Enhance documentation of ISD workflows, standard operating procedures, and escalation routes to improve consistency and audit readiness.
2 - <3	☐ Perform a comprehensive assessment of ISD capability gaps across skills, tools, and processes to guide resourcing decisions. ☐ Implement a formal competency framework to assess and track ISD expertise, certifications, and functional maturity. ☐ Develop standardized templates and guidance for ISD activities, including incident reporting, risk assessments, policy development, and audits. ☐ Increase engagement with NCIIIPC training programmes, threat briefings, and sector-specific workshops to uplift ISD maturity.
3 - <4	☐ Deploy a governance-led programme to strengthen ISD oversight across the enterprise, ensuring uniform security practices and cross-team accountability. ☐ Assign named ISD leads for major domains (risk management, incident response, architecture, compliance) to improve ownership and operational clarity. ☐ Formalize ISD involvement in all major technology initiatives, ensuring that security-by-design requirements are reviewed and approved before deployment. ☐ Increase management oversight of ISD workload, ensuring teams are not overloaded and critical responsibilities remain fully covered.
4 - <5	☐ Urgent intervention required! Conduct an immediate review of ISD staffing, competencies, and responsibilities to remedy critical capability gaps. ☐ Establish a temporary governance committee to support ISD in stabilizing processes, addressing backlogs, and aligning functions with regulatory expectations. ☐ Implement mandatory reporting from ISD to senior leadership on high-risk issues, incidents, and vulnerabilities requiring organizational attention. ☐ Enforce governance directives requiring that all significant security decisions, policies, and incident escalations flow through ISD as the authoritative body.

Also refer to
8.Security Incident Management PC3
13.Workforce Management PC3

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally approved Information Security Policy that aligns with national regulations, organizational objectives, and recognized security standards. ☐ Ensure the policy is reviewed at least annually to reflect new technologies, organizational changes, and emerging threats. ☐ Conduct periodic governance reviews to validate that all business units understand and comply with the Information Security Policy requirements. ☐ Maintain executive-level dashboards that provide visibility into policy compliance, exceptions, and areas requiring management action.
1 - <2	☐ Improve the policy structure to clearly define security principles, mandatory controls, and responsibilities across IT, OT, and business functions. ☐ Establish structured communication mechanisms to ensure timely dissemination of policy updates to all relevant stakeholders. ☐ Conduct regular alignment checks between the Information Security Policy and related documents such as standards, guidelines, and procedures. ☐ Enhance documentation to include clear justification for any deviations or risk-based exceptions approved by management.
2 - <3	☐ Perform a comprehensive review of the current policy set to identify outdated clauses, redundancies, or areas lacking clarity. ☐ Implement a formal policy lifecycle management process covering drafting, review, approval, communication, and retirement. ☐ Develop standardized templates and writing guidelines to ensure consistency across all policy documents produced by the organization. ☐ Increase engagement with regulatory bodies, sectoral CERTs, and industry groups to benchmark policy content and strengthen alignment.
3 - <4	☐ Deploy an organization-wide programme to reinforce adherence to the Information Security Policy through training, campaigns, and targeted interventions. ☐ Assign policy owners for each major domain (access control, network security, data protection, physical security, etc.) to ensure continuous oversight. ☐ Formalise a structured process for business units to request policy clarifications, exceptions, or supplemental guidance. ☐ Increase governance oversight on transformation and technology projects to ensure policy constraints and requirements are addressed from design stage onward.
4 - <5	☐ Urgent intervention required! Conduct an immediate, organization-wide review to rectify critical gaps or outdated clauses in the Information Security Policy. ☐ Establish a temporary governance task force to accelerate policy updates, align with regulatory expectations, and eliminate unresolved exceptions. ☐ Implement mandatory reporting from business units on their compliance with the Information Security Policy, supported by evidence-based attestation. ☐ Enforce a governance directive that prohibits deployment of new systems, applications, or services without documented compliance with the Information Security Policy.

Notes

RP Score

Checklist to follow

Planning Controls

Governance

0 - <1	☐ Maintain a formally approved supply chain security framework that defines due-diligence, contractual, and oversight requirements for all third-party engagements. ☐ Ensure all vendors interacting with critical systems or data undergo mandatory security vetting prior to onboarding. ☐ Conduct periodic governance reviews to validate that NDAs, confidentiality clauses, and security obligations are implemented and current. ☐ Maintain executive-level dashboards tracking high-risk suppliers, contract expiry, non-compliance, and security posture trends.
1 - <2	☐ Improve supplier categorisation by introducing clear tiers of criticality aligned with business impact and access privileges. ☐ Establish structured communication processes to ensure that vendor security requirements and updates are relayed consistently. ☐ Conduct regular compliance checks to ensure supplier contracts include mandatory clauses on data protection, incident reporting, and subcontractor liabilities. ☐ Enhance documentation of supply chain risk decisions, including justification for onboarding, continuation, or exception approvals.
2 - <3	☐ Perform a comprehensive review of all existing supplier contracts to identify gaps in security obligations, audit rights, and data handling requirements. ☐ Implement a formal risk-based assessment methodology for evaluating suppliers across operational, cybersecurity, and regulatory dimensions. ☐ Develop standardized templates for NDAs, SLAs, and security addendums to ensure uniformity and reduce contractual ambiguity. ☐ Increase engagement with national advisories, sectoral CERTs, and industry bodies to refine supply chain threat awareness and control expectations.
3 - <4	☐ Deploy a governance-led supplier assurance programme to perform periodic reviews, audits, and assessments for all critical vendors. ☐ Assign business and security owners for each critical supplier to ensure proper oversight and continuous monitoring. ☐ Formalise escalations for supplier non-compliance, delays in remediation, or failure to fulfil security obligations. ☐ Increase governance oversight on procurement and IT/OT project pipelines to ensure early identification of suppliers requiring enhanced scrutiny.
4 - <5	☐ Urgent intervention required! Conduct an immediate review of all suppliers with elevated access to critical systems, ensuring NDAs, controls, and obligations are current. ☐ Establish a supply chain security task force to address critical gaps, renegotiate high-risk contracts, and elevate overall supplier maturity. ☐ Implement mandatory reporting by departments engaging third parties, ensuring visibility of all external dependencies across the organization. ☐ Enforce a governance directive prohibiting engagement with any supplier lacking signed NDAs, validated security controls, or compliance with required procurement policies.

Also refer to
12. Supply Chain Risk PC10

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally approved framework defining mandatory security certifications for personnel, technologies, and critical processes across the organization. ☐ Ensure certification requirements are regularly reviewed to align with evolving threat landscapes, regulatory obligations, and technology adoption. ☐ Conduct periodic governance reviews to validate that personnel in security-sensitive roles hold required certifications and renew them on time. ☐ Maintain executive dashboards providing visibility into certification coverage, expiration timelines, and competency gaps.
1 - <2	☐ Improve the organizational certification roadmap by identifying priority roles and minimum competency requirements for each domain. ☐ Establish structured communication processes to ensure employees are aware of required certifications, renewal timelines, and available training support. ☐ Conduct regular alignment checks between certification requirements and job descriptions, ensuring responsibilities match competency expectations. ☐ Enhance documentation on certification exceptions, including justification, associated risks, and approved compensating controls.
2 - <3	☐ Perform a comprehensive assessment of certification gaps across IT, OT, cybersecurity, and third-party staff supporting critical systems. ☐ Implement a formal certification lifecycle, including nomination, training, examination, renewal, and continuous education. ☐ Develop standardized competency matrices and templates for tracking certification status across all departments. ☐ Increase engagement with accredited certification bodies and sector regulators to ensure alignment with national best practices.
3 - <4	☐ Deploy a governance-led certification assurance programme to regularly assess the competence levels of staff supporting critical functions. ☐ Assign certification custodians or champions within each department to monitor compliance and coordinate training needs. ☐ Formalise escalation processes for roles operating with expired or missing mandatory certifications, ensuring timely corrective actions. ☐ Increase oversight on recruitment and role transitions to ensure only certified personnel are appointed to high-risk or regulated functions.
4 - <5	☐ Urgent intervention required! Initiate a rapid organization-wide certification review to identify expired credentials, gaps, or high-risk skill deficiencies. ☐ Establish a temporary governance task force to expedite certification renewals, uplift critical skills, and eliminate outstanding compliance issues. ☐ Implement mandatory reporting by department heads on certification completion rates and pending renewals for staff in critical roles. ☐ Enforce a governance directive restricting assignment of high-privilege or security-sensitive tasks to personnel lacking required certifications.

Also refer to
13.Workforce Management PC11

Notes

RP Score

Checklist to follow

Implementation Control

Governance

0 - <1	☐ Maintain a formally approved asset and inventory management framework governing all IT, OT, data, hardware, and software assets. ☐ Ensure the asset inventory is kept continuously updated, accurately reflecting ownership, location, configuration, and lifecycle status. ☐ Conduct periodic governance reviews to validate completeness, accuracy, and relevance of asset records across all departments. ☐ Maintain high-level dashboards that provide visibility into asset distribution, critical asset status, and associated risks.
1 - <2	☐ Improve asset classification criteria to distinguish critical, sensitive, regulated, and non-critical assets for targeted oversight. ☐ Establish structured communication processes ensuring asset changes, additions, and retirements are promptly reported to governance teams. ☐ Conduct regular alignment checks between asset registers, procurement records, configuration databases, and network scans. ☐ Enhance documentation of asset lifecycle decisions, including justification for classification, retention, disposal, or replacement.
2 - <3	☐ Perform a comprehensive review of current asset management tools and practices to identify gaps in coverage and automation. ☐ Implement a formal asset verification process, including periodic physical audits and automated discovery scans for accuracy validation. ☐ Develop standardized templates for asset recording, classification, tagging, and ownership assignment across the organization. ☐ Increase engagement with industry best practices and NCIIPC recommendations to strengthen asset visibility and control measures.
3 - <4	☐ Deploy a governance-led programme to enforce uniform asset management practices across IT, OT, business units, and remote locations. ☐ Assign asset custodians and owners responsible for maintaining accurate records and ensuring compliance with asset policies. ☐ Formalise escalation workflows for undocumented assets, shadow IT discoveries, or non-compliant asset onboarding activities. ☐ Increase governance oversight on project deployments, ensuring all new assets follow mandatory registration and classification procedures.
4 - <5	☐ Urgent intervention required! Conduct an immediate enterprise-wide asset discovery exercise to identify unrecorded, unmanaged, or high-risk assets. ☐ Establish a cross-functional task force to rectify discrepancies between actual asset inventories and existing records. ☐ Implement mandatory reporting on asset management compliance, including overdue updates, missing tags, or unverified assets. ☐ Enforce a governance directive restricting network connectivity or operational use of any asset not registered and approved within the inventory system.

Also refer to
3.Asset Management IC1

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally approved threat reporting framework that outlines when, how, and to whom cyber incidents must be escalated to government agencies. ☐ Ensure reporting procedures are aligned with NCIIPC, CERT-In, sector regulators, and other mandated authorities. ☐ Conduct periodic governance reviews to validate that reporting timelines, accuracy, and required data fields are consistently met. ☐ Maintain executive dashboards that provide visibility into all government-reported incidents, response timelines, and status of regulatory interactions.
1 - <2	☐ Improve internal processes to ensure early detection, preliminary assessment, and timely escalation of incidents meeting reporting thresholds. ☐ Establish structured communication channels between technical teams, ISD, and compliance units to streamline government reporting workflows. ☐ Conduct regular table-top exercises to validate the readiness of teams responsible for compiling and submitting government-mandated incident reports. ☐ Enhance documentation to include justifications for incidents that were not reported, along with supporting risk-based rationale.
2 - <3	☐ Perform a comprehensive review of previous reporting events to identify delays, inaccuracies, or procedural gaps. ☐ Implement a formal mechanism to classify incidents by severity and determine which ones require mandatory reporting. ☐ Develop standardized templates for incident notification, post-incident reporting, and follow-up compliance submissions. ☐ Increase engagement with government advisories, workshops, and sectoral training to ensure continuous alignment with national reporting expectations.
3 - <4	☐ Deploy a governance-led oversight programme to ensure all security teams understand and follow mandated reporting requirements. ☐ Assign named reporting officers responsible for compiling, validating, and submitting incident details to appropriate government agencies. ☐ Formalise escalation procedures for incidents that show indications of nation-state activity, critical infrastructure impact, or widespread systemic risks. ☐ Increase governance involvement in validating that all relevant logs, artefacts, and evidence are preserved for government review or regulatory audit.
4 - <5	☐ Urgent intervention required! Conduct an immediate review of all open incidents to confirm that no government-reportable events were missed or delayed. ☐ Establish a cross-functional reporting task force to address critical deficiencies and ensure immediate alignment with statutory reporting requirements. ☐ Implement mandatory reporting by all departments on suspicious events, ensuring nothing is filtered out before government-reporting evaluation. ☐ Enforce a governance directive requiring immediate escalation to senior leadership for any incident with potential national or cross-sector impact prior to government notification.

Also refer to
7.Threat Intelligence RA1
15.Situational Awareness RA1

Notes

RP Score

Checklist to follow

Reporting and Accountability

Governance

0 - <1	☐ Maintain a formally approved audit and vulnerability assessment framework that defines scope, frequency, methodology, and reporting requirements. ☐ Ensure periodic internal and external audits are conducted in alignment with regulatory expectations, national guidelines, and organizational risk appetite. ☐ Conduct governance reviews to validate that all identified vulnerabilities, non-conformities, and audit findings are tracked and remediated on time. ☐ Maintain executive dashboards showing audit status, remediation progress, overdue findings, and systemic weaknesses across business units.
1 - <2	☐ Improve audit coverage by including OT, SCADA, cloud, third-party environments, and non-traditional assets within the assessment scope. ☐ Establish structured communication pathways to ensure audit observations are shared with asset owners, risk teams, and technical leads promptly. ☐ Conduct regular reconciliations between vulnerability scans, penetration test results, and risk registers to ensure alignment and closure. ☐ Enhance documentation to include rationales for deferred or accepted risks, along with senior management approval.
2 - <3	☐ Perform a comprehensive review of existing audit methodologies to identify gaps related to tooling, sampling, or technical depth. ☐ Implement a formal risk-based audit planning process that prioritises high-impact systems, regulatory requirements, and emerging risks. ☐ Develop standardized templates, checklists, and reporting formats to ensure consistency and repeatability of audit activities. ☐ Increase engagement with regulatory bodies, CERTs, and industry peer groups to benchmark audit practices and uplift maturity.
3 - <4	☐ Deploy a governance-led enterprise audit assurance programme to monitor audit readiness across IT, OT, cyber, and business processes. ☐ Assign named audit liaisons within departments to coordinate evidence collection, remediation plans, and follow-up activities. ☐ Formalise escalation workflows for critical or overdue audit findings, ensuring prompt attention from senior management. ☐ Increase governance oversight to ensure that remediation efforts are risk-based, adequately resourced, and completed within committed timelines.
4 - <5	☐ Urgent intervention required! Conduct a rapid organization-wide audit to assess systemic weaknesses and identify high-risk vulnerabilities requiring immediate action. ☐ Establish a temporary audit remediation task force to drive accelerated closure of critical findings across technology and business domains. ☐ Implement mandatory reporting by departments on remediation progress, with supporting evidence for each resolved finding. ☐ Enforce a governance directive preventing deployment or continued operation of high-risk systems until critical audit findings are resolved.

Also refer to
 2.Risk Management RA2
 6.Vulnerability and Patch Management RA2
 15.Situational Awareness RA2

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally approved compliance framework that defines how security recommendations from audits, assessments, regulators, and internal reviews must be implemented. ☐ Ensure all security recommendations are logged, categorised by risk, and tracked to closure within defined timelines. ☐ Conduct periodic governance reviews to validate the effectiveness and timeliness of remediation actions taken by responsible teams. ☐ Maintain executive dashboards showing compliance status, overdue recommendations, high-risk gaps, and systemic patterns.
1 - <2	☐ Improve the organization's compliance tracking mechanisms to ensure accurate documentation, ownership clarity, and evidence retention. ☐ Establish structured communication processes ensuring all stakeholders receive clear guidance regarding required corrective actions. ☐ Conduct regular reconciliations between audit observations, vulnerability assessments, incident learnings, and actual remediation activities. ☐ Enhance documentation to include justification for any deferred recommendations or accepted risks approved by senior leadership.
2 - <3	☐ Perform a comprehensive review of existing compliance processes to identify bottlenecks, resource constraints, and repeat findings. ☐ Implement a formal prioritisation framework to ensure high-impact or regulatory-driven recommendations receive immediate attention. ☐ Develop standardised templates for remediation plans, evidence submission, exception requests, and closure verification. ☐ Increase engagement with regulatory bodies, industry peers, and national agencies to benchmark compliance expectations and strengthen alignment.
3 - <4	☐ Deploy a governance-led compliance assurance programme to monitor and validate the effectiveness of remediation actions across the enterprise. ☐ Assign named compliance owners for each major domain (network, OT, applications, cloud, physical security) to ensure accountability. ☐ Formalise escalation processes for overdue, high-risk, or non-implemented recommendations requiring senior management intervention. ☐ Increase governance oversight on major projects and technology deployments to ensure compliance requirements are embedded into project governance.
4 - <5	☐ Urgent intervention required! Conduct a rapid compliance audit to identify unresolved high-risk recommendations that may pose immediate operational or regulatory exposure. ☐ Establish a cross-functional compliance remediation task force to accelerate closure of critical issues and eliminate chronic non-conformities. ☐ Implement mandatory reporting from all departments on the status of open recommendations, supported by verifiable closure evidence. ☐ Enforce a governance directive preventing go-live or continued operation of systems that have outstanding high-risk security recommendations.

Also refer to
2.Risk Management RA3

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Risk Management).
2. Locate the appropriate control within the Risk Management domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

2 Risk Management

RP Score

Checklist to follow

Planning Controls

Risk Management

0 - <1	☐ Maintain a risk-based CII identification framework that explicitly links CII classification criteria to likelihood, impact, and threat scenarios. ☐ Ensure all identified CII assets are reflected in the enterprise risk register with clearly defined risk statements and impact ratings. ☐ Conduct periodic risk reviews to validate that CII classifications remain accurate in light of new threats, vulnerabilities, and business changes. ☐ Maintain risk dashboards that provide visibility into top CII-related risks, including systemic, cascading, and cross-sector exposures.
1 - <2	☐ Improve the CII identification methodology by integrating quantitative and qualitative risk factors such as downtime tolerance, safety impact, and regulatory implications. ☐ Establish structured risk workshops with IT, OT, business, and security teams to jointly assess which assets qualify as CII based on risk criteria. ☐ Conduct regular alignment checks between CII inventories, business impact analyses (BIA), and risk assessments to ensure consistency. ☐ Enhance documentation of CII risk decisions, including rationale for inclusion or exclusion of particular assets from the CII list.
2 - <3	☐ Perform a comprehensive risk review of all major services and processes to identify previously overlooked assets that may warrant CII classification. ☐ Implement a formal risk assessment process triggered by major changes (new systems, integrations, decommissioning) to reassess CII status. ☐ Develop standard risk scoring templates and guidance for teams to consistently evaluate the criticality of assets during CII identification. ☐ Increase use of scenario-based risk analysis (e.g., cascading failures, targeted attacks, supply chain disruptions) to stress-test CII classifications.
3 - <4	☐ Deploy a structured risk management programme focused on CII, ensuring dedicated attention to threats, vulnerabilities, and business impacts associated with these assets. ☐ Assign named risk owners for each CII asset and require them to maintain up-to-date risk profiles, treatment plans, and monitoring activities. ☐ Formalise escalation paths for CII-related risks that exceed defined risk appetite thresholds, ensuring rapid management attention. ☐ Increase integration between risk management, incident response, and business continuity teams to ensure CII identification informs planning and response strategies.
4 - <5	☐ Urgent intervention required! Conduct an immediate risk-led review of all critical services to confirm that CII assets are correctly identified and risk-rated. ☐ Establish a cross-functional risk task force to rapidly address gaps in CII identification, risk documentation, and ownership. ☐ Implement mandatory risk reporting from all departments supporting critical services to capture potential CII candidates and associated risk concerns. ☐ Enforce a directive that no high-impact asset may be excluded from CII consideration until a documented risk assessment is performed and approved.

Also refer to
1.Governance PC1
3.Asset Management PC1

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a risk-based interdependency mapping framework that documents how failures in one system, service, or provider may impact others. ☐ Ensure all critical interdependencies- internal and external are reflected in the enterprise risk register with appropriate impact assessments. ☐ Conduct periodic risk reviews to validate that vertical (organizational hierarchy) and horizontal (cross-functional) dependencies remain accurate and current. ☐ Maintain risk dashboards that highlight high-risk dependency clusters, single points of failure, and potential cascading failure paths.
1 - <2	☐ Improve interdependency identification by incorporating threat modelling, operational impact analysis, and multi-level failure scenarios. ☐ Establish structured risk workshops to collaboratively analyse interdependencies across business units, IT, OT, vendors, and upstream/downstream partners. ☐ Conduct alignment checks between interdependency maps, business impact analyses, and continuity plans to ensure unified understanding of risk. ☐ Enhance documentation to include rationale for classifying certain dependencies as critical, moderate, or non-critical.
2 - <3	☐ Perform a comprehensive risk assessment of all upstream and downstream services to identify hidden or emerging interdependencies. ☐ Implement a formal method to calculate and score dependency risks, including likelihood of disruption and severity of cascading impacts. ☐ Develop standard templates for capturing dependency relationships, risk ownership, and mitigation strategies. ☐ Increase integration of interdependency risks into organizational risk modelling, simulations, and resilience exercises.
3 - <4	☐ Deploy a risk-led programme to systematically analyse and monitor dependency risk across critical processes and infrastructures. ☐ Assign dependency risk owners responsible for maintaining updated risk information and leading mitigation initiatives. ☐ Formalise escalation procedures for high-impact dependency risks, including failures that affect multiple business lines or sectors. ☐ Increase risk oversight on new projects and integrations to ensure interdependencies are identified, assessed, and addressed during design and rollout.
4 - <5	☐ Urgent intervention required! Conduct an immediate review of all critical services to identify dependency risks that may cause cascading or systemic failures. ☐ Establish a cross-functional working group to rectify gaps in dependency documentation, risk scoring, and mitigation plans. ☐ Implement mandatory reporting from departments on changes in processes, technology, or vendor usage that may alter dependency risk profiles. ☐ Enforce a directive preventing deployment of new systems or services without thorough dependency risk assessment and approval.

Also refer to
 1.Governance PC2
 7.Threat Intelligence PC2
 9.Resilience Management PC2
 15.Situational Awareness PC2

Notes

RP Score

Checklist to follow

Planning Controls

Risk Management

0 - <1	☐ Maintain a formal VTR assessment framework defining how vulnerabilities, threats, and risks are identified, analysed, and prioritised across all environments. ☐ Ensure all high-risk vulnerabilities, threat scenarios, and risk exposures are captured in the enterprise risk register with assigned owners and treatment plans. ☐ Conduct periodic VTR reviews to validate that assessments reflect current threat intelligence, system changes, and operational realities. ☐ Maintain risk dashboards that highlight top vulnerabilities, threat vectors, emerging risks, and systemic weaknesses requiring management attention.
1 - <2	☐ Improve VTR methodologies by integrating quantitative scoring models, business impact ratings, and threat likelihood estimations. ☐ Establish structured VTR workshops involving IT, OT, security, business, and risk teams to ensure holistic assessment of exposures. ☐ Conduct alignment checks between VTR results, penetration testing findings, vulnerability scans, and incident trends to ensure completeness. ☐ Enhance documentation for all VTR outcomes, including justification for accepted risks or deferred remediation actions.
2 - <3	☐ Perform comprehensive enterprise-wide VTR assessments to identify previously unrecognised risks across applications, infrastructure, and third parties. ☐ Implement a formal risk treatment process that mandates prioritised mitigation plans, timelines, resource allocation, and closure verification. ☐ Develop standard templates and reporting formats for VTR analysis, ensuring consistency and comparability across business units. ☐ Increase integration of VTR results into strategic planning, procurement decisions, technology roadmaps, and architectural reviews.
3 - <4	☐ Deploy a risk-led programme dedicated to continuous identification and remediation of risks tied to critical systems and processes. ☐ Assign VTR owners for major risk categories (cyber, operational, third-party, physical) to ensure sustained oversight and accountability. ☐ Formalise escalation processes for risks exceeding defined appetite levels, ensuring timely intervention by senior management. ☐ Increase oversight to ensure that mitigation actions are realistic, funded, properly sequenced, and aligned with business priorities.
4 - <5	☐ Urgent intervention required! Conduct a rapid organization-wide VTR assessment to identify critical risks requiring immediate remediation. ☐ Establish a temporary VTR response task force to accelerate resolution of high-risk vulnerabilities, threats, and systemic issues. ☐ Implement mandatory reporting from all departments summarising new threats, discovered vulnerabilities, or changes in risk conditions. ☐ Enforce a directive that no high-risk vulnerability or threat may remain unmitigated beyond defined timelines without formal risk acceptance.

Also refer to
6.Vulnerability and Patch Management PC6

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally defined redundancy strategy that identifies critical systems requiring failover, backups, or alternate processing capabilities based on risk impact. ☐ Ensure redundancy requirements are documented in the enterprise risk register with clear linkages to business impact, threat scenarios, and downtime tolerances. ☐ Conduct periodic risk reviews to validate that redundancy mechanisms remain aligned with current system architecture and operational dependencies. ☐ Maintain dashboards highlighting redundancy coverage, single points of failure, high-risk assets lacking failover, and related mitigation plans.
1 - <2	☐ Improve redundancy planning by incorporating quantitative risk metrics such as RTO/ RPO, failure likelihood, and cascading failure potential. ☐ Establish structured workshops between IT, OT, business continuity, and risk teams to evaluate redundancy requirements for critical services. ☐ Conduct alignment checks between redundancy controls, business continuity plans, disaster recovery strategies, and operational resilience assessments. ☐ Enhance documentation for redundancy decisions, including justification for systems where redundancy is not implemented due to cost, feasibility, or accepted risk.
2 - <3	☐ Perform a comprehensive assessment of critical systems to identify gaps in redundancy, including network, power, storage, and application layers. ☐ Implement a formal testing schedule for redundancy mechanisms (failover, replication, clustering) to validate their effectiveness under realistic scenarios. ☐ Develop standardized templates for capturing redundancy architecture, dependencies, and risk treatment actions. ☐ Increase integration of redundancy considerations into architectural reviews, procurement frameworks, and project governance.
3 - <4	☐ Deploy a risk-led resilience improvement programme targeting high-risk areas with insufficient redundancy or outdated failover configurations. ☐ Assign redundancy risk owners responsible for maintaining visibility into system performance, failover readiness, and required improvements. ☐ Formalise escalation procedures for redundancy failures, near misses, or test results indicating significant risk exposure. ☐ Increase oversight to ensure redundancy enhancement projects are adequately funded, prioritised, and tracked through closure.
4 - <5	☐ Urgent intervention required! Conduct an immediate redundancy risk assessment to identify critical systems operating with single points of failure. ☐ Establish a cross-functional task force to accelerate remediation of redundancy gaps and reduce systemic outage risks. ☐ Implement mandatory reporting on redundancy test results, failure rates, unresolved issues, and upcoming risks affecting critical operations. ☐ Enforce a directive that systems classified as critical may not operate in production without validated and tested redundancy in place or formally accepted residual risk.

Also refer to
5.Secure Design and Engineering PC8
9.Resilience Management PC8

Notes

RP Score

Checklist to follow

Operational Control

Risk Management

0 - <1	☐ Maintain a formal Data Loss Prevention (DLP) framework that identifies sensitive data types, associated risks, and required preventive controls across the organization. ☐ Ensure all critical data flows- internal, external, cloud, endpoint, and OT are documented and assessed for data loss risk exposure. ☐ Conduct periodic risk reviews to validate that DLP configurations, rules, and monitoring thresholds reflect current business processes and evolving threats. ☐ Maintain dashboards providing visibility into data leakage attempts, policy violations, high-risk channels, and unresolved DLP incidents.
1 - <2	☐ Improve the DLP risk model by integrating data classification, threat intelligence, and business impact ratings into rule creation and tuning. ☐ Establish structured reviews between security, legal, risk, and business teams to regularly refine DLP policies and handling procedures. ☐ Conduct regular alignment checks between DLP alerts, incident response logs, and risk registers to ensure accurate reflection of data-related risks. ☐ Enhance documentation of data loss incidents, including root-cause analysis, remediation actions, and risk acceptance decisions where applicable.
2 - <3	☐ Perform a comprehensive data inventory and mapping exercise to identify previously unknown or unprotected data repositories. ☐ Implement a formal process to periodically test and validate the effectiveness of DLP controls across email, endpoints, cloud services, and network channels. ☐ Develop standardised templates and procedures for data classification, handling, and exception requests to reduce ambiguity and enforce consistency. ☐ Increase integration of DLP insights with enterprise risk management to strengthen visibility of systemic or persistent data leakage patterns.
3 - <4	☐ Deploy a risk-led programme targeting high-risk areas such as privileged users, external transfers, legacy applications, and unmanaged storage locations. ☐ Assign data owners and risk custodians responsible for monitoring DLP risks within their departments and ensuring timely remediation. ☐ Formalise escalation workflows for high-severity or repeated DLP alerts, ensuring rapid intervention by senior management and risk teams. ☐ Increase oversight to ensure access rights, encryption controls, and endpoint protections correlate with the level of data sensitivity identified in risk assessments.
4 - <5	☐ Urgent intervention required! Conduct an immediate review of all critical data flows to identify severe data loss exposures requiring rapid mitigation. ☐ Establish a dedicated DLP risk task force to close urgent gaps, refine detection logic, and coordinate remediation activities across departments. ☐ Implement mandatory reporting from all business units on data movement practices, exceptions, and emerging data risks. ☐ Enforce a directive prohibiting storage, transfer, or processing of sensitive data outside approved, monitored, and risk-assessed environments.

Also refer to
11.Data Protection OC4

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formal penetration testing framework defining scope, frequency, methodologies, and risk-based prioritisation for all critical systems. ☐ Ensure results of penetration tests are recorded in the enterprise risk register with clear risk ratings, root causes, and required treatments. ☐ Conduct periodic risk reviews to validate that remediation of identified vulnerabilities is completed within approved timelines. ☐ Maintain dashboards showing test coverage, severity trends, unresolved findings, and high-risk systems requiring urgent attention.
1 - <2	☐ Improve test scoping by integrating threat modelling, business impact analysis, and emerging risk intelligence into penetration test planning. ☐ Establish structured collaboration between testers, system owners, and risk teams to ensure findings are clearly understood and risk-rated. ☐ Conduct alignment checks between penetration test findings, vulnerability scans, and incident response data to identify recurring or systemic risks. ☐ Enhance documentation of penetration test outcomes, including justification for accepted risks or deferred remediation actions.
2 - <3	☐ Perform a comprehensive penetration testing programme covering IT, OT, cloud, APIs, network, identity systems, and third-party environments. ☐ Implement a formal remediation lifecycle process ensuring all findings have treatment plans, owners, timelines, and confirmation of closure. ☐ Develop standardised templates for reporting test results, risk scoring, remediation tracking, and management summaries. ☐ Increase integration of penetration test results into architectural reviews, technology upgrades, and security control enhancements.
3 - <4	☐ Deploy a risk-driven improvement programme to address persistent weaknesses identified across multiple penetration testing cycles. ☐ Assign remediation owners for each high-risk finding and ensure accountability for timely mitigation. ☐ Formalise escalation workflows for critical findings that pose significant operational, safety, or regulatory risks if left unaddressed. ☐ Increase risk oversight to ensure penetration testing is conducted before major releases, infrastructure upgrades, and integration projects.
4 - <5	☐ Urgent intervention required! Perform an accelerated penetration test cycle focused on high-risk areas where vulnerabilities may already be exploited. ☐ Establish a cross-functional remediation task force to rapidly close high-risk findings and coordinate technical and governance responses. ☐ Implement mandatory reporting from system owners on progress toward closure of penetration test findings, with evidence-based verification. ☐ Enforce a directive preventing go-live, integration, or continued operation of systems until critical penetration test findings are resolved or formally risk-accepted.

Operational Control

Risk Management

Also refer to
6.Vulnerability and Patch Management OC5

Notes

RP Score

Checklist to follow

Disaster Recovery/ Business

Risk Management

0 - <1	☐ Maintain a formally approved contingency planning framework that defines response, continuity, and graceful degradation requirements for all critical services. ☐ Ensure all contingency plans are risk-based and aligned with business impact analyses, downtime tolerances, and threat scenarios. ☐ Conduct periodic risk reviews to validate that contingency plans remain relevant in light of new technologies, changes in business processes, and emerging threats. ☐ Maintain dashboards showing continuity readiness, plan coverage, high-risk gaps, test results, and areas requiring immediate management attention.
1 - <2	☐ Improve contingency planning by integrating quantitative risk measures such as maximum tolerable downtime, redundancy levels, and dependency risks. ☐ Establish structured planning workshops with IT, OT, operations, risk, and business units to collaboratively refine contingency strategies. ☐ Conduct alignment checks between contingency plans, disaster recovery procedures, redundancy controls, and crisis management processes. ☐ Enhance documentation for all contingency plans, including detailed roles, communication structures, fallback procedures, and recovery prioritisation logic.
2 - <3	☐ Perform comprehensive end-to-end contingency planning across critical processes to identify single points of failure or unrealistic assumptions. ☐ Implement a formal testing cycle for contingency plans through simulations, tabletop exercises, and controlled failover drills. ☐ Develop standard templates for scenario planning, plan activation criteria, escalation steps, and restoration sequencing. ☐ Increase integration between contingency planning and enterprise risk management to ensure risk insights guide plan maturity and investments.
3 - <4	☐ Deploy a risk-led resilience improvement programme targeting weak areas identified in continuity tests or prior incidents. ☐ Assign contingency plan owners responsible for ensuring accuracy, readiness, and periodic testing of their respective plans. ☐ Formalise escalation workflows for deviations in plan execution, missed recovery objectives, or critical gaps discovered during exercises. ☐ Increase governance oversight to ensure contingency planning is embedded into all transformation projects, major changes, and new system deployments.
4 - <5	☐ Urgent intervention required! Conduct an immediate organization-wide contingency review to identify high-risk services lacking adequate fallback or graceful degradation capability. ☐ Establish a cross-functional resilience task force to rapidly rectify gaps in continuity planning, failover design, and operational readiness. ☐ Implement mandatory reporting from business units detailing readiness status, exercise results, and outstanding risks impacting continuity. ☐ Enforce a directive preventing operation of critical services without validated contingency plans that meet organizational risk appetite and regulatory expectations.

Also refer to
9.Resilience Management DR1

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a risk-driven audit and vulnerability assessment programme that prioritises systems based on threat exposure, business impact, and likelihood of exploitation. ☐ Ensure audit and vulnerability assessment outcomes are formally integrated into the enterprise risk register with clear severity ratings and mitigation requirements. ☐ Conduct periodic risk reviews to evaluate whether audit findings materially change the organization's risk profile or exceed risk appetite thresholds. ☐ Maintain dashboards highlighting high-risk findings, systemic weaknesses, recurring vulnerabilities, and areas of elevated exposure.
1 - <2	☐ Improve audit scoping by aligning assessments with threat intelligence, recent incidents, and adversary techniques relevant to the organization. ☐ Establish structured risk assessment workshops to jointly analyse audit findings, their root causes, and potential cascading impacts. ☐ Conduct alignment checks to ensure audit results, penetration test findings, red-team observations, and vulnerability scan results reflect a unified risk perspective. ☐ Enhance documentation to include clear risk justification for findings that are deferred, partially remediated, or accepted as residual risk.
2 - <3	☐ Perform comprehensive thematic audits (e.g., identity, OT, cloud, network segmentation) to identify systemic risks across technology domains. ☐ Implement risk-based remediation plans that clearly define timelines, prioritisation, compensating controls, and dependencies for closure. ☐ Develop standardised templates for risk scoring, mitigation planning, and reporting of audit observations to ensure consistent risk evaluation. ☐ Increase integration of audit and VAPT insights into risk forecasting, scenario analysis, and stress testing exercises.
3 - <4	☐ Deploy a risk-led improvement programme targeting chronic or repeated audit issues that signal structural or cultural weaknesses. ☐ Assign risk owners for major audit categories (such as configuration management, identity security, network controls) to ensure accountability. ☐ Formalise escalation workflows for findings classified as high or critical, requiring attention at risk committee or executive level. ☐ Increase oversight to ensure that remediation activities address root causes rather than only technical symptoms.
4 - <5	☐ Urgent intervention required! Conduct an accelerated audit cycle for high-risk systems where vulnerabilities may present immediate exploitation risk. ☐ Establish a cross-functional mitigation task force to coordinate rapid closure of severe findings with risk, security, IT, and OT stakeholders. ☐ Implement mandatory reporting by all system owners on remediation status, newly discovered risks, and emerging vulnerabilities. ☐ Enforce a directive prohibiting the operation of critical systems that retain unresolved high-risk audit findings beyond risk appetite thresholds.

Also refer to
 1.Governance RA2
 6.Vulnerability and Patch Management RA2
 15.Situational Awareness RA2

Notes

RP Score

Checklist to follow

Reporting and Accountability

Risk Management

0 - <1	☐ Maintain a risk-based compliance framework ensuring all security recommendations are evaluated for their impact on organizational risk exposure. ☐ Ensure remediation requirements from audits, VAPT, incidents, and assessments are captured in the enterprise risk register with appropriate risk ratings. ☐ Conduct periodic risk reviews to validate whether delayed or incomplete remediation increases residual risk beyond tolerance levels. ☐ Maintain dashboards highlighting outstanding high-risk remediation items, systemic weaknesses, and risk trends requiring executive attention.
1 - <2	☐ Improve the risk evaluation of recommendations by incorporating threat likelihood, business impact, exploitation feasibility, and compensating controls. ☐ Establish structured risk workshops to prioritise recommendations based on measurable risk reduction rather than operational convenience. ☐ Conduct alignment checks between risk registers, remediation plans, incident lessons, and audit findings to ensure consistent risk treatment. ☐ Enhance documentation of risk acceptance decisions, ensuring justification, compensatory measures, and approval are formally recorded.
2 - <3	☐ Perform comprehensive reviews to identify repeated or chronic non-compliance cases that indicate deeper risk governance issues. ☐ Implement a formal risk-based prioritisation model to ensure high-impact deficiencies are remediated before moderate or low-risk issues. ☐ Develop standardized templates for risk treatment plans that articulate action owners, timelines, required resources, and residual risk. ☐ Increase integration of compliance findings into risk forecasting, scenario analysis, and long-term resilience planning.
3 - <4	☐ Deploy a risk-led improvement programme focused on reducing exposure from long-pending recommendations and high-risk technical debt. ☐ Assign risk custodians responsible for tracking remediation progress and ensuring closure of high-risk recommendations. ☐ Formalise escalation routes for overdue high-severity recommendations requiring intervention from senior management or the risk committee. ☐ Increase oversight to ensure remediation actions address underlying risk drivers (e.g., process gaps, architectural flaws) rather than superficial fixes.
4 - <5	☐ Urgent intervention required! Conduct a rapid review of all critical open recommendations to quantify accumulated risk and prioritise immediate actions. ☐ Establish a cross-functional remediation council to drive rapid closure of severe issues spanning multiple departments or technology domains. ☐ Implement mandatory reporting from business and technical owners detailing progress, obstacles, and updated risk assessments for open findings. ☐ Enforce a directive preventing the continued operation or deployment of high-risk systems until all critical security recommendations have been remediated or formally risk-accepted.

Also refer to
1.Governance RA3

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Asset Management).
2. Locate the appropriate control within the Asset Management domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

3 Asset Management

RP Score

Checklist to follow

Planning Controls

Asset Management

0 - <1	☐ Maintain a centralised inventory that links all CII assets to business processes, functions, and dependencies. ☐ Ensure CII-designated assets are clearly tagged and identifiable within asset management systems. ☐ Conduct periodic reviews to confirm that asset classifications accurately reflect evolving criticality and operational importance. ☐ Maintain dashboards showcasing asset criticality levels, ownership, lifecycle status, and associated risks.
1 - <2	☐ Improve CII asset categorisation by incorporating technical, operational, and environmental sensitivity criteria. ☐ Establish structured processes for reporting new assets or changes affecting CII designation. ☐ Conduct reconciliation between CII lists, configuration repositories, procurement data, and CMDB entries. ☐ Enhance documentation on rationale for asset inclusion or exclusion from the CII inventory.
2 - <3	☐ Perform end-to-end assessments across business units to identify previously unclassified CII-related assets. ☐ Implement mandatory CII tagging and asset registration during procurement, deployment, and commissioning stages. ☐ Develop standard templates for recording asset details, operational dependencies, and criticality assessments. ☐ Increase alignment between CII identification and asset lifecycle management, including maintenance and retirement.
3 - <4	☐ Deploy systematic reviews to validate asset ownership, ensuring accountability for CII stewardship. ☐ Assign CII custodians responsible for ensuring inventory accuracy and asset readiness. ☐ Formalise escalation when discrepancies or undocumented CII assets are discovered. ☐ Increase oversight on asset onboarding to ensure all CII candidates undergo criticality assessment before activation.
4 - <5	☐ Urgent intervention required! Conduct a rapid CII asset discovery to identify unmanaged or undocumented critical assets. ☐ Establish a cross-functional team to rectify inaccuracies in CII asset records. ☐ Implement mandatory reporting from all departments on changes affecting CII-related assets. ☐ Enforce a directive preventing activation of any asset supporting CII functions until it is fully registered and risk-assessed.

Also refer to
1.Governance PC1
2.Risk Management PC1

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a centralised, continuously updated inventory for all IT, OT, data, and physical assets supporting critical operations. ☐ Ensure all assets have unique identifiers, ownership assignments, and lifecycle metadata recorded in the inventory system. ☐ Conduct periodic asset verification exercises to validate physical presence, configuration, and operational accuracy. ☐ Maintain dashboards showing asset distribution, ageing, utilisation, and discrepancies across departments.
1 - <2	☐ Improve asset discovery through automated scanning tools, endpoint management systems, and network mapping. ☐ Establish strict processes requiring new assets to be registered prior to deployment into any operational environment. ☐ Conduct alignment checks between inventory records, procurement systems, maintenance logs, and disposal records. ☐ Enhance documentation for asset ownership transfers, configuration changes, and operational handovers.
2 - <3	☐ Perform full asset reconciliation across locations and business units to identify unauthorised or unmanaged assets. ☐ Implement continuous monitoring of asset status, warranty, compliance, and update requirements. ☐ Develop standard templates for asset tagging, metadata recording, and lifecycle documentation. ☐ Increase integration of asset intelligence with risk, security operations, and business continuity planning.
3 - <4	☐ Deploy an asset assurance programme to verify completeness, accuracy, and currency of records. ☐ Assign asset custodians responsible for ensuring data accuracy and timely updates. ☐ Formalise escalation workflows for missing assets, unregistered equipment, or policy violations. ☐ Increase oversight on asset retirement, ensuring secure decommissioning and record updates.
4 - <5	☐ Urgent intervention required! Conduct a rapid enterprise-wide asset audit to identify high-risk gaps in visibility. ☐ Establish a remediation task force to correct inaccurate inventory data and implement stronger controls. ☐ Implement mandatory reporting on asset status, untagged assets, and unresolved discrepancies. ☐ Enforce a directive that no asset may join the network or OT environment unless it is inventoried, tagged, and approved.

Also refer to
1.Governance IC1

Notes

RP Score

Checklist to follow

Operational Control

Asset Management

0 - <1	☐ Maintain operational processes that ensure all critical assets are consistently tracked throughout their lifecycle. ☐ Ensure operational teams update asset records when assets are moved, reconfigured, or serviced. ☐ Conduct routine physical inspections to confirm accuracy of operational asset records. ☐ Maintain dashboards that track asset health, maintenance schedules, incidents, and operational dependencies.
1 - <2	☐ Improve asset monitoring by integrating telemetry, SNMP data, OT logs, and endpoint metrics into inventory systems. ☐ Establish structured handover processes between operations, maintenance, and security teams when asset changes occur. ☐ Conduct reconciliations between operational logs, maintenance updates, and inventory systems to detect mismatches. ☐ Enhance documentation capturing operational usage, criticality, and dependency relationships.
2 - <3	☐ Perform operational sweeps to identify unmonitored, misconfigured, or obsolete assets. ☐ Implement automated monitoring for asset lifecycle stages such as warranty expiry, patch requirements, and performance degradation. ☐ Develop standard templates for operational asset reporting, maintenance tasks, and issue tracking. ☐ Increase integration between operations, security, and risk teams to ensure asset status informs risk posture.
3 - <4	☐ Deploy an operational improvement programme focused on reducing asset-related incidents and manual tracking errors. ☐ Assign operational asset stewards responsible for continuity of data updates and maintenance coordination. ☐ Formalise escalation pathways for operational failures caused by unmanaged or outdated assets. ☐ Increase oversight on vendor-managed assets to ensure updates, maintenance, and service tasks are properly documented.
4 - <5	☐ Urgent intervention required! Conduct a rapid operational asset review to identify devices posing immediate reliability or security risks. ☐ Establish an operations-led task force to address high-priority asset issues and enforce corrective actions. ☐ Implement mandatory reporting of asset failures, anomalies, and irregularities affecting operational availability. ☐ Enforce a directive prohibiting operational use of any asset until it is fully documented, updated, and monitored.

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a secure disposal and transfer framework defining how all critical information-bearing assets must be sanitised, wiped, destroyed, or transferred. ☐ Ensure all critical media movements internal or external are logged, tracked, and risk-evaluated. ☐ Conduct periodic reviews to confirm disposal processes align with regulatory and organizational security requirements. ☐ Maintain dashboards tracking outstanding disposals, pending sanitisation tasks, and high-risk transfer events.
1 - <2	☐ Improve sanitisation procedures by adopting certified tools, forensic wiping standards, and chain-of-custody controls. ☐ Establish structured processes for evaluating disposal risks based on asset sensitivity and data criticality. ☐ Conduct reconciliations between disposal logs, inventory records, and physical audits to ensure no untracked media exists. ☐ Enhance documentation capturing disposal decisions, authorisations, and verification of sanitisation.
2 - <3	☐ Perform comprehensive disposal audits to identify gaps, improper handling, or unverified destruction events. ☐ Implement mandatory data sanitisation for all decommissioned assets prior to physical removal or reuse. ☐ Develop standardized templates for documenting wiping, degaussing, shredding, or controlled destruction. ☐ Increase integration between disposal processes and asset lifecycle workflows to ensure timely updates in inventory systems.
3 - <4	☐ Deploy a risk-led disposal assurance programme targeting high-sensitivity or high-volume disposal operations. ☐ Assign disposal custodians responsible for verifying completion and ensuring proper evidentiary documentation. ☐ Formalise escalation procedures for missing media, failed destruction attempts, or chain-of-custody deviations. ☐ Increase oversight on third-party vendors performing destruction, ensuring compliance with contractual and security obligations.
4 - <5	☐ Urgent intervention required! Initiate a rapid sweep to identify unaccounted-for storage media or improperly stored retired assets. ☐ Establish a remediation task force to correct gaps in disposal processes and strengthen controls. ☐ Implement mandatory reporting from departments on disposal volumes, risks, and outstanding items requiring review. ☐ Enforce a directive prohibiting disposal or transfer of information-bearing assets without documented sanitisation and inventory closure.

Operational Control

Asset Management

Also refer to
11.Data Protection OC9

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Identity and Access Management).
2. Locate the appropriate control within the Identity and Access Management domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

4 Identity and Access Management

4 Access Control and Identity management

IC2

RP Score

Checklist to follow

Implementation Control

Access Control and Identity management

0 - <1	☐ Maintain a formally approved access control framework defining role-based, least privilege, and segregation-of-duty requirements for all systems. ☐ Ensure all access rights are mapped to documented roles, responsibilities, and job functions. ☐ Conduct periodic access reviews to validate that privileges align with current job requirements. ☐ Maintain dashboards highlighting privilege distribution, high-privilege accounts, and outstanding access discrepancies.
1 - <2	☐ Improve access definitions by incorporating business impact, data sensitivity, and operational risk criteria. ☐ Establish structured workflows for access provisioning, modification, suspension, and revocation. ☐ Conduct alignment checks between HR records, system accounts, and access control lists to detect inconsistencies. ☐ Enhance documentation for justification of elevated access or temporary privilege grants.
2 - <3	☐ Perform comprehensive access audits across IT, OT, applications, cloud platforms, and third-party environments. ☐ Implement automated tools to monitor permissions, detect anomalies, and flag privilege creep. ☐ Develop standard templates for role definitions, access request forms, and approval routes. ☐ Increase integration between access management and identity lifecycle processes to ensure real-time updates.
3 - <4	☐ Deploy a privilege reduction programme targeting unused, excessive, or outdated permissions. ☐ Assign access custodians responsible for reviewing and validating entitlements within their domains. ☐ Formalise escalation workflows for high-risk access deviations or inappropriate privilege assignments. ☐ Increase oversight of privileged access, ensuring PAM controls are enforced for all critical operations.
4 - <5	☐ Urgent intervention required! Conduct an accelerated organization-wide access review to identify and remove high-risk entitlements. ☐ Establish a remediation task force to resolve privilege gaps, enforce role cleanliness, and improve approval discipline. ☐ Implement mandatory reporting on access violations, privilege escalations, and non-compliant access changes. ☐ Enforce a directive preventing system access until appropriate role assignment, approval, and verification are complete.

Notes

4 Access Control and Identity management

IC3

RP Score

Checklist to follow

0 - <1	☐ Maintain a formal authentication framework defining identity verification, password hygiene, MFA requirements, and account lifecycle policies. ☐ Ensure all users including IT, OT, third-parties, and vendors are uniquely identified and authenticated before accessing any system. ☐ Conduct periodic authentication reviews to validate compliance with MFA, password controls, and authentication strength requirements. ☐ Maintain dashboards tracking authentication failures, lockouts, misuse patterns, and high-risk login attempts.
1 - <2	☐ Improve authentication mechanisms by incorporating adaptive risk scoring, behavioural indicators, and device context. ☐ Establish structured processes for issuing, updating, and revoking digital identities, including emergency access. ☐ Conduct alignment checks between identity sources, authentication logs, and access control systems to identify discrepancies. ☐ Enhance documentation for privileged identity issuance, including justification, approval lineage, and validity duration.
2 - <3	☐ Perform comprehensive authentication assessments on all internal, cloud, and OT systems to identify weak or legacy authentication points. ☐ Implement strong MFA controls for all privileged accounts and high-risk applications. ☐ Develop standard identity issuance templates covering identity proofing, onboarding, offboarding, and credential renewal. ☐ Increase integration between authentication systems, SIEM, and monitoring tools to detect anomalous authentication behaviour.
3 - <4	☐ Deploy a risk-based identity monitoring programme to identify suspicious activity and automate protective responses. ☐ Assign identity custodians responsible for validating identity accuracy, lifecycle updates, and credential hygiene. ☐ Formalise escalation workflows for compromised accounts, unusual login patterns, or authentication bypass attempts. ☐ Increase enforcement of password policies, credential rotation, and secure authentication protocols.
4 - <5	☐ Urgent intervention required! Conduct an immediate identity and credential audit to detect disabled, stale, or unauthorized accounts. ☐ Establish a remediation working group to improve authentication coverage, update outdated mechanisms, and remove weak credentials. ☐ Implement mandatory reporting for identity exceptions, unmanaged accounts, and authentication anomalies. ☐ Enforce a directive restricting access to any system where authentication does not meet the organization's minimum security standard.

Implementation Control

Access Control and Identity management

Notes

4 Access Control and Identity management

OC10

RP Score

Checklist to follow

Operational Control

Access Control and Identity management

0 - <1	☐ Maintain a secure intranet access framework defining user groups, viewing permissions, editing rights, and restricted sections. ☐ Ensure segregation of intranet roles is enforced based on principle of least privilege and business relevance. ☐ Conduct periodic access reviews to confirm intranet privileges match current job responsibilities. ☐ Maintain dashboards tracking intranet usage, access anomalies, and restricted-content violations.
1 - <2	☐ Improve intranet security by implementing data sensitivity classifications and access tiers. ☐ Establish structured workflows for publishing, modifying, or retiring intranet content to prevent exposure of sensitive information. ☐ Conduct reconciliation between intranet users, AD groups, and role-based access models to detect misalignments. ☐ Enhance documentation for restricted areas, justification for special access, and retention of audit logs.
2 - <3	☐ Perform comprehensive intranet security assessments to identify weak access points, misconfigurations, or outdated permissions. ☐ Implement encryption for sensitive intranet content and enforce HTTPS across all internal sites. ☐ Develop standard content governance templates ensuring proper tagging, approval, review, and archival. ☐ Increase integration between intranet access logs, SIEM, and monitoring systems to detect unusual patterns.
3 - <4	☐ Deploy an intranet hardening programme addressing patching, plugin risks, legacy applications, and misconfigured repositories. ☐ Assign intranet administrators responsible for maintaining access models and monitoring sensitive content areas. ☐ Formalise escalation workflows for detected policy violations or unauthorised access attempts on restricted content. ☐ Increase oversight of third-party and contractor access to ensure intranet exposure is minimised and monitored.
4 - <5	☐ Urgent intervention required! Initiate a rapid intranet privilege review to identify high-risk or outdated access privileges. ☐ Establish a remediation team to correct misconfigurations, remove stale content, and update access control models. ☐ Implement mandatory reporting on intranet content risks, user access anomalies, and security exceptions. ☐ Enforce a directive preventing publication or hosting of sensitive content on intranet sections without explicit approval and access control validation.

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Secure Design and Engineering).
2. Locate the appropriate control within the Situational Awareness domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

5 Secure Design and Engineering

RP Score		Checklist to follow
Planning Controls	0 - <1	☐ Maintain a formally approved integration framework defining how IT, OT, SCADA, and cybersecurity components must interoperate securely. ☐ Ensure all integrations follow secure design principles, including network segmentation, least privilege, and authenticated interfaces. ☐ Conduct periodic design reviews to validate that newly integrated systems comply with architectural and cybersecurity baseline requirements. ☐ Maintain dashboards tracking integration points, data flows, trust boundaries, and associated design risks.
	1 - <2	☐ Improve integration requirements by incorporating threat modelling, dependency mapping, and compatibility checks early in the design phase. ☐ Establish structured workflows requiring security review and approval before any IT-OT or system-to-system integration is implemented. ☐ Conduct alignment checks between integration diagrams, configuration records, and actual deployed architecture to identify deviations. ☐ Enhance documentation for all integration touchpoints, including protocols used, authentication methods, and expected data exchanges.
	2 - <3	☐ Perform comprehensive reviews of legacy integrations to identify insecure interfaces, unsupported protocols, or undocumented connections. ☐ Implement a formal change impact analysis process to evaluate integration risks during upgrades, replacements, or new deployments. ☐ Develop standard templates for integration design, data flow diagrams, and interconnection security requirements. ☐ Increase incorporation of security controls such as encryption, mutual authentication, logging, and whitelisting at all integration boundaries.
	3 - <4	☐ Deploy a secure integration programme to identify redundant connections, reduce attack surfaces, and strengthen architectural hygiene. ☐ Assign integration owners responsible for maintaining documentation, ensuring compliance, and overseeing lifecycle changes. ☐ Formalise escalation workflows for integration failures, insecure connections, or deviations from approved design patterns. ☐ Increase oversight on vendor-provided integrations to ensure configurations, drivers, and protocols comply with security and interoperability requirements.
	4 - <5	☐ Urgent intervention required! Conduct an immediate assessment of all IT-OT integration points to identify high-risk or unmonitored communication paths. ☐ Establish a cross-functional integration task force to rapidly rectify insecure interfaces and enforce robust design controls. ☐ Implement mandatory reporting of new or modified integrations, ensuring each is risk-assessed, documented, and approved before activation. ☐ Enforce a directive prohibiting the deployment of any integration- IT, OT, cloud, or vendor-provided without a validated secure design review and explicit approval.

Also refer to
14.Change Management PC5

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally approved enterprise security architecture framework defining principles, patterns, and control requirements for all technology environments. ☐ Ensure architectural designs document trust boundaries, data flows, authentication points, and security control placement. ☐ Conduct periodic architecture reviews to validate alignment between deployed systems and approved security design baselines. ☐ Maintain architectural dashboards highlighting deviations, exceptions, risk concentrations, and control coverage across environments.
1 - <2	☐ Improve architectural models by incorporating threat modelling, adversary techniques, and attack surface analysis into design decisions. ☐ Establish structured workflows ensuring all new deployments, integrations, and significant changes undergo mandatory security architecture approval. ☐ Conduct reconciliation checks between architecture diagrams, configuration repositories, and actual system configurations to detect drift. ☐ Enhance documentation for architectural exceptions, including justification, compensating controls, and approved validity periods.
2 - <3	☐ Perform comprehensive architecture assessments across IT, OT, cloud, network, application, and identity layers to identify weaknesses. ☐ Implement a formal configuration management process ensuring standardised builds, hardened configurations, and controlled updates. ☐ Develop standard templates for architecture diagrams, risk assessments, design decisions, and configuration baselines. ☐ Increase integration of architectural controls with CI/CD pipelines, automation tools, and infrastructure-as-code processes to ensure consistent deployments.
3 - <4	☐ Deploy a secure architecture maturity programme targeting reduction of complexity, elimination of legacy patterns, and uplift of control standardisation. ☐ Assign architecture owners responsible for maintaining domain-specific reference architectures and reviewing proposed deviations. ☐ Formalise escalation workflows for architectural non-compliance, high-risk exceptions, or unapproved design changes. ☐ Increase oversight on third-party or vendor-driven architectural components to ensure compliance with organizational security patterns.
4 - <5	☐ Urgent intervention required! Conduct an immediate architecture risk assessment to identify insecure designs, obsolete components, or undocumented control gaps. ☐ Establish an architectural remediation task force to resolve critical issues such as misconfigurations, missing controls, and unsegmented environments. ☐ Implement mandatory reporting from all technology teams on configuration drift, exceptions, and architectural violations. ☐ Enforce a directive prohibiting deployment of any system, integration, or service that does not comply with approved security architecture baselines or has outstanding high-risk deviations.

Also refer to
14.Change Management PC7

Notes

RP Score

Checklist to follow

Planning Controls

Secure Design and Engineering

0 - <1	☐ Maintain a formally approved redundancy design standard defining required failover, replication, clustering, and backup mechanisms for all critical systems. ☐ Ensure redundancy requirements are incorporated into system design documents, architectural diagrams, and engineering specifications. ☐ Conduct periodic design reviews to validate that redundancy mechanisms remain aligned with current architecture patterns and technology stacks. ☐ Maintain architectural dashboards showing redundancy coverage, failover paths, performance baselines, and fault-tolerance metrics.
1 - <2	☐ Improve redundancy designs by integrating dependency mapping, fault-tree analysis, and resilience modelling during architecture creation. ☐ Establish structured workflows requiring redundancy validation before new systems or upgrades are approved for deployment. ☐ Conduct thorough alignment checks between design intent, actual implementation, and operational test results to identify gaps. ☐ Enhance documentation describing active/passive roles, replication modes, fallback behaviour, and conditions under which redundancy is triggered.
2 - <3	☐ Perform comprehensive assessments of network, compute, storage, and OT layers to identify components lacking adequate redundancy. ☐ Implement a formal engineering testing programme that validates failover scenarios, load balancing, recovery times, and resilience under stress. ☐ Develop standardized templates for redundancy diagrams, failover logic, configuration baselines, and dependency matrices. ☐ Increase incorporation of resilience controls such as multi-region deployment, redundant communication channels, and diverse pathways into system design.
3 - <4	☐ Deploy a secure architecture enhancement programme targeting critical single points of failure and architecturally brittle components. ☐ Assign redundancy architects or system owners responsible for maintaining accuracy of redundancy designs and ensuring their ongoing validation. ☐ Formalise escalation workflows for redundancy failures, design deviations, or failures discovered during resilience testing. ☐ Increase oversight of third-party solutions to ensure redundancy configurations offered by vendors meet architectural requirements and are not single-vendor-dependent.
4 - <5	☐ Urgent intervention required! Execute a rapid redundancy review to identify mission-critical systems lacking validated or functional failover mechanisms. ☐ Establish a cross-functional architecture task force to remediate high-risk redundancy gaps and enforce secure design principles across environments. ☐ Implement mandatory reporting from all teams on redundancy test outcomes, configuration drift, and deviations from approved design patterns. ☐ Enforce a directive prohibiting deployment or production operation of any critical system until redundancy controls are validated, tested, and architecturally approved.

Also refer to
2.Risk Management PC8
9.Resilience Management PC8

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally approved framework defining security requirements, compensating controls, and integration patterns for all legacy systems. ☐ Ensure legacy system interfaces, protocols, and dependencies are documented in architectural diagrams and design specifications. ☐ Conduct periodic security architecture reviews to validate that legacy components remain safely integrated within modern environments. ☐ Maintain dashboards showing legacy system exposure, unsupported components, integration risks, and dependency hotspots.
1 - <2	☐ Improve integration designs by incorporating compensating controls such as segmentation, protocol filtering, and hardening guidelines tailored for legacy systems. ☐ Establish structured processes requiring architectural approval before integrating legacy components into new platforms or networks. ☐ Conduct reconciliation checks between design intent, actual configuration, and operational behaviour of legacy systems to identify drift. ☐ Enhance documentation detailing limitations, workarounds, and inherent risks associated with legacy technologies.
2 - <3	☐ Perform comprehensive assessments to identify legacy solutions lacking encryption, authentication, patch support, or monitoring capabilities. ☐ Implement gateway-based or wrapper-based security controls to shield legacy systems from direct exposure to untrusted networks. ☐ Develop standardized templates for recording legacy system attributes, integration constraints, and compensating control requirements. ☐ Increase incorporation of isolation techniques such as VLANs, firewalled segments, DMZ placement, or one-way diodes where applicable.
3 - <4	☐ Deploy a legacy system modernisation programme prioritising replacement or containment of high-risk assets. ☐ Assign integration owners responsible for validating compatibility, performance impact, and security alignment of legacy components. ☐ Formalise escalation workflows for legacy system failures, architectural deviations, or high-risk integration requests. ☐ Increase oversight on vendor dependencies associated with legacy systems, ensuring serviceability, documentation, and support limitations are addressed.
4 - <5	☐ Urgent intervention required! Conduct an immediate assessment of all legacy systems directly exposed to external networks, unsafe protocols, or unsegmented environments. ☐ Establish a cross-functional legacy remediation task force to implement containment controls, upgrade pathways, or accelerated decommissioning plans. ☐ Implement mandatory reporting on legacy system risks, outages, vulnerabilities, and integration failures across IT and OT domains. ☐ Enforce a directive restricting integration of legacy systems into any critical environment unless compensating controls, monitored interfaces, and approved secure design patterns are implemented.

Also refer to
14.Change Management PC9

Notes

RP Score

Checklist to follow

Implementation Control

Secure Design and Engineering

0 - <1	☐ Maintain a formally approved perimeter security architecture defining required controls such as firewalls, gateways, DMZs, IPS/IDS, and segmentation boundaries. ☐ Ensure all perimeter devices follow standardized secure configuration baselines aligned with organizational and regulatory requirements. ☐ Conduct periodic design reviews to validate that perimeter controls effectively enforce trust boundaries and block unauthorized access. ☐ Maintain dashboards showing perimeter coverage, traffic anomalies, blocked threats, misconfigurations, and rule-set health.
1 - <2	☐ Improve perimeter design by integrating threat modelling to identify likely attack paths and high-exposure ingress/egress points. ☐ Establish structured workflows requiring architectural approval before making changes to firewall rules, DMZ structures, or external connectivity. ☐ Conduct reconciliation checks between perimeter architecture diagrams, firewall rule sets, and actual network behaviour to detect deviations. ☐ Enhance documentation detailing rule logic, allowed services, port usage, trust zones, and justification for each allowed connection.
2 - <3	☐ Perform comprehensive perimeter assessments to identify open ports, unused rules, shadow rules, and insecure ingress/egress channels. ☐ Implement a formal firewall rule lifecycle covering creation, review, expiry, recertification, and retirement of outdated rules. ☐ Develop standardized templates for network zoning, rule creation, exception requests, and perimeter design updates. ☐ Increase incorporation of advanced controls such as application-layer filtering, TLS inspection, geo-blocking, and behavioural analytics.
3 - <4	☐ Deploy a perimeter hardening programme focused on reducing attack surfaces, removing legacy exposures, and improving control granularity. ☐ Assign perimeter control owners responsible for rule set hygiene, configuration accuracy, and continuous perimeter monitoring. ☐ Formalise escalation workflows for unauthorized rule changes, high-risk traffic patterns, or detected perimeter breaches. ☐ Increase oversight of third-party connections, ensuring vendor links, remote access, and partner integrations comply with perimeter design requirements.
4 - <5	☐ Urgent intervention required! Conduct an immediate perimeter review to identify insecure rules, bypass paths, or uncontrolled external exposure. ☐ Establish a remediation task force to rapidly correct high-risk perimeter misconfigurations, legacy rules, and segmentation weaknesses. ☐ Implement mandatory reporting on perimeter drift, new external connectivity, rule exceptions, and intrusion detection trends. ☐ Enforce a directive prohibiting activation of any new external connection, partner link, or remote access channel until fully reviewed and approved by secure design.

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally approved testing and evaluation framework defining mandatory security validation requirements for all hardware and software introduced into the environment. ☐ Ensure all new systems undergo security testing- functional, configuration, vulnerability, and integration before production deployment. ☐ Conduct periodic reviews to validate the effectiveness and completeness of testing processes across IT, OT, cloud, and application ecosystems. ☐ Maintain dashboards tracking test coverage, defects identified, failed validations, and high-risk components awaiting remediation.
1 - <2	☐ Improve testing methodology by incorporating threat modelling, misconfiguration analysis, firmware/software risk assessment, and secure design principles. ☐ Establish structured workflows to ensure security testing is embedded into procurement, integration, and change management processes. ☐ Conduct reconciliation checks between test artefacts, configuration baselines, and approved design specifications to detect deviations. ☐ Enhance documentation for test results, risk ratings, exception decisions, and proof-of-mitigation for identified issues.
2 - <3	☐ Perform comprehensive evaluations of vendor hardware/software to identify insecure protocols, unsupported firmware, hidden features, or supply chain risks. ☐ Implement a formal acceptance process requiring all critical findings to be remediated or formally risk-accepted before deployment. ☐ Develop standard templates for evaluation checklists, test scripts, security acceptance criteria, and integration validation forms. ☐ Increase incorporation of automated testing tools, static/dynamic analysis, fuzzing, and compliance scanners for consistent evaluation.
3 - <4	☐ Deploy a continuous validation programme to re-test systems after major updates, configuration changes, or emerging threat disclosures. ☐ Assign evaluation owners responsible for ensuring completeness, accuracy, and timeliness of security testing activities. ☐ Formalise escalation workflows for unresolved high-severity issues, failed tests, or components rejected during evaluation. ☐ Increase oversight on third-party software, ensuring components, libraries, and dependencies meet the organization's secure evaluation requirements.
4 - <5	☐ Urgent intervention required! Conduct immediate testing of high-risk components currently in production without validated test results or security assurance. ☐ Establish a cross-functional evaluation task force to address critical testing backlogs, accelerate validation, and uplift overall testing maturity. ☐ Implement mandatory reporting on insecure components, outdated firmware, testing gaps, and remediation progress across teams. ☐ Enforce a directive prohibiting deployment or continued operation of any hardware or software that has not passed mandatory security testing and evaluation.

Also refer to
6.Vulnerability and Patch Management IC6
12.Supply Chain Risk IC6

Notes

RP Score

Checklist to follow

Operational Control

Secure Design and Engineering

0 - <1	☐ Maintain a formally approved network device security standard defining baseline configurations, access requirements, and hardening controls for all routers, switches, firewalls, and OT network components. ☐ Ensure all network devices are deployed using secure configurations aligned with architectural design patterns and zero-trust segmentation principles. ☐ Conduct periodic secure design reviews to validate that network device configurations remain consistent with approved baselines. ☐ Maintain dashboards tracking configuration drift, device health, unauthorized changes, and high-risk vulnerabilities across network infrastructure.
1 - <2	☐ Improve device protection by integrating threat modelling to identify choke points, exposure surfaces, and architecture-sensitive dependencies. ☐ Establish structured workflows requiring secure design approval before implementing configuration changes, firmware upgrades, or topology modifications. ☐ Conduct reconciliation checks between approved design diagrams, device configurations, and actual network behaviour to detect deviations or bypass paths. ☐ Enhance documentation for device roles, configuration intent, segmentation logic, access restrictions, and protocol usage.
2 - <3	☐ Perform comprehensive device assessments to identify weak configurations, legacy protocols, missing encryption, or unmonitored interfaces. ☐ Implement configuration automation and golden baseline enforcement to reduce misconfigurations and maintain architectural hygiene. ☐ Develop standardized templates for device hardening checklists, segmentation schemas, ACL definitions, and configuration approval workflows. ☐ Increase integration of network devices with logging, SIEM, and behavioural analytics tools to enhance security visibility.
3 - <4	☐ Deploy a network hardening programme targeting elimination of insecure defaults, removal of unused services, and enforcement of strong authentication. ☐ Assign device owners responsible for configuration accuracy, secure maintenance, and validation of implemented changes. ☐ Formalise escalation workflows for unauthorized configuration changes, detected policy violations, or deviations from approved security architecture. ☐ Increase oversight of vendor-managed network devices, ensuring firmware versions, patches, and support models meet secure design requirements.
4 - <5	☐ Urgent intervention required! Conduct an immediate review of all network devices with high-risk exposure, unsupported firmware, or uncontrolled access paths. ☐ Establish a cross-functional network remediation team to correct critical misconfigurations, upgrade vulnerable devices, and enforce architectural controls. ☐ Implement mandatory reporting on device drift, configuration exceptions, and unresolved vulnerabilities across network environments. ☐ Enforce a directive prohibiting deployment or continued operation of any network device that does not comply with secure baseline configurations and approved design patterns.

Also refer to
6.Vulnerability and Patch Management OC7

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally approved cloud security architecture defining required controls for identity, network segmentation, data protection, logging, and workload security across all cloud platforms. ☐ Ensure all cloud services follow standardized secure configuration baselines aligned with organizational patterns and cloud provider best practices. ☐ Conduct periodic architecture reviews to validate that deployed cloud resources remain consistent with approved design blueprints. ☐ Maintain dashboards tracking misconfigurations, high-risk services, unmonitored assets, open ports, and cloud exposure paths.
1 - <2	☐ Improve cloud design by incorporating threat modelling, shared responsibility clarifications, and cloud-specific attack surface analysis. ☐ Establish structured workflows requiring secure design approval before provisioning new cloud resources or enabling external connectivity. ☐ Conduct reconciliation checks between IaC templates, deployed cloud configurations, and architectural diagrams to detect drift. ☐ Enhance documentation for cloud architectures, including trust boundaries, key management schemes, identity mappings, and data flow paths.
2 - <3	☐ Perform comprehensive cloud security assessments to identify insecure defaults, overly permissive IAM roles, public exposures, or unencrypted assets. ☐ Implement automated configuration scanning and policy enforcement tools to maintain alignment with approved cloud security standards. ☐ Develop standardized templates for cloud network design, IAM policies, encryption configurations, and multi-region deployment patterns. ☐ Increase adoption of cloud-native security capabilities such as CASB, CSPM, CWPP, and managed key vaults for layered protection.
3 - <4	☐ Deploy a cloud-hardening programme targeting elimination of risky services, closure of public endpoints, and enforcement of least-privilege IAM models. ☐ Assign cloud security architects responsible for reviewing workload designs, validating controls, and approving architectural exceptions. ☐ Formalise escalation workflows for detected misconfigurations, privilege escalation risks, or deviations from cloud security baselines. ☐ Increase oversight on third-party cloud integrations to ensure data access, API connections, and shared resources are properly segmented and secured.
4 - <5	☐ Urgent intervention required! Conduct an immediate cloud exposure audit to identify publicly accessible assets, misconfigured buckets, or unprotected workloads. ☐ Establish a cross-functional cloud remediation task force to rapidly correct high-severity cloud vulnerabilities and enforce architectural compliance. ☐ Implement mandatory reporting on cloud configuration drift, unresolved CSPM findings, and non-compliant deployments. ☐ Enforce a directive prohibiting activation of any cloud workload unless deployed through approved templates, scanned for misconfigurations, and validated by secure design.

Operational Control

Secure Design and Engineering

Also refer to
11.Data Protection OC8
12.Supply Chain Risk OC8

Notes

RP Score

Checklist to follow

Disaster Recovery/ Business

Secure Design and Engineering

0 - <1	☐ Maintain a formally approved resilient architecture framework defining required controls for redundancy, segmentation, failover, disaster recovery integration, and high-availability design. ☐ Ensure all new systems are deployed using secure, resilience-aligned architectural patterns such as multi-zone distribution, load balancing, and segmentation. ☐ Conduct periodic architecture reviews to verify that deployed environments remain consistent with approved secure and resilient design principles. ☐ Maintain dashboards showing resilience coverage, single points of failure, architectural deviations, and system-level readiness metrics.
1 - <2	☐ Improve resilient design patterns by incorporating threat modelling, dependency analysis, and attack surface reduction during architectural planning. ☐ Establish structured deployment workflows requiring secure design approval prior to major releases, integrations, or infrastructure rollouts. ☐ Conduct reconciliation checks between design documentation, IaC templates, implementation details, and operational behaviour to detect drift. ☐ Enhance documentation detailing expected failover behaviour, recovery logic, data protection constraints, and dependency fail-safes.
2 - <3	☐ Perform comprehensive resilience assessments across application, network, OT, and cloud layers to identify architectural weaknesses. ☐ Implement automated resilience testing including chaos testing, controlled failovers, and dependency disruption scenarios to validate architectural robustness. ☐ Develop standardized templates for resilience architecture diagrams, dependency matrices, failover sequences, and recovery workflows. ☐ Increase integration between resilience engineering, secure design, and business continuity functions to ensure unified architectural intent.
3 - <4	☐ Deploy a resilience uplift programme targeting brittle architectures, insufficient segmentation, legacy dependencies, and weak recovery paths. ☐ Assign resilience architects responsible for validating architectural integrity, reviewing resilience-related changes, and guiding remediation efforts. ☐ Formalise escalation workflows for resilience failures, deviations from architectural design, or identified high-risk dependencies. ☐ Increase oversight of third-party architectural components, ensuring cloud services, network appliances, and vendor-managed environments meet resilience requirements.
4 - <5	☐ Urgent intervention required! Conduct an immediate resilience architecture audit to identify critical single points of failure and high-risk dependency chains. ☐ Establish a cross-functional architectural remediation team to address structural weaknesses and enforce resilient design standards. ☐ Implement mandatory reporting on recovery testing results, resilience gaps, configuration drift, and deviations from approved architectures. ☐ Enforce a directive prohibiting deployment or production operation of systems that do not meet minimum resilience, segmentation, and secure design criteria.

Also refer to
9.Resilience Management DR3
14.Change Management DR3

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Vulnerability and Patch Management).
2. Locate the appropriate control within the Vulnerability and Patch Management domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

6 Vulnerability and Patch Management

6 Response and Recovery

PC6

RP Score

Checklist to follow

Planning Controls

Vulnerability and Patch Management

0 - <1	☐ Maintain a formal vulnerability assessment schedule ensuring all systems are scanned with appropriate depth and frequency. ☐ Ensure vulnerability findings are prioritised using a risk-based scoring model that considers exploitability, asset criticality, and business impact. ☐ Conduct periodic reviews to validate that vulnerability scanning tools, signatures, and configurations are up to date. ☐ Maintain dashboards showing open vulnerabilities, remediation progress, age of findings, and exposure trends.
1 - <2	☐ Improve assessment coverage by including cloud workloads, OT devices, network appliances, APIs, and third-party components. ☐ Establish structured workflows mandating timely remediation of high-severity vulnerabilities according to defined SLAs. ☐ Conduct alignment checks between vulnerability scans, pen test results, and configuration audits to eliminate blind spots. ☐ Enhance documentation for accepted vulnerabilities, including justification, compensating controls, and expiration dates.
2 - <3	☐ Perform full-scope assessments following major changes, new deployments, or after emerging threat alerts. ☐ Implement authenticated scanning methods to improve depth and accuracy of vulnerability detection. ☐ Develop standard templates for reporting vulnerability findings, recommended fixes, and associated risk ratings. ☐ Increase integration of VTR results with patch management tools to automate prioritisation and remediation tracking.
3 - <4	☐ Deploy a vulnerability reduction programme targeting recurring issues such as missing patches, weak configurations, or unsupported platforms. ☐ Assign vulnerability owners who are accountable for tracking and closing findings in their respective domains. ☐ Formalise escalation routes for overdue high-severity vulnerabilities requiring leadership attention. ☐ Increase oversight on third-party systems to ensure they meet organizational vulnerability assessment requirements.
4 - <5	☐ Urgent intervention required! Conduct immediate scanning of high-risk environments to identify actively exploited vulnerabilities. ☐ Establish a cross-functional vulnerability remediation team to resolve systemic issues and accelerate closure of ageing findings. ☐ Implement mandatory reporting on vulnerability backlog, SLA adherence, and repeated or reopened findings. ☐ Enforce a directive preventing deployment or operation of systems until critical vulnerabilities are remediated or formally risk-accepted.

Also refer to
2.Risk Management PC6

Notes

6 Response and Recovery

IC6

RP Score

Checklist to follow

0 - <1	☐ Maintain a vulnerability-based evaluation process requiring all new hardware/software to be examined for known vulnerabilities before approval. ☐ Ensure components are checked for patch availability, vendor support status, and exposure to common CVEs prior to onboarding. ☐ Conduct periodic reviews to validate that existing hardware/software configurations remain free from known vulnerabilities. ☐ Maintain dashboards tracking vulnerable components, patch applicability, and outdated or unsupported technologies.
1 - <2	☐ Improve evaluation depth by incorporating vulnerability scanning, SBOM analysis, and secure configuration verification during assessments. ☐ Establish structured workflows linking evaluation results directly to patch management processes. ☐ Conduct reconciliation checks between evaluation findings, deployed versions, and patch status to detect inconsistencies. ☐ Enhance documentation for components with unresolved vulnerabilities, including mitigation actions and expiration of temporary controls.
2 - <3	☐ Perform ongoing reviews of third-party libraries, firmware, and embedded components to identify inherited vulnerabilities. ☐ Implement a formal rejection criteria for components that cannot meet minimum patching or vulnerability remediation requirements. ☐ Develop standardized evaluation templates capturing version, vendor roadmap, CVE exposure, and patch compatibility. ☐ Increase integration with vulnerability intelligence feeds to detect new CVEs affecting approved products.
3 - <4	☐ Deploy a validation programme ensuring vulnerabilities identified during evaluation are remediated promptly after deployment. ☐ Assign component evaluation owners responsible for tracking vulnerabilities throughout the product lifecycle. ☐ Formalise escalation workflows for components with critical vulnerabilities lacking immediate patches or vendor support. ☐ Increase oversight on vendor-supplied devices to verify vulnerability disclosures, update commitments, and patch release timelines.
4 - <5	☐ Urgent intervention required! Perform immediate evaluation of mission-critical systems potentially exposed to newly published exploits. ☐ Establish an evaluation remediation working group to address high-risk vulnerabilities identified during testing. ☐ Implement mandatory reporting of components running outdated firmware, unsupported OS versions, or deprecated dependencies. ☐ Enforce a directive prohibiting deployment of any component that has not passed vulnerability evaluation or has unresolved critical exposure.

Implementation Control

Vulnerability and Patch Management

Also refer to
5.Secure Design and Engineering IC6
12.Supply Chain Risk IC6

Notes

6 Response and Recovery

OC5

RP Score

Checklist to follow

Operational Controls

Vulnerability and Patch Management

0 - <1	☐ Maintain a penetration testing programme focused on identifying vulnerabilities that automated scanners may miss. ☐ Ensure penetration test findings are rapidly translated into patching and configuration updates. ☐ Conduct periodic penetration tests targeting high-risk systems, exposed interfaces, and newly deployed technologies. ☐ Maintain dashboards showing open pen-test findings, severity trends, exploited vectors, and remediation progress.
1 - <2	☐ Improve coverage by including cloud workloads, APIs, OT networks, and identity systems in pen-testing scope. ☐ Establish structured workflows linking pen-test results to patch deployment tasks and configuration fixes. ☐ Conduct alignment checks to ensure pen-test findings are closed across all environments configured similarly. ☐ Enhance documentation on remediation steps taken, validating that vulnerabilities identified via pen-testing are fully patched.
2 - <3	☐ Perform targeted tests following newly published exploits or significant system upgrades. ☐ Implement mandatory retesting processes to verify closure of high-risk findings. ☐ Develop standardized templates for reporting exploited vulnerabilities, attack paths, and required patches. ☐ Increase integration between pen-testing teams and patch management owners to accelerate vulnerability closure.
3 - <4	☐ Deploy a remediation acceleration plan for vulnerabilities repeatedly exploited during tests. ☐ Assign remediation owners for pen-test findings with SLA-based accountability. ☐ Formalise escalation procedures for high-severity exploited vulnerabilities not patched in time. ☐ Increase oversight to ensure pen-testing results inform patching priorities across all teams.
4 - <5	☐ Urgent intervention required! Conduct immediate exploitation tests on systems suspected to contain actively exploited vulnerabilities. ☐ Establish a cross-team task force to close high-priority vulnerabilities uncovered through pen-testing. ☐ Implement mandatory reporting on outstanding pen-test findings, retest failures, and unresolved exploitation paths. ☐ Enforce a directive prohibiting go-live or continued operation of systems with unpatched pen-test-identified critical vulnerabilities.

Also refer to
2.Risk Management OC5

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a patching baseline defining update frequency, firmware requirements, and vulnerability handling for all network devices. ☐ Ensure all routers, switches, firewalls, and OT network components are regularly scanned for vulnerabilities and configuration weaknesses. ☐ Conduct periodic reviews to validate that devices are running supported firmware versions free from known critical vulnerabilities. ☐ Maintain dashboards tracking device patch status, missing updates, unsupported models, and vulnerability trends.
1 - <2	☐ Improve network device patching workflows by aligning update cycles with vendor advisories and security bulletins. ☐ Establish structured workflows ensuring device patches are tested in controlled environments before production deployment. ☐ Conduct reconciliation checks comparing device configuration, firmware versions, and vulnerability scan data. ☐ Enhance documentation capturing patch history, applied fixes, and pending updates for each device.
2 - <3	☐ Perform assessments to identify devices with insecure protocols, weak encryption, or outdated firmware. ☐ Implement an automated device inventory and vulnerability correlation system for real-time exposure analysis. ☐ Develop standard templates for patching procedures, rollback plans, and pre-deployment testing requirements. ☐ Increase integration between network monitoring tools and vulnerability management platforms.
3 - <4	☐ Deploy a device hardening and patching programme targeting persistent vulnerabilities and misconfigurations. ☐ Assign device patch owners responsible for ensuring timely remediation of vulnerabilities. ☐ Formalise escalation processes for critical vulnerabilities requiring immediate patch application or device isolation. ☐ Increase oversight of third-party managed network devices to ensure consistent patching and vulnerability remediation.
4 - <5	☐ Urgent intervention required! Patch or isolate devices exposed to exploit kits, active scanning, or critical CVEs. ☐ Establish a network patch remediation team responsible for high-volume device updates and emergency patch deployments. ☐ Implement mandatory reporting on device vulnerabilities, patch status, and overdue remediation items. ☐ Enforce a directive prohibiting operation of network devices that remain unpatched for critical vulnerabilities beyond approved SLAs.

Operational Controls

Vulnerability and Patch Management

Also refer to
5.Secure Design and Engineering OC7

Notes

6 Response and Recovery

RA2

RP Score

Checklist to follow

Reporting and Accountability

Vulnerability and Patch Management

0 - <1	☐ Maintain a periodic vulnerability audit programme ensuring all systems undergo structured assessments at defined intervals. ☐ Ensure audit results are mapped directly to patch management activities, ensuring actionable remediation. ☐ Conduct periodic vulnerability audits to validate the effectiveness of patch deployment and identify missed updates. ☐ Maintain dashboards showing audit coverage, recurring vulnerabilities, patch compliance rates, and systemic weaknesses.
1 - <2	☐ Improve audit depth by correlating CVEs with asset criticality and patch urgency. ☐ Establish clear workflows requiring immediate remediation of audit-identified critical vulnerabilities. ☐ Conduct reconciliation checks between audit reports, scanner data, and patch deployment logs. ☐ Enhance documentation for vulnerability exceptions, including business justification and compensating controls.
2 - <3	☐ Perform audits following major threat advisories or vendor patch releases to confirm timely application. ☐ Implement formal patch compliance scoring to track maturity and improvement over time. ☐ Develop standardized templates for audit findings, remediation plans, and verification evidence. ☐ Increase integration between audit processes and patch automation tools to accelerate closure.
3 - <4	☐ Deploy a continuous validation programme ensuring applied patches remain effective and do not regress. ☐ Assign audit owners responsible for verifying closure of vulnerabilities and updating records. ☐ Formalise escalation workflows for repeated audit failures or persistent vulnerability themes. ☐ Increase oversight on legacy systems and OT devices which often show chronic patching gaps.
4 - <5	☐ Urgent intervention required! Conduct immediate audits of high-risk systems potentially exposed to zero-day exploits. ☐ Establish a vulnerability audit remediation task force to drive rapid closure of severe findings. ☐ Implement mandatory reporting of audit status, overdue findings, and exceptions requiring leadership attention. ☐ Enforce a directive preventing continued operation of systems failing to meet minimum vulnerability and patch compliance standards.

Also refer to
 1.Governance RA2
 2.Risk Management RA2
 15.Situational Awareness RA2

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Threat Intelligence).
2. Locate the appropriate control within the Threat Intelligence domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

7 Threat Intelligence

RP Score

Checklist to follow

Planning Controls

Threat Intelligence

0 - <1	☐ Maintain an intelligence-led dependency mapping framework correlating upstream and downstream services with threat exposure. ☐ Ensure interdependency models incorporate threat intelligence on sector-wide attacks, cascading failure risks, and adversary techniques. ☐ Conduct periodic intelligence reviews to validate that interdependency maps reflect current attack vectors and sector trends. ☐ Maintain dashboards showing dependency-driven threat exposure, cross-domain correlations, and high-risk linkages.
1 - <2	☐ Improve interdependency mapping by integrating adversary TTPs to identify where compromise can propagate laterally or vertically. ☐ Establish structured intelligence-sharing workflows across business units to update dependency risks based on new threat insights. ☐ Conduct alignment checks between threat reports, dependency diagrams, and incident response findings. ☐ Enhance documentation explaining how threat events could impact dependent processes, assets, or integrated environments.
2 - <3	☐ Perform comprehensive dependency threat assessments to identify weak nodes susceptible to exploitation. ☐ Implement monitoring for anomalous behaviours at high-risk dependency points such as shared services or integration gateways. ☐ Develop templates capturing dependency risks, threat likelihood, and adversary exploitation paths. ☐ Increase consumption of sectoral threat intelligence to update dependency impact assessments.
3 - <4	☐ Deploy a dependency risk awareness programme ensuring operational teams understand threat propagation channels. ☐ Assign dependency intelligence owners responsible for tracking threat changes and updating impact models. ☐ Formalise escalation routes when interdependency analysis reveals potential cascading failures triggered by emerging threats. ☐ Increase oversight on third-party and cross-sector interdependencies where intelligence indicates heightened adversary activity.
4 - <5	☐ Urgent intervention required! Conduct a rapid intelligence-led dependency review for services targeted by new campaigns. ☐ Establish a cross-functional threat modelling group to continuously analyse attack paths leveraging interdependencies. ☐ Implement mandatory reporting of interdependency anomalies observed through monitoring, threat intel feeds, or incidents. ☐ Enforce a directive restricting activation of new dependencies until threat modelling and intelligence reviews are complete.

Also refer to

- 1.Governance PC2
- 2.Risk Management PC2
- 9.Resilience Management PC2
- 15.Situational Awareness PC2

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a threat intelligence programme focused on detecting, analysing, and responding to advanced persistent threats (APTs). ☐ Ensure APT indicators, adversary TTPs, and behavioural patterns are continuously updated from trusted intelligence sources. ☐ Conduct periodic assessments of APT readiness to validate detection coverage, response maturity, and monitoring depth. ☐ Maintain dashboards showing APT-related alerts, behaviours, campaigns, and high-risk assets under observation.
1 - <2	☐ Improve APT defences by integrating MITRE ATT&CK mapping into detection, logging, and response workflows. ☐ Establish structured threat hunting cycles targeting high-value assets, privileged users, and sensitive environments. ☐ Conduct alignment checks between SOC detections, threat intel feeds, and incident response investigations. ☐ Enhance documentation for APT detections, including suspected adversary groups, activity timelines, and pivot points.
2 - <3	☐ Perform comprehensive behavioural analysis on network traffic, authentication patterns, endpoint data, and OT telemetry. ☐ Implement advanced monitoring such as EDR, NDR, sandboxing, and anomaly detection focused on stealthy attacker behaviour. ☐ Develop standard templates for APT briefings, detection playbooks, and threat escalation criteria. ☐ Increase integration of threat intelligence with SIEM correlation logic and detection engineering.
3 - <4	☐ Deploy an APT resilience programme strengthening logging, authentication controls, segmentation, and deception capabilities. ☐ Assign threat hunters responsible for continuous APT hypothesis testing and adversary emulation. ☐ Formalise escalation pathways for APT-grade indicators requiring immediate executive attention. ☐ Increase oversight on third-party connections and OT systems often targeted during APT lateral movement.
4 - <5	☐ Urgent intervention required! Conduct an emergency threat hunt in response to global APT advisories relevant to the organization's sector. ☐ Establish a cross-functional APT response cell uniting threat intel, SOC, IR, and architecture teams. ☐ Implement mandatory reporting on APT detections, unresolved anomalies, and emerging adversary campaigns. ☐ Enforce a directive ensuring all critical systems implement APT-specific monitoring, segmentation, and hardening controls.

Operational Control

Threat Intelligence

Also refer to
8.Security Incidence Management OC11
15.Situational Awareness OC11

Notes

RP Score

Checklist to follow

Reporting and Accountability

Threat Intelligence

0 - <1	☐ Maintain an intelligence-driven reporting framework that ensures timely escalations of threat indicators, anomalies, and confirmed incidents to government agencies. ☐ Ensure reporting thresholds incorporate intelligence severity, adversary attribution, and national-sector relevance. ☐ Conduct periodic reviews to validate that threat reporting aligns with national intelligence advisories and updated requirements. ☐ Maintain dashboards showing all intelligence reports submitted, response timelines, and cross-agency coordination.
1 - <2	☐ Improve reporting processes by integrating automated threat ingestion and correlation prior to submission. ☐ Establish structured intelligence-sharing channels with CERT-In, NCIIPC, sectoral CERTs, and law enforcement. ☐ Conduct alignment checks between internal detections, intelligence feeds, and what is shared externally. ☐ Enhance documentation capturing rationale for reporting, supporting evidence, and threat context.
2 - <3	☐ Perform correlation analysis between national advisories and internal indicators to identify reportable patterns. ☐ Implement a formal triage process to assess reportability of emerging threats and anomalies. ☐ Develop templated formats for threat reporting including IOCs, TTPs, timelines, impacted systems, and defensive measures. ☐ Increase integration between SOC, IR, and threat intel units to ensure accurate and timely reporting.
3 - <4	☐ Deploy a situational awareness programme translating national intelligence into actionable internal defensive measures. ☐ Assign reporting officers trained in intelligence reporting protocols and threat interpretation. ☐ Formalise escalation workflows for threats deemed nationally significant or sector-wide. ☐ Increase oversight ensuring intelligence reports sent externally are consistent, accurate, and validated.
4 - <5	☐ Urgent intervention required! Conduct accelerated reporting of emerging threats identified through ongoing investigations or unusual activity patterns. ☐ Establish a cross-agency communication group for rapid intelligence exchange during active threat campaigns. ☐ Implement mandatory reporting of significant anomalies, even if not confirmed incidents, where intelligence indicates possible coordinated targeting. ☐ Enforce a directive requiring immediate submission of threat intelligence to authorities for any activity with potential national impact.

Also refer to
1.Governance RA1
15.Situational Awareness RA1

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Security Incidence Management).
2. Locate the appropriate control within the Security Incidence Management domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

Security Incidence Management

RP Score

Checklist to follow

Planning Controls

Security Incident Management

0 - <1	☐ Maintain an operationally capable Information Security Department (ISD) with clearly defined incident response, SOC, threat hunting, and forensic functions. ☐ Ensure incident handling roles incident commander, handler, analyst, investigator are explicitly assigned and documented within the ISD. ☐ Conduct periodic capability assessments to validate ISD readiness across monitoring, detection, triage, containment, and recovery activities. ☐ Maintain dashboards showing incident workload, capacity, staffing gaps, response times, and repeat incident categories.
1 - <2	☐ Improve ISD structure by aligning teams along modern IR disciplines such as detection engineering, digital forensics, and adversary emulation. ☐ Establish structured communication paths ensuring ISD receives timely alerts from monitoring systems, operational teams, and automated detections. ☐ Conduct alignment checks between ISD roles, SOC responsibilities, and business escalation requirements. ☐ Enhance documentation of IR workflows, including triage criteria, severity assignment, containment protocols, and communication templates.
2 - <3	☐ Perform comprehensive workload analysis to identify bottlenecks in incident handling and resource allocation. ☐ Implement a shift-based or follow-the-sun operating model, where appropriate, to ensure continuous incident monitoring and response. ☐ Develop standard playbooks for high-frequency incident types (malware, phishing, credential compromise, lateral movement). ☐ Increase integration of ISD with OT operations, cloud teams, network operations, and business units to improve visibility during incidents.
3 - <4	☐ Deploy an ISD maturity uplift programme focused on automation, event correlation, and improved detection engineering. ☐ Assign domain owners within ISD (e.g., endpoint, network, cloud) responsible for driving incident response improvements in their area. ☐ Formalise escalation workflows requiring ISD to notify senior leadership during major incidents or significant security events. ☐ Increase oversight of external IR vendors to ensure alignment with internal ISD processes during collaborative investigations.
4 - <5	☐ Urgent intervention required! Conduct an immediate ISD capability review for any function showing gaps in incident triage or containment. ☐ Establish a cross-functional IR coordination team to unify ISD, SOC, IT, OT, legal, HR, and communications during major incidents. ☐ Implement mandatory reporting on IR performance metrics, incident backlogs, detection gaps, and lessons learned. ☐ Enforce a directive prohibiting closure of any incident without ISD verification and documentation of containment, eradication, and recovery activities.

Also refer to
1.Governance PC3
13.Workforce Management PC3

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a formally approved incident response framework defining roles, responsibilities, escalation paths, and communication requirements. ☐ Ensure incident classifications, severity levels, and response timelines are documented and understood across all operational teams. ☐ Conduct periodic incident response reviews to verify that procedures reflect current technologies, threats, and organizational structure. ☐ Maintain dashboards showing ongoing incidents, response timelines, root-cause themes, and outstanding remediation actions.
1 - <2	☐ Improve incident playbooks by incorporating threat intelligence, behavioural indicators, and cross-domain dependencies. ☐ Establish structured workflows ensuring every incident is documented, triaged, assigned, and updated in a central tracking system. ☐ Conduct alignment checks between SOC alerts, monitoring logs, and IR tickets to ensure no incident is missed or misclassified. ☐ Enhance documentation of incident narratives, lessons learned, and final containment and eradication steps.
2 - <3	☐ Perform comprehensive incident simulations and tabletop exercises to evaluate readiness and capability across teams. ☐ Implement a formal after-action review process ensuring systemic weaknesses are identified and assigned for remediation. ☐ Develop standard templates for incident logging, evidence handling, impact assessment, and stakeholder reporting. ☐ Increase integration between monitoring tools, SIEM, EDR, IR platforms, and threat intelligence feeds.
3 - <4	☐ Deploy a response acceleration programme aimed at reducing mean time to detect (MTTD) and mean time to respond (MTTR). ☐ Assign incident handlers and incident commanders responsible for coordinated response and timely decision-making. ☐ Formalise escalation routes for major incidents requiring senior management or external authority notification. ☐ Increase oversight ensuring containment actions do not inadvertently disrupt critical services or cause collateral impact.
4 - <5	☐ Urgent intervention required! Conduct a rapid review of high-severity incidents to validate containment, identify affected assets, and eliminate residual threats. ☐ Establish a cross-functional major-incident team to coordinate response across IT, OT, SOC, risk, and business operations. ☐ Implement mandatory reporting of incident metrics, unresolved cases, repeat incident patterns, and observations requiring executive attention. ☐ Enforce a directive prohibiting closure of incidents until containment, eradication, recovery, and lessons learned activities are fully completed and verified.

Also refer to
9.Resilience Management OC2
15.Situational Awareness OC2

Notes

8 Security Incident Management

OC11

RP Score

Checklist to follow

Operational Control

Security Incident Management

0 - <1	☐ Maintain an APT-focused incident response framework defining detection methods, containment strategies, escalation flows, and forensic requirements. ☐ Ensure the SOC and IR teams are trained to recognise APT behaviours, including lateral movement, credential theft, and stealthy persistence mechanisms. ☐ Conduct periodic APT readiness assessments to validate that response playbooks, tools, and telemetry sources are adequate for advanced threats. ☐ Maintain dashboards showing APT-related alerts, active investigations, unresolved anomalies, and residual risks.
1 - <2	☐ Improve APT response playbooks by integrating behavioural detections aligned to adversary TTPs and MITRE ATT&CK techniques. ☐ Establish structured workflows for deep-dive investigation, ensuring suspicious activity receives multi-layered analysis across host, network, and identity data. ☐ Conduct alignment checks between SOC alerts, threat hunting observations, and IR findings to ensure no potential APT indicators are overlooked. ☐ Enhance documentation covering attack timelines, observed adversary behaviours, privilege escalation events, and potential data exfiltration attempts.
2 - <3	☐ Perform full forensic investigations on suspected APT intrusions, including memory analysis, system imaging, and timeline reconstruction. ☐ Implement continuous monitoring and anomaly detection in high-value assets and sensitive environments prone to APT targeting. ☐ Develop standardised templates for APT incident reports, escalation summaries, and technical deep-dive artefacts. ☐ Increase integration between IR teams, architecture, and IT/OT operations to ensure rapid containment measures during suspected APT events.
3 - <4	☐ Deploy an APT containment programme that includes isolation procedures, credential resets, segmentation adjustments, and enhanced monitoring. ☐ Assign dedicated APT incident handlers responsible for coordinating multi-team investigation and ensuring accurate interpretation of threat signals. ☐ Formalise escalation triggers requiring immediate notification of leadership and relevant authorities upon detection of APT-grade behaviours. ☐ Increase oversight on privileged accounts and service accounts, which are frequent targets in advanced attack campaigns.
4 - <5	☐ Urgent intervention required! Conduct an emergency threat hunt when sector-wide or national advisories indicate active APT campaigns relevant to your organization. ☐ Establish a cross-functional APT response cell unifying SOC, IR, threat intel, forensics, identity, and network teams for coordinated action. ☐ Implement mandatory reporting on unresolved APT indicators, incomplete investigations, and anomalies requiring further analysis. ☐ Enforce a directive preventing closure of any APT-related case until containment is verified, persistence mechanisms removed, and full eradication confirmed by IR and threat hunting teams.

Also refer to
7.Threat Intelligence OC11
15.Situational Awareness OC11

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Resilience Management).
2. Locate the appropriate control within the Resilience Management domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

9 Resilience Management

RP Score

Checklist to follow

Planning Controls

Resilience Management

0 - <1	☐ Maintain a resilience-focused interdependency map identifying upstream and downstream systems that support critical services. ☐ Ensure interdependency analyses include operational, infrastructural, technological, and third-party linkages that influence service continuity. ☐ Conduct periodic resilience reviews to validate that interdependency mappings reflect current operational realities and system integrations. ☐ Maintain dashboards showing resilience-critical dependencies, single points of failure, and high-impact interconnection risks.
1 - <2	☐ Improve resilience modelling by incorporating failure propagation, cascading outage scenarios, and dependency loads during stress conditions. ☐ Establish structured processes to evaluate how disruptions in one system may affect dependent services across business lines. ☐ Conduct alignment checks between continuity plans, dependency diagrams, and redundancy designs to ensure consistency. ☐ Enhance documentation detailing fallback behaviours, failover dependencies, and manual workarounds for interconnected processes.
2 - <3	☐ Perform resilience assessments across critical interdependencies to identify fragile or non-redundant pathways. ☐ Implement monitoring of key dependencies to detect early warning signs such as capacity degradation, latency, or partial outages. ☐ Develop standard templates for documenting dependency relationships, resilience requirements, and alternative pathways. ☐ Increase testing of dependency resilience through failure simulations, dependency removal exercises, and controlled interruption tests.
3 - <4	☐ Deploy an interdependency strengthening programme targeting high-risk connections and undocumented reliance points. ☐ Assign dependency resilience owners responsible for maintaining accurate models and leading mitigation efforts. ☐ Formalise escalation routes for dependency failures affecting multiple services or presenting continuity risks. ☐ Increase oversight on vendor-managed dependencies, ensuring they meet resilience expectations and provide continuity assurances.
4 - <5	☐ Urgent intervention required! Conduct an immediate dependency resilience review following system outages or major integration changes. ☐ Establish a cross-functional dependency resilience task force to address weaknesses that threaten continuity of operations. ☐ Implement mandatory reporting on dependency-related disruptions, capacity issues, and early-warning indicators. ☐ Enforce a directive preventing deployment of new systems or integrations without completing dependency resilience analysis and obtaining approval.

Also refer to
 1.Governance PC2
 2.Risk Management PC2
 7.Threat Intelligence PC2
 15.Situational Awareness PC2

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a resilience-driven redundancy framework defining backup components, failover mechanisms, and alternate service paths for all critical systems. ☐ Ensure redundancy designs support continuity objectives such as RTO, RPO, and maximum tolerable downtime. ☐ Conduct periodic resilience assessments to validate that redundancy functions operate correctly under real-world conditions. ☐ Maintain dashboards showing redundancy coverage, failover readiness, system health, and resilience gaps across critical services.
1 - <2	☐ Improve redundancy architectures by incorporating dual-provider designs, multi-region deployment, and diverse communication paths. ☐ Establish structured workflows ensuring all redundancy mechanisms including clusters, load balancers, and replication engines are tested regularly. ☐ Conduct reconciliation checks between redundancy design specifications and actual operational configurations to detect deviations. ☐ Enhance documentation describing failover triggers, fallback procedures, and recovery behaviour for each redundant component.
2 - <3	☐ Perform resilience stress tests to identify fragile components that fail under load, latency shifts, or partial system degradation. ☐ Implement continuous monitoring for redundancy readiness, focusing on replication lags, node health, storage sync failures, and backup freshness. ☐ Develop standard templates covering redundancy roles, configuration details, test results, and dependency relationships. ☐ Increase the use of active-active or active-passive resilience patterns to reduce reliance on manual recovery processes.
3 - <4	☐ Deploy a redundancy improvement programme to eliminate single points of failure and enhance survivability of mission-critical workloads. ☐ Assign redundancy owners responsible for ensuring operational readiness, maintenance, and testing of failover systems. ☐ Formalise escalation routes for redundancy failures or test results indicating unacceptable resilience risk. ☐ Increase oversight on third-party components and external services to confirm their redundancy posture aligns with organizational continuity needs.
4 - <5	☐ Urgent intervention required! Execute an immediate redundancy readiness review for critical services following outages or performance degradation. ☐ Establish a cross-functional resilience engineering team to remediate high-risk redundancy gaps and optimize fallback behaviour. ☐ Implement mandatory reporting on redundancy test results, failover anomalies, and unresolved resilience issues. ☐ Enforce a directive preventing production operation of any critical service that lacks validated and operational redundancy capabilities.

Also refer to
2.Risk Management PC8
5.Secure Design and Engineering PC8

Notes

RP Score

Checklist to follow

Planning Controls

Resilience Management

0 - <1	☐ Maintain a resilience-driven physical security framework that ensures critical facilities remain operational during environmental, accidental, or malicious events. ☐ Ensure perimeter, access control, and surveillance systems have redundancy and backup power to operate during outages. ☐ Conduct periodic resilience assessments of physical controls to verify their ability to withstand disruptions, sabotage attempts, or equipment failures. ☐ Maintain dashboards tracking physical security incidents, control failures, environmental alarms, and facility readiness indicators.
1 - <2	☐ Improve facility resilience by integrating physical security controls with redundancy planning, emergency response, and continuity strategies. ☐ Establish structured workflows ensuring maintenance, inspection, and periodic testing of all physical controls supporting critical operations. ☐ Conduct alignment checks between physical layouts, environmental monitoring systems, and resilience plans to confirm accuracy. ☐ Enhance documentation describing fallback procedures if physical security systems such as access gates or biometric readers fail.
2 - <3	☐ Perform comprehensive facility vulnerability assessments to identify weak points, single access paths, or exposure to environmental hazards. ☐ Implement environmental controls such as temperature, humidity, fire suppression, and water ingress protection in alignment with resilience requirements. ☐ Develop standard templates for facility hardening, physical access logging, environmental monitoring, and emergency response procedures. ☐ Increase integration between physical security, facility management, and continuity teams to coordinate resilience improvements.
3 - <4	☐ Deploy a facility resilience enhancement programme addressing structural vulnerabilities, equipment ageing, and outdated safeguards. ☐ Assign facility resilience owners responsible for maintaining operational uptime and coordinating response to physical disruptions. ☐ Formalise escalation pathways when physical security system failures pose continuity or safety risks. ☐ Increase oversight of critical facilities (e.g., data centers, OT control rooms) to ensure physical controls function during extreme conditions.
4 - <5	☐ Urgent intervention required! Conduct immediate physical resilience testing following alarms, unexpected shutdowns, or near-miss events. ☐ Establish a cross-functional facility resilience team to address structural, environmental, and physical protection gaps. ☐ Implement mandatory reporting of physical security failures, environmental incidents, and control malfunctions requiring resilience intervention. ☐ Enforce a directive preventing the operation of critical facilities without fully functional physical and environmental controls verified for resilience.

Also refer to
10.Physical and Environmental Security PC12

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a resilience-focused physical and environmental security framework ensuring all critical facilities can operate under adverse or degraded conditions. ☐ Ensure environmental controls (power, cooling, humidity, fire suppression) are redundant, monitored, and tested for failover capability. ☐ Conduct periodic resilience assessments to validate that physical and environmental systems support required uptime and continuity standards. ☐ Maintain dashboards tracking environmental events, power irregularities, equipment health, and facility-level resilience indicators.
1 - <2	☐ Improve critical facility design by incorporating multi-path power, diverse cooling systems, and environmental zoning for high-availability requirements. ☐ Establish structured inspection and maintenance workflows for backup generators, UPS units, HVAC systems, and fire suppression equipment. ☐ Conduct alignment checks between environmental monitoring telemetry, facility layouts, and resilience documentation. ☐ Enhance documentation describing fallback procedures for environmental control failures and manual interventions required during emergencies.
2 - <3	☐ Perform comprehensive evaluations of facility environmental risks such as overheating, water ingress, vibration, contamination, or external hazards. ☐ Implement continuous monitoring for temperature, humidity, air quality, power stability, and early warning signs of environmental stress. ☐ Develop standard templates for environmental incident reporting, facility hardening, preventive maintenance, and continuity planning inputs. ☐ Increase integration between physical security, facility management, IT/OT operations, and resilience planning teams.
3 - <4	☐ Deploy a facility resilience uplift programme addressing outdated equipment, single points of failure, and insufficient environmental safeguards. ☐ Assign environmental resilience owners responsible for verifying system health, conducting tests, and remediating risks. ☐ Formalise escalation pathways when environmental conditions approach operational thresholds or present continuity risks. ☐ Increase oversight ensuring all critical equipment rooms maintain strict adherence to environmental control standards.
4 - <5	☐ Urgent intervention required! Conduct immediate inspection and remediation of facilities experiencing repeated alarms, temperature excursions, or power fluctuations. ☐ Establish a cross-functional environmental resilience task force to address critical weaknesses and plan infrastructure upgrades. ☐ Implement mandatory reporting of environmental deviations, power redundancy failures, and incidents impacting facility resilience. ☐ Enforce a directive preventing the operation of critical systems in environments not meeting verified physical and environmental resilience conditions.

Also refer to
10.Physical and Environmental Security IC5

Notes

RP Score

Checklist to follow

Operational Control

Resilience Management

0 - <1	☐ Maintain a resilience-oriented incident response framework ensuring continuity of critical services during disruptions, outages, or system degradation. ☐ Ensure incident scenarios incorporate continuity impacts, fallback options, and minimum viable service levels. ☐ Conduct periodic resilience-focused incident simulations to validate team preparedness for major outages and multi-system failures. ☐ Maintain dashboards tracking incidents affecting service availability, recovery times, degraded-mode operations, and continuity metrics.
1 - <2	☐ Improve incident classification to include resilience impact ratings such as service criticality loss, degraded capability, and operational dependency failures. ☐ Establish structured workflows ensuring prompt activation of resilience processes when incidents exceed predefined thresholds. ☐ Conduct alignment checks between incident plans, continuity plans, and redundancy designs to ensure integrated response capability. ☐ Enhance documentation capturing continuity actions taken during incidents, including fallback activation, resource reallocation, and service prioritisation.
2 - <3	☐ Perform end-to-end post-incident reviews focusing on resilience gaps, dependency weaknesses, and recovery delays. ☐ Implement recovery sequencing playbooks defining the order in which systems and services should be restored based on criticality. ☐ Develop standardized incident templates capturing downtime, root cause, impacted dependencies, and resilience lessons learned. ☐ Increase integration between incident response, business continuity, facility operations, and IT/OT engineering teams to accelerate service restoration.
3 - <4	☐ Deploy a continuity-focused incident uplift programme targeting slow recovery areas, unclear responsibilities, or resource bottlenecks. ☐ Assign resilience incident commanders responsible for coordinating cross-domain recovery actions and service stabilization. ☐ Formalise escalation workflows for incidents with potential to disrupt essential services or cause cascading operational failures. ☐ Increase oversight to ensure incident containment actions do not compromise redundancy, failover capability, or continuity posture.
4 - <5	☐ Urgent intervention required! Conduct a rapid resilience impact assessment during major incidents to identify high-risk functions requiring immediate stabilization. ☐ Establish a cross-functional major-incident resilience group to coordinate failover, fallback, and recovery tasks during severe disruptions. ☐ Implement mandatory reporting on resilience-impacting incidents, degraded-mode operations, and time-to-recover performance. ☐ Enforce a directive prohibiting service restoration closure until continuity requirements, dependency stabilization, and resilience verification are completed.

Also refer to
8.Security Incident Management OC2
15.Situational Awareness OC2

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a resilience-driven contingency planning framework defining fallback modes, continuity priorities, and minimum service levels for all critical operations. ☐ Ensure contingency plans incorporate operational dependencies, redundancy capabilities, and service-critical resource requirements. ☐ Conduct periodic resilience reviews to validate that contingency plans remain aligned with evolving processes, technologies, and business needs. ☐ Maintain dashboards tracking contingency plan coverage, test results, unresolved gaps, and readiness indicators across critical services.
1 - <2	☐ Improve contingency plans by incorporating scenarios such as partial outages, system degradation, supply chain disruption, and facility loss. ☐ Establish structured workflows ensuring contingency plans are activated rapidly when predefined resilience thresholds are breached. ☐ Conduct alignment checks between contingency plans, continuity plans, DR procedures, and redundancy architectures. ☐ Enhance documentation detailing fallback workflows, manual procedures, communication routes, and resource reallocation strategies.
2 - <3	☐ Perform practical simulations and continuity exercises to validate that teams can operate effectively in degraded or fallback modes. ☐ Implement defined recovery sequence protocols ensuring controlled restoration of services based on criticality and dependency maps. ☐ Develop standardised templates for fallback procedures, continuity resource lists, communication trees, and operational prioritisation schemes. ☐ Increase integration between contingency planning and operational readiness teams to ensure feasibility of fallback procedures.
3 - <4	☐ Deploy a maturity uplift programme focused on closing gaps identified during continuity tests or after major incidents. ☐ Assign contingency owners responsible for maintaining readiness, updating documentation, and coordinating training across teams. ☐ Formalise escalation workflows for disruptions that exceed contingency plan capacity or require cross-functional mobilisation. ☐ Increase oversight on external service providers to ensure their contingency capabilities align with organizational resilience requirements.
4 - <5	☐ Urgent intervention required! Conduct an immediate review of contingency plans for services recently impacted by outages, instability, or structural changes. ☐ Establish a cross-functional resilience coordination group to orchestrate fallback activation, manual operations, and service reprioritisation. ☐ Implement mandatory reporting on contingency invocations, gaps discovered, and operational challenges encountered during fallback execution. ☐ Enforce a directive preventing sign-off of contingency plans until they are fully tested, updated, and validated against key continuity objectives.

Also refer to
2.Risk Management DR1

Notes

RP Score

Checklist to follow

Disaster Recovery/ Business

Resilience Management

0 - <1	☐ Maintain a resilience-driven backup and recovery framework defining backup frequency, retention, critical asset coverage, and restoration priorities. ☐ Ensure all critical systems, databases, configurations, and operational data have validated backup strategies aligned with recovery objectives (RTO/RPO). ☐ Conduct periodic resilience reviews to confirm backup integrity, restoration success rates, and coverage gaps. ☐ Maintain dashboards showing backup status, failed jobs, restoration testing results, and recovery readiness for all critical environments.
1 - <2	☐ Improve backup strategies by incorporating immutable storage, air-gapped copies, versioning, and geographically diverse backup locations. ☐ Establish structured workflows ensuring critical backups are prioritised, validated, and monitored continuously. ☐ Conduct alignment checks between asset inventories, DR plans, and backup configurations to ensure consistency. ☐ Enhance documentation describing restoration procedures, failover workflows, and dependencies required for successful recovery.
2 - <3	☐ Perform comprehensive restoration drills to validate real-world recoverability, not just backup completion. ☐ Implement automated validation of backup integrity, comparing data consistency and identifying corruption or incomplete captures. ☐ Develop standard templates for backup schedules, risk ratings, retention policies, and recovery runbooks. ☐ Increase integration between backup systems, DR solutions, and continuity plans to ensure seamless failover and fallback capability.
3 - <4	☐ Deploy a recovery uplift programme targeting systems with slow restoration times, corrupted backups, or incomplete coverage. ☐ Assign backup and recovery owners responsible for ensuring readiness, monitoring failures, and maintaining restoration procedures. ☐ Formalise escalation workflows for repeated backup failures, restoration errors, or critical data not included in backup scope. ☐ Increase oversight on third-party or cloud-based backups to confirm compliance with resilience, encryption, and recovery requirements.
4 - <5	☐ Urgent intervention required! Conduct immediate restoration tests on critical systems with outdated or unverified backups. ☐ Establish a cross-functional recovery team to address systemic backup gaps, coordinate restoration during incidents, and improve recovery speed. ☐ Implement mandatory reporting on backup failures, restoration performance, unresolved issues, and risk exceptions. ☐ Enforce a directive prohibiting production operation of critical services without validated, restorable backups meeting resilience standards.

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a resilience-driven architectural framework defining required controls for continuity, failover, redundancy, and operational stability across all critical systems. ☐ Ensure resilient architecture designs explicitly address dependency mapping, capacity thresholds, degradation modes, and recovery pathways. ☐ Conduct periodic resilience validation to confirm deployed architectures behave as expected under stress, load, or partial system failures. ☐ Maintain dashboards highlighting resilience posture, dependency risks, architectural deviations, and observed recovery gaps.
1 - <2	☐ Improve resilient architecture by incorporating distributed design, multi-zone deployment, and tolerance for component-level failures. ☐ Establish structured workflows ensuring architectural resilience considerations are mandatory during new deployments and major changes. ☐ Conduct reconciliation checks between documented resilient architecture patterns, implementation details, and actual operational behaviour. ☐ Enhance documentation describing resilience logic, failover sequencing, fallback steps, dependency interactions, and recovery assurance conditions.
2 - <3	☐ Perform resilience stress tests simulating outages, latency spikes, resource exhaustion, and partial system loss to validate architectural robustness. ☐ Implement automated failover and validation mechanisms ensuring critical workloads transition seamlessly during disruptions. ☐ Develop standard templates for resilience architecture diagrams, risk assessments, fallback logic, and capacity management. ☐ Increase integration between resilience engineering, infrastructure teams, business continuity, and operations to ensure unified architectural intent.
3 - <4	☐ Deploy a resilience enhancement programme targeting brittle components, outdated architectural patterns, and high-dependency fragility. ☐ Assign resilience architects responsible for reviewing proposed changes, validating resilience controls, and coordinating improvements. ☐ Formalise escalation workflows when architectural failures threaten uptime, degrade critical service performance, or violate continuity objectives. ☐ Increase oversight ensuring all critical third-party integrations meet architectural resilience requirements and provide failover assurances.
4 - <5	☐ Urgent intervention required! Conduct an immediate resilience audit for systems with recent outages, cascading failures, or unanticipated behaviour. ☐ Establish a cross-functional resilience engineering squad to remediate high-risk architecture issues and design robust fallback pathways. ☐ Implement mandatory reporting on resilience deviations, failover anomalies, and recovery performance across critical systems. ☐ Enforce a directive preventing deployment or continued operation of systems that fail to meet defined resilient architecture criteria and validation tests.

Also refer to
5.Secure Design and Engineering DR3
14.Change Management DR3

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Physical and Environmental Security).
2. Locate the appropriate control within the Physical and Environmental Security domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

10 Physical and Environmental Security

10 Physical and Environmental Security | PC12

RP Score

Checklist to follow

Planning Controls

Physical and Environmental Security

0 - <1	☐ Maintain a comprehensive physical security framework defining access controls, surveillance coverage, and facility protection requirements for all critical areas. ☐ Ensure all critical rooms including data centres, OT control rooms, and telecom closets are protected by multi-layered physical access controls. ☐ Conduct periodic physical security inspections to validate functioning of CCTV, badge readers, intrusion sensors, and perimeter defences. ☐ Maintain dashboards showing access violations, unauthorised entry attempts, equipment tampering alerts, and physical security gaps.
1 - <2	☐ Improve physical perimeter design by incorporating restricted zones, mantraps, and monitored entry points for sensitive environments. ☐ Establish structured workflows to manage access provisioning, revocation, visitor control, and escort guidelines. ☐ Conduct alignment checks between physical access logs, HR records, and system access privileges to prevent inconsistencies. ☐ Enhance documentation describing physical control layouts, sensor coverage maps, camera retention standards, and guard duties.
2 - <3	☐ Perform threat-based assessments to identify vulnerable entry points, unmonitored areas, and blind spots. ☐ Implement tamper-evident seals, locking mechanisms, and protective enclosures for high-value or critical equipment. ☐ Develop standardized templates for physical security audits, access reviews, equipment protection guidelines, and visitor logs. ☐ Increase integration between physical security systems and security operations monitoring for unified alerting.
3 - <4	☐ Deploy a physical protection enhancement programme to upgrade ageing equipment, expand surveillance, and improve response capability. ☐ Assign physical security custodians responsible for facility readiness, control testing, and compliance with physical protection standards. ☐ Formalise escalation workflows for unauthorised access, equipment tampering attempts, or sensor failures. ☐ Increase oversight of third-party contractors performing work in restricted areas, ensuring adherence to physical security protocols.
4 - <5	☐ Urgent intervention required! Conduct an immediate physical security sweep following detection of unusual access patterns or facility alarms. ☐ Establish a cross-functional physical security response team to coordinate actions during suspected breaches or tampering events. ☐ Implement mandatory reporting of physical incidents, failed controls, maintenance gaps, and environmental concerns affecting security. ☐ Enforce a directive preventing operation of critical facilities without verified and functional physical security controls in place.

Also refer to
9. Resilience Management PC12

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a physical and environmental control framework ensuring all critical equipment is protected from temperature, humidity, dust, vibration, and power instability. ☐ Ensure data centres, equipment rooms, and OT environments maintain environmental conditions within vendor-defined tolerances. ☐ Conduct periodic environmental inspections validating performance of HVAC systems, sensors, alarms, and environmental redundancy. ☐ Maintain dashboards showing environmental deviations, power instability, cooling performance, and facility risk levels.
1 - <2	☐ Improve environmental control design by incorporating dual HVAC units, hot/cold aisle containment, and diverse power feeds. ☐ Establish structured workflows for environmental monitoring, escalation of alarms, and coordinated maintenance activities. ☐ Conduct alignment checks between environmental telemetry, facility designs, and operational load to detect early-stage failures. ☐ Enhance documentation detailing environmental standards, monitoring thresholds, alarm conditions, and corrective procedures.
2 - <3	☐ Perform comprehensive assessments identifying risks from fire, water ingress, chemical exposure, vibration, or structural weakness. ☐ Implement automated environmental alerting and failover mechanisms to reduce downtime and protect equipment integrity. ☐ Develop standard templates for facility checks, incident reporting, hazard assessments, and maintenance logs. ☐ Increase integration between facilities, IT, OT, and security to ensure environmental concerns are addressed before impacting operations.
3 - <4	☐ Deploy an environmental control improvement programme targeting obsolete infrastructure, weak redundancy, and high-risk environmental patterns. ☐ Assign environmental custodians responsible for monitoring, verifying alarm responses, and maintaining compliance with standards. ☐ Formalise escalation workflows for temperature excursions, humidity spikes, power anomalies, or critical environmental sensor failures. ☐ Increase oversight on generator testing, UPS health, battery backups, and electrical panel integrity.
4 - <5	☐ Urgent intervention required! Conduct immediate inspections following environmental alarms, equipment overheating, or recurring power fluctuations. ☐ Establish an environmental response team to coordinate corrective actions across facilities, engineering, and operations. ☐ Implement mandatory reporting on environmental incidents, unplanned outages, sensor failures, and facility risk conditions. ☐ Enforce a directive preventing operation of high-criticality equipment in environments that fail to meet approved physical and environmental control criteria.

Also refer to
9. Resilience Management IC5

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Data Protection).
2. Locate the appropriate control within the Data Protection domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

11 Data Protection

RP Score

Checklist to follow

Operational Control

Data Protection

0 - <1	☐ Maintain a formally approved data classification framework defining sensitivity levels, handling requirements, and protection controls. ☐ Ensure all data assets structured, unstructured, cloud-based, or OT-related are classified according to sensitivity and business impact. ☐ Conduct periodic classification reviews to confirm alignment with evolving regulatory, legal, and operational requirements. ☐ Maintain dashboards showing classification coverage, unclassified data volumes, and gaps in protection for sensitive categories.
1 - <2	☐ Improve classification metadata by integrating automated tagging tools and content inspection mechanisms. ☐ Establish structured workflows ensuring classification is applied at data creation, ingestion, modification, and archival. ☐ Conduct alignment checks between classification labels, access controls, encryption policies, and DLP configurations. ☐ Enhance documentation explaining classification criteria, retention obligations, and minimum security safeguards.
2 - <3	☐ Perform comprehensive discovery exercises to identify sensitive data stored in undocumented or unapproved locations. ☐ Implement encryption and tokenisation controls based on classification level and data criticality. ☐ Develop standard templates for data handling guidelines, protection rules, and classification decision matrices. ☐ Increase integration between data classification, IAM, cloud security, and DLP systems to ensure consistency.
3 - <4	☐ Deploy a classification maturity uplift programme targeting misclassified, unclassified, or incorrectly stored sensitive data. ☐ Assign data owners responsible for verifying classification accuracy and ensuring protection of high-sensitivity datasets. ☐ Formalise escalation workflows for improperly stored sensitive data, uncontrolled sharing, or classification violations. ☐ Increase oversight on third-party and cloud environments to ensure classified data receives mandated protection.
4 - <5	☐ Urgent intervention required! Conduct immediate discovery scans for sensitive data following audits, incidents, or suspected leakage events. ☐ Establish a classification governance committee to periodically review policies, exceptions, and regulatory changes. ☐ Implement mandatory reporting on classification non-compliance, protection gaps, and data movement anomalies. ☐ Enforce a directive preventing processing, sharing, or storage of sensitive data outside approved, protected environments.

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a comprehensive DLP framework governing monitoring, protection, and controlled movement of sensitive information. ☐ Ensure DLP policies reflect data classification levels, regulatory obligations, and organizational risk appetite. ☐ Conduct periodic DLP tuning to reduce false positives while improving detection of high-risk data movement. ☐ Maintain dashboards tracking DLP alerts, blocked transmissions, policy violations, and recurring data leakage patterns.
1 - <2	☐ Improve DLP rules by incorporating contextual, behavioural, and content-aware detection models. ☐ Establish structured workflows requiring triage, investigation, and closure of DLP incidents within defined timelines. ☐ Conduct alignment checks between DLP rules, data classification labels, encryption controls, and access rights. ☐ Enhance documentation outlining DLP policies, exception approval procedures, and monitoring thresholds.
2 - <3	☐ Perform full-spectrum DLP assessments covering email, endpoints, cloud storage, collaboration platforms, and removable media. ☐ Implement adaptive DLP controls to dynamically apply restrictions based on user role, data type, and risk indicators. ☐ Develop standard templates for DLP incident handling, root-cause analysis, and corrective action documentation. ☐ Increase integration between DLP and SIEM, CASB, cloud DLP, and insider risk systems to unify visibility.
3 - <4	☐ Deploy a data leakage reduction programme targeting persistent sources of risk such as overprivileged users and unmanaged data paths. ☐ Assign DLP custodians responsible for rule governance, events review, and continuous improvement. ☐ Formalise escalation pathways for high-severity DLP events involving sensitive or regulated data. ☐ Increase oversight on external data transfers, ensuring contracts, encryption, and monitoring requirements are enforced.
4 - <5	☐ Urgent intervention required! Conduct immediate investigation and containment upon detection of large-volume or suspicious data exfiltration attempts. ☐ Establish a DLP governance group to review policy gaps, approve exceptions, and evaluate new data channels requiring monitoring. ☐ Implement mandatory reporting on sensitive data movements, repeated violations, and unmonitored channels requiring DLP coverage. ☐ Enforce a directive preventing storage or transfer of classified data via channels not protected or monitored by DLP technologies.

Operational Control

Data Protection

Also refer to
2.Risk Management OC4

Notes

RP Score

Checklist to follow

Operational Control

Data Protection

0 - <1	☐ Maintain a cloud data protection framework defining encryption, retention, residency, access, and monitoring requirements for all cloud-stored data. ☐ Ensure classification-based protection controls are applied consistently across all cloud environments and storage repositories. ☐ Conduct periodic reviews to validate that cloud workloads comply with data governance, privacy, and protection standards. ☐ Maintain dashboards showing cloud data exposure, encryption coverage, misconfigured storage, and cross-region transfer events.
1 - <2	☐ Improve cloud data protection by integrating automated discovery tools to identify sensitive data stored in unapproved or unprotected cloud locations. ☐ Establish structured workflows requiring data sensitivity assessment before enabling new cloud storage or SaaS integrations. ☐ Conduct alignment checks between cloud IAM roles, data access privileges, encryption policies, and classification rules. ☐ Enhance documentation describing cloud data flows, access governance, retention schedules, and protection controls.
2 - <3	☐ Perform comprehensive assessments to identify misconfigured buckets, public-facing storage, overly permissive roles, or unencrypted data. ☐ Implement encryption-at-rest, encryption-in-transit, and customer-managed keys for sensitive cloud-hosted datasets. ☐ Develop standard templates for cloud data handling, residency controls, backup policies, and secure sharing guidelines. ☐ Increase integration between cloud security posture management (CSPM), DLP, and data classification systems for unified protection.
3 - <4	☐ Deploy a cloud data protection uplift programme addressing legacy storage, unmanaged APIs, and inconsistent encryption. ☐ Assign cloud data owners responsible for verifying compliance with data protection obligations across workloads. ☐ Formalise escalation workflows for cloud data exposure events, misconfigurations, or policy non-compliance. ☐ Increase oversight on vendor-managed SaaS and cloud services to ensure they enforce contractual and regulatory data controls.
4 - <5	☐ Urgent intervention required! Initiate rapid remediation for publicly exposed data, misconfigured cloud storage, or unencrypted sensitive datasets. ☐ Establish a cloud data protection committee to review exceptions, approve architecture, and evaluate emerging risks. ☐ Implement mandatory reporting on cloud data risks, encryption gaps, storage anomalies, and excessive data sharing patterns. ☐ Enforce a directive prohibiting deployment or integration of cloud services storing sensitive data without validated and compliant data protection controls.

Also refer to
5.Secure Design and Engineering OC8
12.Supply Chain Risk OC8

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a data lifecycle management framework defining secure disposal, destruction, archiving, and transfer requirements for sensitive information. ☐ Ensure all disposal and transfer activities follow classification-derived protection requirements and regulatory retention rules. ☐ Conduct periodic reviews of disposal processes to confirm effectiveness, completeness, and auditability. ☐ Maintain dashboards tracking disposal events, destruction verification, transfer approvals, and outstanding media items.
1 - <2	☐ Improve data disposal by adopting certified destruction methods, sanitisation standards, and tamper-proof chain-of-custody procedures. ☐ Establish structured workflows requiring approval, logging, and evidence of destruction for all high-sensitivity data assets. ☐ Conduct alignment checks between asset inventories, data repositories, disposal logs, and retention schedules. ☐ Enhance documentation describing disposal methods, transfer protocols, encryption requirements, and accountability roles.
2 - <3	☐ Perform comprehensive audits to identify stored sensitive data beyond approved retention periods. ☐ Implement secure transfer mechanisms including encryption, integrity validation, and custody verification for all sensitive data moves. ☐ Develop standard templates for disposal documentation, transfer approvals, shipping manifests, and chain-of-custody forms. ☐ Increase integration between disposal processes, backup policies, archives, and data classification systems.
3 - <4	☐ Deploy a data sanitisation programme addressing legacy media, decommissioned systems, and untracked storage locations. ☐ Assign disposal custodians responsible for validating destruction and ensuring compliance with legal and policy obligations. ☐ Formalise escalation workflows for lost media, incomplete destruction, or unverified disposal events. ☐ Increase oversight on third-party destruction providers to ensure compliance with contractual and security requirements.
4 - <5	☐ Urgent intervention required! Conduct immediate disposal review for media containing high-sensitivity data stored beyond retention limits. ☐ Establish a cross-functional data lifecycle group to coordinate archival, sanitisation, and disposal activities. ☐ Implement mandatory reporting on disposal failures, transfer incidents, and residual data discovered during audits. ☐ Enforce a directive preventing the disposal, re-use, or transfer of sensitive information-bearing assets without verified sanitisation and complete documentation.

Operational Control

Data Protection

Also refer to
3.Asset Management OC9

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Supply Chain Risk).
2. Locate the appropriate control within the Supply Chain Risk domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

12 Supply Chain Risk

RP Score

Checklist to follow

Planning Controls

Supply Chain Risk

0 - <1	☐ Maintain a supply chain security framework defining due-diligence, contractual obligations, risk assessment, and oversight requirements for all vendors. ☐ Ensure suppliers handling sensitive systems or data undergo mandatory security vetting prior to onboarding. ☐ Conduct periodic supplier risk reviews to validate ongoing compliance with security, privacy, and resilience obligations. ☐ Maintain dashboards showing supplier risk ratings, performance indicators, non-compliance trends, and contract expiration timelines.
1 - <2	☐ Improve supplier segmentation by categorising vendors based on criticality, access level, dependency, and business impact. ☐ Establish structured workflows enforcing NDA execution, data handling agreements, and security clauses before any engagement proceeds. ☐ Conduct alignment checks between supplier capabilities, contracted obligations, and actual security controls implemented. ☐ Enhance documentation describing supplier responsibilities, security controls, audit rights, and reporting obligations.
2 - <3	☐ Perform comprehensive assessments to identify high-risk suppliers lacking adequate controls, monitoring, or regulatory alignment. ☐ Implement a supplier onboarding checklist including security maturity, certifications, data policy compliance, and cyber incident history. ☐ Develop standard templates for security addendums, SLAs, data processing agreements, and third-party assurance reports. ☐ Increase integration between procurement, security, and risk teams to ensure supply chain decisions reflect organizational exposure.
3 - <4	☐ Deploy a supplier assurance programme targeting continuous monitoring of critical vendors through attestations, audits, or technical assessments. ☐ Assign vendor owners responsible for managing supplier relationships, tracking compliance, and raising escalations. ☐ Formalise escalation pathways for supplier non-compliance, security incidents, or refusal to implement required safeguards. ☐ Increase oversight on subcontractors to ensure cascading risk is not introduced through uncontrolled secondary engagements.
4 - <5	☐ Urgent intervention required! Conduct immediate reassessment of suppliers linked to recent vulnerabilities, breaches, or geopolitical concerns. ☐ Establish a cross-functional supply chain security committee to coordinate oversight, prioritise risks, and review contract compliance. ☐ Implement mandatory reporting on supplier incidents, exceptions, critical dependencies, and SLA breaches. ☐ Enforce a directive prohibiting engagement with suppliers without validated security controls, executed contracts, and approved risk ratings.

Also refer to
1.Governance PC10

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a third-party component evaluation framework requiring vendors to provide security assurance for supplied hardware and software. ☐ Ensure all procured components undergo vulnerability assessment, configuration review, and supply chain integrity checks before acceptance. ☐ Conduct periodic evaluations of vendor updates, patches, and firmware releases to identify inherited risks. ☐ Maintain dashboards showing evaluation results, component risk ratings, supplier issues, and unresolved vulnerabilities.
1 - <2	☐ Improve evaluation procedures by incorporating SBOM (Software Bill of Materials) analysis and hardware provenance checks. ☐ Establish structured workflows ensuring suppliers provide testing evidence, certifications, and security validation artifacts. ☐ Conduct alignment checks between supplier documentation, delivered configurations, and internal validation results to detect inconsistencies. ☐ Enhance documentation detailing evaluation criteria, approved configurations, defect findings, and remediation expectations.
2 - <3	☐ Perform comprehensive evaluations of critical components to identify hidden functionality, insecure dependencies, or unsupported firmware. ☐ Implement acceptance criteria requiring suppliers to remediate or justify vulnerabilities before components are deployed. ☐ Develop standard templates for supplier test reports, risk assessments, evaluation checklists, and approval summaries. ☐ Increase integration between component evaluation, procurement, asset management, and vulnerability teams for unified risk tracking.
3 - <4	☐ Deploy a supply chain testing programme targeting high-risk components such as network devices, OT controllers, and embedded systems. ☐ Assign evaluation owners responsible for validating component integrity and coordinating remediation with suppliers. ☐ Formalise escalation pathways for components found to be insecure, unsupported, or inconsistent with supplier claims. ☐ Increase oversight on vendor patching commitments, ensuring timelines and coverage align with organizational risk appetite.
4 - <5	☐ Urgent intervention required! Conduct immediate evaluation of components from suppliers linked to exposed vulnerabilities or suspected compromise. ☐ Establish a technical working group to assess supply chain-related vulnerabilities and coordinate remediation across teams. ☐ Implement mandatory reporting of insecure components, missing patches, unsupported versions, and supplier delays. ☐ Enforce a directive preventing procurement or deployment of components unless validated through testing and evaluation.

Implementation Control

Supply Chain Risk

Also refer to
5. Secure Design and Engineering IC6
6. Vulnerability and Patch Management IC6

Notes

RP Score

Checklist to follow

Operational Control

Supply Chain Risk

0 - <1	☐ Maintain a cloud supplier security framework defining contractual, technical, and monitoring requirements for all cloud service providers. ☐ Ensure cloud providers demonstrate compliance with data protection, encryption, logging, and regulatory requirements prior to onboarding. ☐ Conduct periodic cloud supplier assessments to validate adherence to agreed controls and shared responsibility obligations. ☐ Maintain dashboards showing cloud supplier risks, configuration drifts, SLA compliance, and exposure scenarios.
1 - <2	☐ Improve cloud supplier due-diligence by incorporating CSPM findings, vulnerability disclosures, and tenant isolation assurance. ☐ Establish structured workflows requiring review of provider documentation, certifications, and SOC reports prior to contract renewal. ☐ Conduct alignment checks between cloud provider capability, contractual commitments, and actual technical implementation. ☐ Enhance documentation describing cloud data flows, tenant boundaries, backup treatments, and provider-side security controls.
2 - <3	☐ Perform comprehensive reviews of provider service offerings to identify risks in storage, compute, identity, or networking layers. ☐ Implement mandatory encryption, MFA, logging, and key-management requirements for all cloud-hosted sensitive workloads. ☐ Develop standard templates for cloud due-diligence reports, SLA requirements, technical onboarding checklists, and risk assessments. ☐ Increase integration between cloud governance, vendor management, and cybersecurity teams for unified oversight.
3 - <4	☐ Deploy a cloud supplier assurance programme focusing on monitoring high-risk CSP services and validating cross-region resilience. ☐ Assign cloud supplier owners responsible for verifying compliance, assessing risk, and coordinating with CSPs. ☐ Formalise escalation routes for service outages, misconfigurations, SLA breaches, or emergent cloud vulnerabilities. ☐ Increase oversight on SaaS providers handling sensitive data, ensuring security attestations and technical controls are validated.
4 - <5	☐ Urgent intervention required! Initiate accelerated review of CSP environments impacted by new vulnerabilities, breaches, or supply chain advisories. ☐ Establish a cross-functional cloud risk committee to rationalise provider usage, evaluate emerging threats, and approve exceptions. ☐ Implement mandatory reporting on cloud supplier incidents, configuration violations, and unresolved security issues. ☐ Enforce a directive prohibiting cloud workloads from going live without completed supplier assessment and approval.

Also refer to
5.Secure Design and Engineering OC8
11.Data Protection OC8

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Workforce Management).
2. Locate the appropriate control within the Workforce Management domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

13 Workforce Management

RP Score

Checklist to follow

Planning Controls

Workforce Management

0 - <1	☐ Maintain a formally defined ISD structure with clearly documented roles, responsibilities, and reporting lines for all security functions. ☐ Ensure staffing levels within the ISD align with organizational size, threat landscape, and regulatory requirements. ☐ Conduct periodic workforce capability assessments to identify gaps in skills, competencies, and capacity. ☐ Maintain dashboards tracking ISD staffing maturity, open positions, training completion, and workload distribution.
1 - <2	☐ Improve job role definitions by incorporating specialised competencies required for SOC, IR, forensics, cloud, OT, and threat intelligence. ☐ Establish structured onboarding processes ensuring new ISD personnel receive domain-specific orientation and tools. ☐ Conduct alignment checks between ISD roles and operational expectations to ensure adequate coverage across all security domains. ☐ Enhance documentation detailing duty rotations, escalation responsibilities, and backup arrangements for key functions.
2 - <3	☐ Perform comprehensive workforce planning to anticipate skill needs, emerging technologies, and succession requirements. ☐ Implement training pathways enabling ISD personnel to progress through defined competency levels. ☐ Develop standard templates for role descriptions, capability assessments, and skill matrices. ☐ Increase integration between ISD, HR, and training teams to ensure timely recruitment and development interventions.
3 - <4	☐ Deploy a workforce maturity uplift programme to address skill shortages and enhance security operational effectiveness. ☐ Assign role custodians responsible for ensuring competency within their domain and mentoring junior staff. ☐ Formalise escalation workflows for resource shortages, workload overload, or service gaps requiring management intervention. ☐ Increase oversight on outsourcing or staff augmentation arrangements to ensure they meet competency and performance expectations.
4 - <5	☐ Urgent intervention required! Conduct a rapid skill gap assessment following major incidents, technology shifts, or compliance failures. ☐ Establish a cross-functional security leadership committee to coordinate workforce planning and strategic capability development. ☐ Implement mandatory reporting on ISD staffing risks, open roles, training progress, and capability improvements. ☐ Enforce a directive preventing assignment of high-risk or privileged duties to personnel without validated competency.

Also refer to
1.Governance PC3
8.Security Incident Management PC3

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a competency-driven certification framework defining required qualifications for each security role across the organization. ☐ Ensure personnel in critical cybersecurity functions hold certifications relevant to their responsibilities and technology domains. ☐ Conduct periodic reviews to validate certification status, renewal requirements, and coverage across high-impact areas. ☐ Maintain dashboards tracking certification maturity, gap areas, expiry timelines, and progress toward organizational targets.
1 - <2	☐ Improve certification requirements by incorporating emerging disciplines such as cloud, OT, data protection, and threat intelligence. ☐ Establish structured training paths enabling staff to pursue certifications based on role maturity and business needs. ☐ Conduct alignment checks between job descriptions, required certifications, and demonstrated skill levels. ☐ Enhance documentation outlining certification pathways, eligibility criteria, reimbursement policies, and development expectations.
2 - <3	☐ Perform comprehensive skill assessments to identify personnel requiring additional training or certification uplift. ☐ Implement continuous learning requirements such as CPE credits to maintain certification validity and current knowledge. ☐ Develop standardised matrices mapping certifications to roles, career progression, and competency categories. ☐ Increase integration of learning management systems, certification tracking tools, and performance management.
3 - <4	☐ Deploy a certification uplift programme targeting critical functions with low certification coverage. ☐ Assign certification coordinators responsible for tracking renewal schedules and supporting candidates. ☐ Formalise escalation workflows for expired, missing, or insufficient certifications in high-risk roles. ☐ Increase oversight on outsourced teams to ensure contracted personnel meet certification requirements.
4 - <5	☐ Urgent intervention required! Conduct an immediate certification audit following regulatory demands, audits, or major operational incidents. ☐ Establish a cross-functional competency board to approve exceptions, review pathways, and guide capability investments. ☐ Implement mandatory reporting on certification attainment, renewals, gaps, and staff readiness for upcoming projects. ☐ Enforce a directive prohibiting assignment of sensitive tasks to personnel lacking required certifications or up-to-date validations.

Also refer to
1.Governance PC11

Notes

RP Score

Checklist to follow

Operational Control

Workforce Management

0 - <1	☐ Maintain a formal security awareness framework defining training categories, frequency, delivery methods, and target audiences. ☐ Ensure all personnel including contractors and third parties complete mandatory security awareness training annually. ☐ Conduct periodic training effectiveness reviews to evaluate comprehension, behavioural change, and retention of security principles. ☐ Maintain dashboards showing training completion rates, assessment scores, and areas requiring targeted interventions.
1 - <2	☐ Improve awareness content by incorporating emerging threats, real incident examples, and sector-specific risk scenarios. ☐ Establish structured workflows ensuring new joiners complete foundational security training within defined timelines. ☐ Conduct alignment checks between training content, security policies, and observed incident trends to ensure relevance. ☐ Enhance documentation outlining training curricula, delivery schedules, role-specific modules, and learning objectives.
2 - <3	☐ Perform targeted awareness sessions for high-risk roles such as finance, HR, privileged users, and OT operators. ☐ Implement phishing simulations and behavioural testing to measure real-world readiness. ☐ Develop standard templates for campaign materials, assessment questions, and communication content. ☐ Increase integration between awareness programmes, insider risk management, and HR development initiatives.
3 - <4	☐ Deploy a behavioural uplift programme addressing recurring human errors and weak security practices. ☐ Assign awareness champions across departments to reinforce training messages and promote good practices. ☐ Formalise escalation workflows for repeated training non-compliance or high-risk behavioural violations. ☐ Increase oversight ensuring all personnel with access to sensitive systems receive specialised role-based training.
4 - <5	☐ Urgent intervention required! Deploy targeted awareness campaigns following major phishing waves, new threat advisories, or internal incidents. ☐ Establish a cross-functional training committee to review curriculum relevance and approve updates. ☐ Implement mandatory reporting of training gaps, behavioural risks, and trends observed during testing exercises. ☐ Enforce a directive prohibiting system access for personnel who fail to complete mandatory awareness training within the approved timeline.

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Change Management).
2. Locate the appropriate control within the Change Management domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

14 Change Management

RP Score

Checklist to follow

Planning Controls

Change Management

0 - <1	☐ Maintain a change-governed integration framework requiring all system integrations to undergo formal review, approval, and risk assessment before implementation. ☐ Ensure integration proposals include impact analysis on existing systems, data flows, dependencies, and operational stability. ☐ Conduct periodic change reviews to validate that all integrations follow approved patterns and do not introduce unassessed risks. ☐ Maintain dashboards tracking integration-related changes, pending approvals, deviations, failures, and post-change observations.
1 - <2	☐ Improve integration governance by incorporating structured risk scoring, dependency mapping, and business impact criteria into the change workflow. ☐ Establish workflows mandating CAB (Change Advisory Board) review for integrations affecting critical systems or cross-domain communication. ☐ Conduct alignment checks between integration change records, architecture documents, and implemented configurations to detect discrepancies. ☐ Enhance documentation for integration change requests, including rollback plans, configuration details, test evidence, and approval lineage.
2 - <3	☐ Perform pre-implementation testing of integrations in controlled environments to validate compatibility, stability, and security. ☐ Implement mandatory post-change validation to confirm operational readiness, performance baselines, and error-free interfacing. ☐ Develop standardised templates for integration change requests, impact statements, test plans, and authorization forms. ☐ Increase integration between change management, architecture, security, and operations teams to ensure all perspectives are included in approval decisions.
3 - <4	☐ Deploy an integration quality improvement programme targeting recurring integration issues, failures, or poorly documented changes. ☐ Assign integration owners responsible for coordinating testing, documenting changes, and validating successful deployment. ☐ Formalise escalation workflows for integration changes that fail testing, violate standards, or introduce unforeseen operational impacts. ☐ Increase oversight of vendor or third-party integrations to ensure changes are governed by internal approvals and meet baseline requirements.
4 - <5	☐ Urgent intervention required! Conduct immediate review of recent integrations following outages, performance degradation, or incident indicators. ☐ Establish a cross-functional integration review board to approve major integrations, evaluate risks, and guide remediation actions. ☐ Implement mandatory reporting of integration-related issues, change defects, and deviations from approved design or process. ☐ Enforce a directive prohibiting deployment of any new integration without complete testing, documented approvals, and successful post-change validation.

Also refer to
5.Secure Design and Engineering PC5

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a change-governed security architecture framework requiring all system, application, and infrastructure changes to undergo formal architectural review. ☐ Ensure architectural change proposals include security impact analysis, dependency considerations, and alignment with approved patterns. ☐ Conduct periodic reviews to validate that changes implemented in production adhere to approved security architecture principles. ☐ Maintain dashboards showing architecture-related change requests, deviations, exceptions, and post-change architectural issues.
1 - <2	☐ Improve architectural oversight by integrating threat modelling and impact simulation into the change evaluation process. ☐ Establish structured workflows mandating architectural sign-off before implementing major system upgrades, integrations, or reconfigurations. ☐ Conduct alignment checks between implemented changes, architectural diagrams, and baseline configurations to detect drift. ☐ Enhance documentation describing change rationale, design decisions, control implementations, and architectural exception cases.
2 - <3	☐ Perform architectural change assessments to identify security gaps, resilience weaknesses, or dependency failures introduced by modifications. ☐ Implement mandatory testing for high-impact architectural changes, ensuring resilience, segmentation, and control behaviour meet expectations. ☐ Develop standard templates for architectural change requests, approval artefacts, design deviations, and review findings. ☐ Increase integration between architecture, change management, operations, and security engineering to ensure cohesive change decisions.
3 - <4	☐ Deploy an architectural uplift programme targeting legacy design patterns, inconsistent configurations, and repeated architecture-related incidents. ☐ Assign architecture owners responsible for validating change proposals, guiding design decisions, and ensuring compliance with standards. ☐ Formalise escalation workflows for architectural changes that present high security risk, resilience impact, or potential service degradation. ☐ Increase oversight to ensure vendor-provided solutions or managed services align with architectural requirements before deployment.
4 - <5	☐ Urgent intervention required! Conduct accelerated architectural review following major incidents, outages, or systemic failures linked to recent changes. ☐ Establish a cross-functional architecture governance board to approve strategic changes, review exceptions, and prioritise remediation actions. ☐ Implement mandatory reporting on architectural deviations, exceptions, remediation progress, and recurring issues from change implementations. ☐ Enforce a directive preventing deployment of any architectural change not validated, approved, and documented in accordance with change governance standards.

Also refer to
5.Secure Design and Engineering PC7

Notes

RP Score

Checklist to follow

Planning Controls

Change Management

0 - <1	☐ Maintain a change-governed legacy integration framework defining mandatory assessments, risk scoring, and approval requirements for all legacy system modifications. ☐ Ensure all proposed integrations involving legacy systems include detailed risk evaluation covering vulnerabilities, unsupported components, and operational constraints. ☐ Conduct periodic reviews of legacy integration changes to validate compliance with approved standards and compensating control requirements. ☐ Maintain dashboards showing legacy-related change requests, dependency issues, compatibility risks, and post-change failures.
1 - <2	☐ Improve legacy integration governance by incorporating enhanced risk scoring for outdated technologies, unsupported software, and deprecated architectures. ☐ Establish structured workflows mandating CAB review and architectural approval for any integration introducing legacy system dependencies. ☐ Conduct alignment checks between legacy system configurations, integration change records, and established security baselines to identify drift. ☐ Enhance documentation describing legacy interface constraints, compensating controls, security exceptions, and technical debt associated with each integration.
2 - <3	☐ Perform compatibility testing for legacy integrations to validate stability, performance, and resilience under expected operational loads. ☐ Implement mandatory mitigation measures such as isolation, segmentation, or gateway enforcement when integrating legacy systems with modern environments. ☐ Develop standard templates for legacy integration assessments, exception justifications, and approval documentation. ☐ Increase integration between architecture, security engineering, and operations teams to ensure legacy limitations are understood during change planning.
3 - <4	☐ Deploy a legacy risk reduction programme targeting replacement, containment, or isolation of high-risk legacy components. ☐ Assign legacy system custodians responsible for validating configuration integrity and coordinating integration-related changes. ☐ Formalise escalation workflows for legacy integrations that introduce unacceptable security risk or deviation from approved standards. ☐ Increase oversight on vendor support arrangements and end-of-life schedules to proactively plan for legacy system replacement.
4 - <5	☐ Urgent intervention required! Conduct immediate review of all legacy integrations following any incident, outage, or security alert involving outdated components. ☐ Establish a cross-functional legacy integration committee to evaluate high-impact changes and prioritise remediation actions. ☐ Implement mandatory reporting on legacy-specific change failures, recurring defects, and residual risks requiring management attention. ☐ Enforce a directive prohibiting deployment of new integrations to legacy systems unless all risks are assessed, controls validated, and approvals completed.

Also refer to
5.Secure Design and Engineering PC9

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a deployment governance framework ensuring all architectural changes undergo formal review, approval, and controlled release processes. ☐ Ensure deployment requests include detailed design artefacts, resilience expectations, dependency mapping, and change impact analysis. ☐ Conduct periodic deployment audits to validate adherence to approved architecture patterns, resilience controls, and configuration baselines. ☐ Maintain dashboards showing deployment readiness, change success rates, rollback events, and resilience validation findings.
1 - <2	☐ Improve deployment governance by integrating resilience scoring, dependency checks, and architectural risk analysis into the change approval process. ☐ Establish structured workflows requiring CAB and architectural sign-off for all deployments affecting critical infrastructure, cloud workloads, or OT systems. ☐ Conduct alignment checks between deployed configurations, approved design documents, and resilience requirements to detect drift. ☐ Enhance documentation detailing pre-deployment checks, resilience safeguards, test results, rollback procedures, and deployment authorisations.
2 - <3	☐ Perform controlled deployment testing such as smoke tests, failover tests, and controlled break simulations to validate stability and resilience. ☐ Implement mandatory pre-deployment and post-deployment validation to confirm resilience objectives are met and no unintended impacts are introduced. ☐ Develop standard templates for deployment change requests, stability testing, resilience verification, and sign-off records. ☐ Increase integration between architecture, change management, operations, and resilience engineering teams to ensure cohesive deployment decisions.
3 - <4	☐ Deploy a deployment quality improvement programme targeting recurring deployment failures, configuration mismatches, and resilience issues. ☐ Assign deployment owners responsible for coordinating change execution, validating outcomes, and ensuring compliance with approval requirements. ☐ Formalise escalation workflows for deployments that fail validation, cause service degradation, or deviate from approved architecture. ☐ Increase oversight on vendor-managed deployments or third-party changes to ensure adherence to organizational deployment standards.
4 - <5	☐ Urgent intervention required! Conduct immediate resilience and stability reviews for recent deployments linked to incidents or performance anomalies. ☐ Establish a deployment governance board to evaluate high-impact changes, approve major rollouts, and oversee remediation actions. ☐ Implement mandatory reporting on deployment metrics, failure trends, exception handling, and resilience test performance. ☐ Enforce a directive prohibiting production deployment of any architectural change without complete testing, validated resilience controls, and formal approval in accordance with change governance standards.

Also refer to
5.Secure Design and Engineering DR3
9.Resilience Management DR3

Notes

Instructions

1. Retrieve the calculated RP score from workbook 1 (Situational Awareness).
2. Locate the appropriate control within the Situational Awareness domain.
3. Select the RP range that corresponds to the calculated score.
4. Complete the respective checklist for that control.

Disclaimer

Self-perception differences may cause the calculated RP score to differ from the defined range, it is recommended to complete all checklists from bottom to top to ensure maximum compliance.

15 Situational Awareness

RP Score

Checklist to follow

Planning Controls

Situational Awareness

0 - <1	☐ Maintain a dynamic interdependency mapping framework to identify upstream and downstream relationships across business services and systems. ☐ Ensure interdependency maps reflect real-time operational behaviour, critical asset relationships, and service-level dependencies. ☐ Conduct periodic mapping reviews to validate that changes in infrastructure, integrations, or business processes are accurately captured. ☐ Maintain dashboards visualising dependency risks, single points of failure, and potential cascading impact zones.
1 - <2	☐ Improve situational awareness by integrating monitoring data, logs, and performance metrics into dependency visualisation tools. ☐ Establish structured workflows requiring teams to update dependency models following major system changes or integration updates. ☐ Conduct alignment checks between documented dependencies and actual runtime interactions observed through monitoring tools. ☐ Enhance documentation describing dependency criticality, tolerance thresholds, fallback options, and resilience expectations.
2 - <3	☐ Perform dependency risk assessments to identify segments that may amplify service disruption during incidents. ☐ Implement continuous monitoring for anomalies in dependency behaviours, such as unexpected traffic spikes or degraded service chains. ☐ Develop standard templates for interdependency analysis, risk scoring, and impact evaluation. ☐ Increase integration of interdependency data with incident detection, threat intelligence, and operational analytics platforms.
3 - <4	☐ Deploy a dependency visibility uplift programme targeting blind spots, undocumented connections, and emerging integration risks. ☐ Assign dependency owners responsible for validating accuracy and reporting changes in their service domains. ☐ Formalise escalation pathways for dependency failures that pose organization-wide operational or security risks. ☐ Increase oversight on third-party dependencies to ensure visibility into external service performance and risk posture.
4 - <5	☐ Urgent intervention required! Conduct a rapid dependency analysis during major incidents to determine potential propagation paths. ☐ Establish a cross-functional dependency intelligence committee to review systemic risks and recommend mitigation strategies. ☐ Implement mandatory reporting on dependency anomalies, mismatches, and incidents arising from inter-service interactions. ☐ Enforce a directive requiring all critical service teams to maintain accurate and continuously updated dependency documentation.

Also refer to

- 1.Governance PC2
- 2.Risk Management PC2
- 7.Threat Intelligence PC2
- 9.Resilience Management PC2

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a centralised monitoring framework defining logging standards, telemetry coverage, and detection requirements across all environments. ☐ Ensure all critical assets generate event data aligned with detection use cases and organizational risk scenarios. ☐ Conduct periodic monitoring maturity assessments to validate coverage, timeliness, and effectiveness of detection rules. ☐ Maintain dashboards showing alert volume, detection quality, false-positive rates, and coverage gaps.
1 - <2	☐ Improve situational awareness by integrating logs from IT, OT, cloud, network, and identity systems into unified monitoring platforms. ☐ Establish structured triage workflows ensuring timely classification, assignment, and analysis of alerts. ☐ Conduct alignment checks between monitoring configurations, threat intelligence, and attack surface changes. ☐ Enhance documentation covering detection use cases, log sources, tuning logic, and alert thresholds.
2 - <3	☐ Perform continuous detection rule tuning to respond to emerging threats, environmental changes, and observed incident patterns. ☐ Implement behavioural analytics, anomaly detection, and entity-based monitoring to increase visibility into subtle threat indicators. ☐ Develop standard templates for detection playbooks, alert handling procedures, and monitoring guidelines. ☐ Increase integration between SOC, threat intelligence, and operations teams to enhance contextual awareness.
3 - <4	☐ Deploy a monitoring uplift programme targeting log source expansion, tuning improvements, and use-case maturity. ☐ Assign detection engineers responsible for maintaining rule accuracy, reducing noise, and improving alert fidelity. ☐ Formalise escalation workflows for severe or high-confidence detections requiring urgent investigation. ☐ Increase oversight on cloud, OT, and third-party environments to ensure monitoring data is complete and timely.
4 - <5	☐ Urgent intervention required! Investigate detection gaps following major incidents, SOC observations, or unexpected system behaviours. ☐ Establish a detection governance committee to review rule quality, prioritise improvements, and approve new use cases. ☐ Implement mandatory reporting on detection failures, inconsistencies, delayed alerts, and unresolved anomalies. ☐ Enforce a directive preventing the operation of critical systems without validated logging and monitoring capabilities.

Operational Control

Situational Awareness

Also refer to
8.Security Incident Management OC2
9.Resilience Management OC2

Notes

RP Score

Checklist to follow

Operational Control

Situational Awareness

0 - <1	☐ Maintain an APT-focused monitoring framework using behavioural analytics, advanced telemetry, and threat intelligence integration. ☐ Ensure detection rules map to known adversary TTPs from frameworks such as MITRE ATT&CK. ☐ Conduct periodic visibility assessments to validate telemetry sufficiency for detecting lateral movement, persistence, and other APT behaviours. ☐ Maintain dashboards showing APT-related anomalies, suspicious behaviours, and threat hunt findings.
1 - <2	☐ Improve detection coverage by integrating network, identity, endpoint, and OT telemetry for cross-domain threat correlation. ☐ Establish structured workflows for deep investigation of APT-like anomalies, including enriched context gathering and correlation. ☐ Conduct alignment checks between APT intelligence updates and the organization's monitoring and detection configurations. ☐ Enhance documentation detailing observed tactics, potential adversary profiles, and forensic indicators.
2 - <3	☐ Perform periodic threat hunts to proactively identify undetected or stealthy adversarial activity. ☐ Implement deception technologies and honeypots to enhance visibility into attacker behaviour. ☐ Develop standard templates for threat hunt hypotheses, findings, and recommended mitigation actions. ☐ Increase integration of APT detection with SOC operations, incident response, and situational intelligence platforms.
3 - <4	☐ Deploy an APT-awareness improvement programme ensuring teams understand high-risk behaviours and adversary tradecraft. ☐ Assign threat hunters responsible for evaluating APT patterns, validating anomalies, and escalating suspicious findings. ☐ Formalise escalation routes for suspected APT indicators requiring immediate leadership and external notification. ☐ Increase oversight on privileged access, identity anomalies, and system behaviours often exploited by APT actors.
4 - <5	☐ Urgent intervention required! Initiate emergency hunts following sector advisories, intelligence alerts, or geopolitical escalations. ☐ Establish a cross-functional APT visibility committee to evaluate readiness, review anomalies, and prioritise improvements. ☐ Implement mandatory reporting on APT indicators, detection limitations, and visibility gaps. ☐ Enforce a directive requiring high-risk systems to maintain enhanced APT monitoring and behavioural visibility.

Also refer to
7.Threat Intelligence OC11
8.Security Incidence Management OC11

Notes

RP Score

Checklist to follow

0 - <1	☐ Maintain a threat reporting framework ensuring timely and accurate submission of relevant incidents, anomalies, and indicators to government agencies. ☐ Ensure reporting criteria incorporate severity, national impact, regulatory requirements, and intelligence relevance. ☐ Conduct periodic assessments of reporting readiness to validate processes, documentation, and communication pathways. ☐ Maintain dashboards tracking all reports sent, pending submissions, feedback received, and agency interactions.
1 - <2	☐ Improve reporting processes by integrating automated intelligence correlation and prioritisation tools. ☐ Establish structured workflows assigning responsibilities for evidence preparation, validation, and approval of threat reports. ☐ Conduct alignment checks between internal detections, incident findings, and government reporting frameworks. ☐ Enhance documentation outlining reporting requirements, timelines, content expectations, and roles.
2 - <3	☐ Perform correlation analysis between national advisories and internal observations to identify report-worthy events. ☐ Implement mechanisms to record, track, and evaluate feedback from government agencies. ☐ Develop standard templates for reports, escalation notes, and structured threat submissions. ☐ Increase integration between SOC, IR, legal, and compliance to ensure reporting accuracy and timeliness.
3 - <4	☐ Deploy a reporting quality improvement programme targeting completeness, precision, and actionable intelligence. ☐ Assign reporting officers responsible for managing communications with agencies and validating report content. ☐ Formalise escalation workflows for events requiring immediate government notification. ☐ Increase oversight to ensure sensitive data shared with authorities meets privacy and legal requirements.
4 - <5	☐ Urgent intervention required! Perform accelerated submission of threat indicators following widespread attacks or sector-specific advisories. ☐ Establish a structured liaison mechanism with CERT-In, NCIIIPC, and sector regulators to improve situational awareness exchange. ☐ Implement mandatory reporting on missed deadlines, incomplete submissions, and delayed communications. ☐ Enforce a directive requiring all reportable threats to be submitted within defined timelines and validated through appropriate channels.

Notes

RP Score

Checklist to follow

Reporting and Accountability

Situational Awareness

0 - <1	☐ Maintain a periodic audit and assessment programme providing visibility into organizational cybersecurity posture and exposure. ☐ Ensure assessments cover critical assets, business processes, cloud workloads, OT systems, and third-party elements. ☐ Conduct periodic vulnerability assessments to identify evolving exposure and misconfiguration risks. ☐ Maintain dashboards showing audit findings, vulnerability trends, high-risk areas, and unresolved issues.
1 - <2	☐ Improve situational awareness by correlating audit findings with threat intelligence and environmental changes. ☐ Establish structured workflows to prioritise, assign, and track remediation of audit findings and identified vulnerabilities. ☐ Conduct alignment checks between audit recommendations, policy requirements, and implemented controls. ☐ Enhance documentation describing risk themes, systemic weaknesses, and audit methodologies.
2 - <3	☐ Perform targeted assessments to investigate emerging risk areas or recurring issues. ☐ Implement continuous scanning of critical assets to maintain visibility into real-time exposure. ☐ Develop standard templates for audit reports, vulnerability summaries, and remediation plans. ☐ Increase integration of audit and vulnerability data with SOC, risk, and governance teams.
3 - <4	☐ Deploy a visibility enhancement programme focused on closing blind spots identified in assessments. ☐ Assign audit liaisons responsible for ensuring findings are properly documented, tracked, and resolved. ☐ Formalise escalation routes for overdue high-severity findings requiring leadership action. ☐ Increase oversight on third-party assessments to validate independence, competence, and coverage.
4 - <5	☐ Urgent intervention required! Conduct accelerated assessments following major environmental changes or confirmed incidents. ☐ Establish a governance board to review assessment results, track remediation, and prioritise high-impact issues. ☐ Implement mandatory reporting on assessment deficiencies, unresolved vulnerabilities, and posture gaps. ☐ Enforce a directive requiring closure or risk acceptance of all critical findings within approved timelines.

Also refer to
 1. Governance RA2
 2. Risk Management RA2
 6. Vulnerability and Patch Management RA2

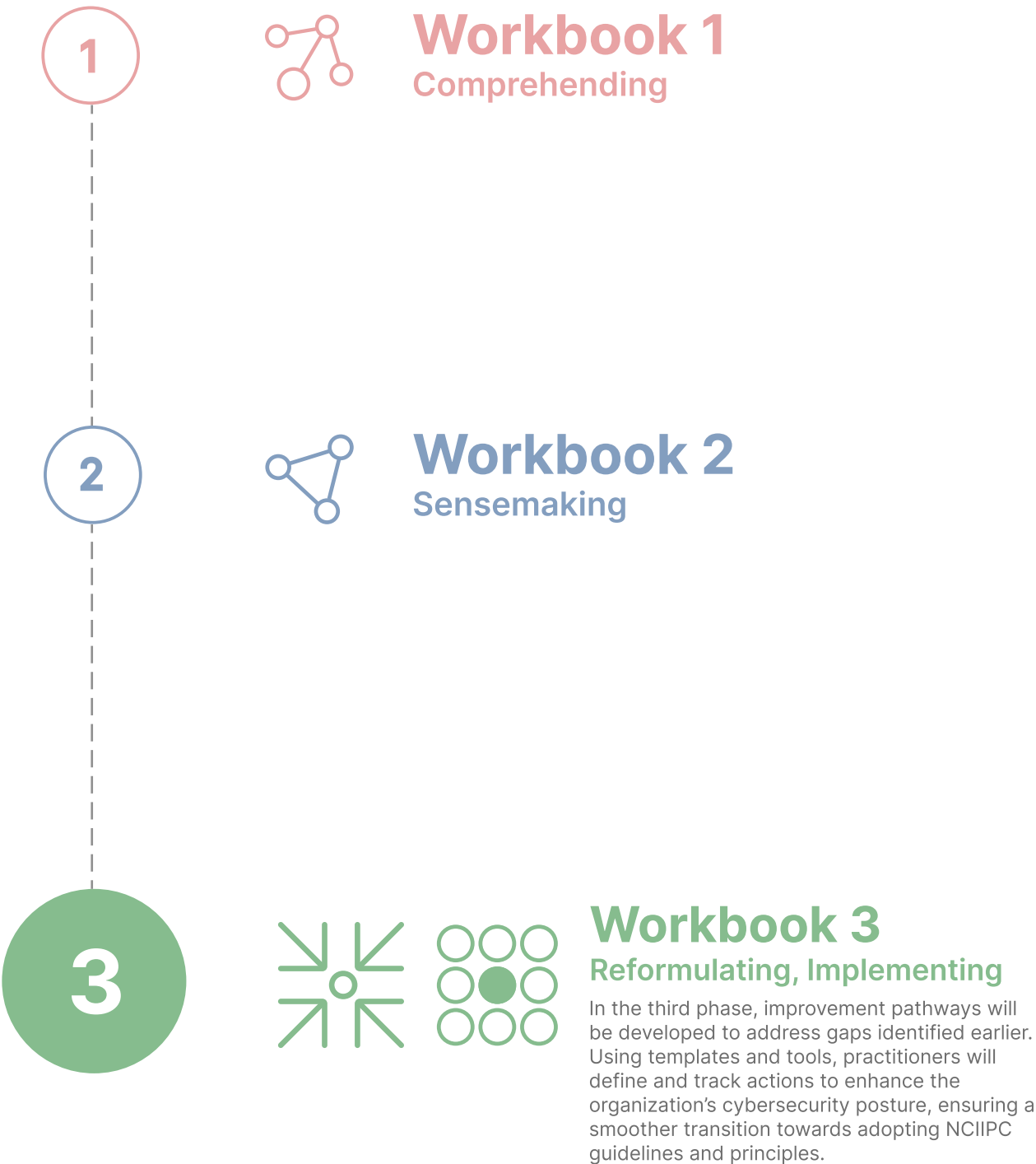
Notes

Navigating Through the Workbooks

Next Phase - Workbook 3: Reformulating, Implementing

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 Sensemaking 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