



Workbook for NCIIPC based Transformation of Indian Organizations

Enhancing the Cybersecurity Posture for Critical
Information Infrastructures

Reformulating,
Implementing

3,4

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



9 789361 282539

Navigating Through the Workbooks

Current Phase - Workbook 3: Reformulating, Implementing

How to use this workbook along with others?

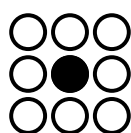
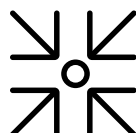
This workbook functions as part of a progressive series designed to guide organizations through various stages of cybersecurity maturity. Each workbook builds upon insights from the previous one, ensuring a structured and continuous improvement process. When used collectively, they create an integrated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



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
Reformulating	11
Domain and Control Comparison Matrix.....	12
Risk Priority & Business Continuity Impact.....	14
Strategic Planning for Domains.....	15
Strategic Planning for Controls.....	18
Resource Mapping: Current Scenario.....	20
Resource Mapping: Alternate Scenarios.....	22
Mapping for Human Systems Integration.....	24
Resource Planning for Inclusive Change.....	26
Consensus Formation.....	28
Implementing	31
Action Priority Matrix.....	32
Implementation- Prioritize.....	33
Implementation- Execute.....	34
Implementation- Schedule.....	35
Implementation- Postpone.....	36



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

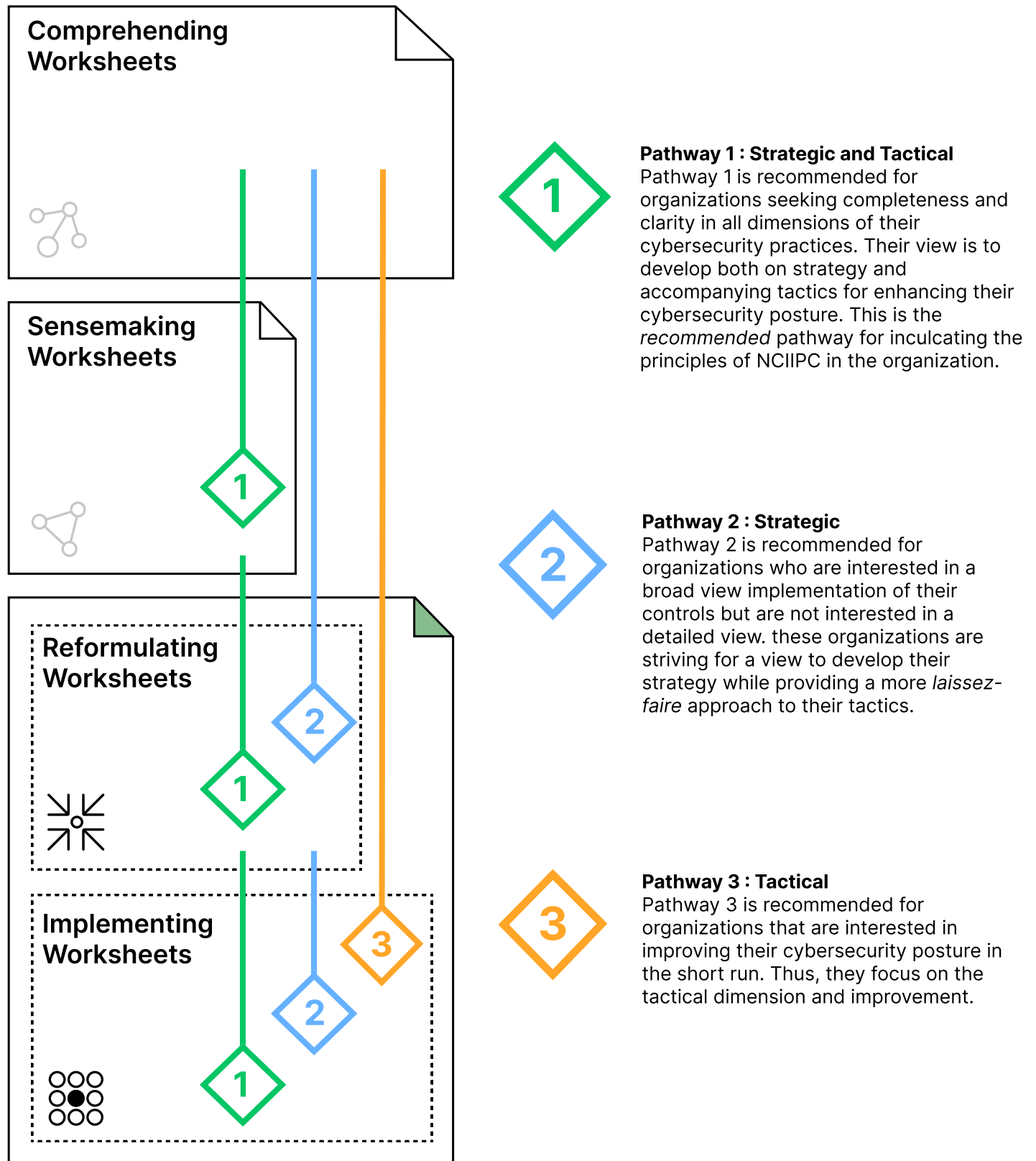
In this third phase, improvement pathways are created by delving into particular domains and controls in multiple ways. These can be made possible by the use of templates that provide clarity and insight into the particular areas.

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.

Guide - 1

4 Strategic Planning for Controls

Reformulating Worksheet

2

Second step is to execute the Reformulating Worksheets (Pages 10 to 21). These pages are designed as a set of analytical tools to be completed as a group.

The Reformulating Worksheets are not just forms; they are large-format analytical tools designed to facilitate dynamic, hands-on sessions. You should ideally print these templates out (A3 size is recommended for collaboration) for team use. This collaborative setting is vital for CISOs and senior management to drive brainstorming activities and utilize a systems-thinking approach. The workbook's structure supports this: the left side provides the complete description, context, and a pre-filled example for immediate understanding, while the right side contains the blank template (like '4 Strategic Planning for Controls') for documenting your team's unique data.

How to use the worksheets

Guide - 2

X Worksheet Title
Implementation Worksheet

This Worksheet helps in categorizing the Domain and Controls based on Importance and Urgency
1. Based on worksheets 1-8, categorize the identified Domains and Controls under each Quadrant
• Refer to the scorecard of each Domain for the RP scores and categorize the Domains and associated controls one by one to each quadrant
• Prioritize: Refers to the Domains and Controls that are Important and needs Urgent Implementation
• Execute: Refers to the Domains and Controls that are Less Important but needs Urgent Implementation
• Schedule: Refers to the Domains and Controls that are Important but are Less Urgent
• Postpone: Refers to the Domains and Controls that are Less Important and are Less Urgent

Important	Urgent	Less Urgent
	A.Prioritize Domain 2 Controls IC5, OC5, OC7 Intervention	C.Schedule Domain 4 Controls IC2 Intervention 1 Intervention2
Less Important	B.Execute Domain 1 Controls PC1 Intervention Domain 5 Controls PC2, IC4, RAI Intervention Domain 7 Controls OC8 Intervention	D.Postpone Domain 9 Controls PC9, DR3 Intervention Domain 6 Controls OC2, OC4, DR1 Intervention

3 Fifth step involves the Implementation Worksheet section. These would help you in comprehending the data gathered from the sensemaking worksheets and aid in successful implementation of the identified action courses.

Implementation Worksheet will have a description and a step by step approach to successfully execute the activity. All the Implementation Worksheets are arranged in a logical manner and so ideally it would be the best to follow the Worksheet sequence to yield the maximum benefits.

This is the section where you will write the Domains and Controls and its intervention(s) identified under each quadrant. These are categorized in terms of - Prioritize, Execute, Schedule, Postpone. Complete the Worksheets to make each quadrant actionable with respect to your organization.

X Implementation - Quadrant #
Implementation Worksheet

This Worksheet helps in keeping track of the Implementation of the Controls
1. Refer to A. Prioritize Quadrant of the Worksheet 0 and fill the table below
• Fill the table with all the Domains and associated Controls identified in the Prioritize Quadrant

Domain #	Control #	Responsibility	Timeline	Completion Date	Status
Domain 2	IC5	Shubh Singh	1 week	25/07/25	☒
	OC5	Aniket R	3 weeks	12/08/25	☐
	OC7	Shrinivas M	1 month	19/08/25	☐
E.g. Domain 5	PC2	E.g. Vivek Kant	E.g. 1 week	DD/MM/YY	☒
	IC4	E.g. Soham M	E.g. 1 week	DD/MM/YY	☐
	OC3	E.g. Thomas Raju	E.g. 1 week	DD/MM/YY	☐

4 Sixth step involves filling the 4 Worksheets under the Implementation section. These Worksheets will help in making the implementational steps more actionable

Each Quadrant has its own Implementational Worksheet where you can list down the identified Domains and Controls and assign responsibility, timeline, completion date and can track it for successful implementation.



Reformulating

3

1 Domain & Control Comparison Matrix

Reformulating Worksheet - Example

This Worksheet gives an overview of the organization's Domain posture with respect to NCIIPC controls

1. Fill the Average RP score for each domain and control group respectively
 - Refer to the scorecard page for each domain and fill the white boxes in the matrix
2. Compare the scores of the Domain and associated control to understand their relationship

	Planning Control	Implementation Control	Operational Control	Disaster Recovery/ Business	Reporting and Accountability
1. Governance	3,2	4			2,1
2. Risk Management	1		2,1	5	3
3. Asset Management	3	3,2	2,5		
4. Identity & Access Mgmt		4	2,5		
5. Secure Design & Engineering	3	2	2	4	
6. Vulnerability & Patch Mgmt	4	2,1	3,2		2,5
7. Threat Intelligence	2		3		2
8. Security Incident Mgmt	2,5		4		
9. Resilience Management	3,2	2,1	3	2	
10. Physical & Environmental Security	3	2,1			
11. Data Protection			3		
12. Supply Chain Risk	2,1	2,5	4		
13. Workforce Management	2,5		3,2		
14. Change Management	4			3	
15. Situational Awareness	2,1	4	3		2,5

1 Domain & Control Comparison Matrix

Reformulating Worksheet - Template

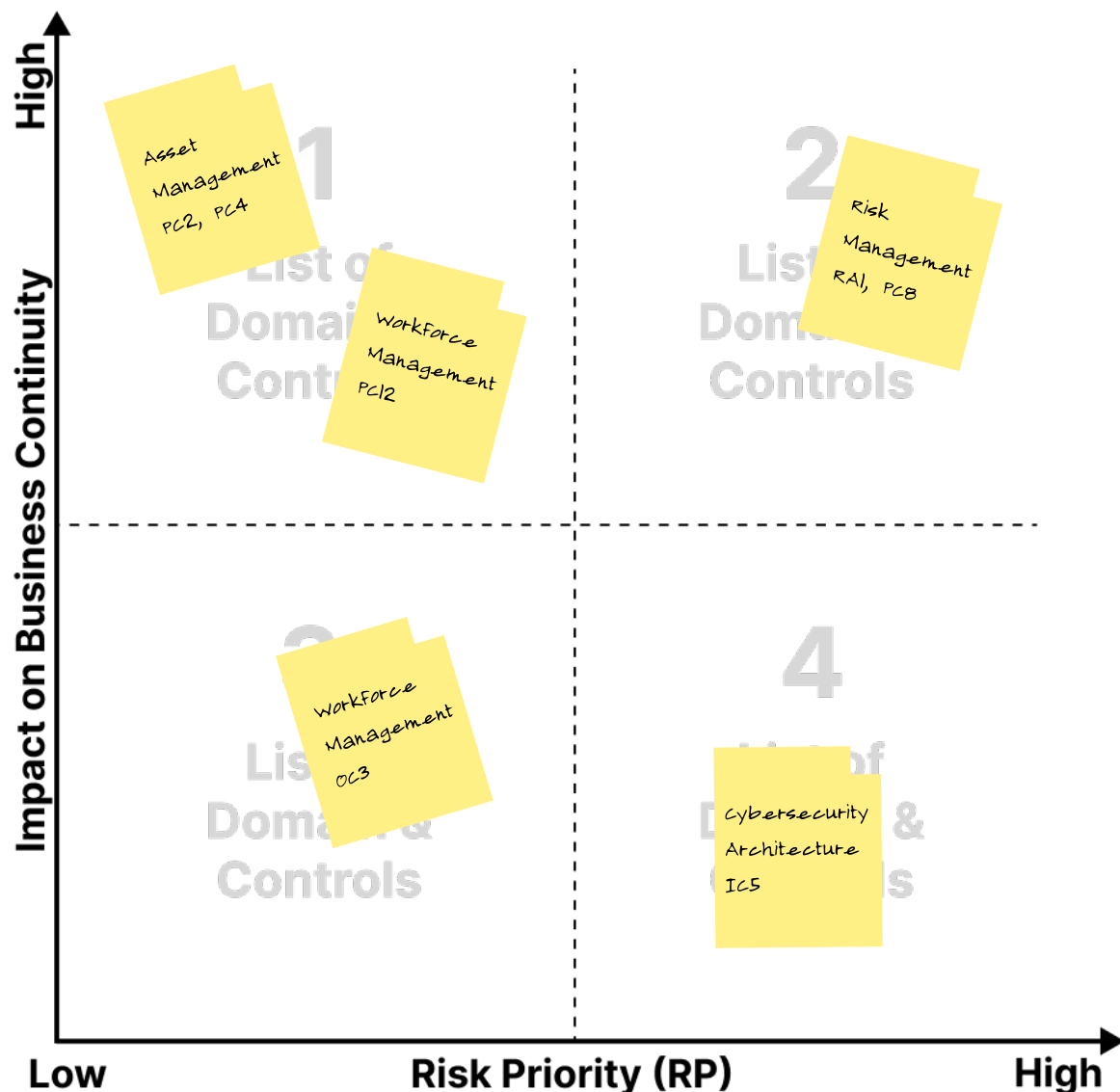
	Planning Control	Implementation Control	Operational Control	Disaster Recovery/ Business	Reporting and Accountability
1. Governance					
2. Risk Management					
3. Asset Management					
4. Identity & Access Mgmt					
5. Secure Design & Engineering					
6. Vulnerability & Patch Mgmt					
7. Threat Intelligence					
8. Security Incident Mgmt					
9. Resilience Management					
10. Physical & Environmental Security					
11. Data Protection					
12. Supply Chain Risk					
13. Workforce Management					
14. Change Management					
15. Situational Awareness					

2 Risk Priority & Business Continuity Impact

Reformulating Worksheet - Example

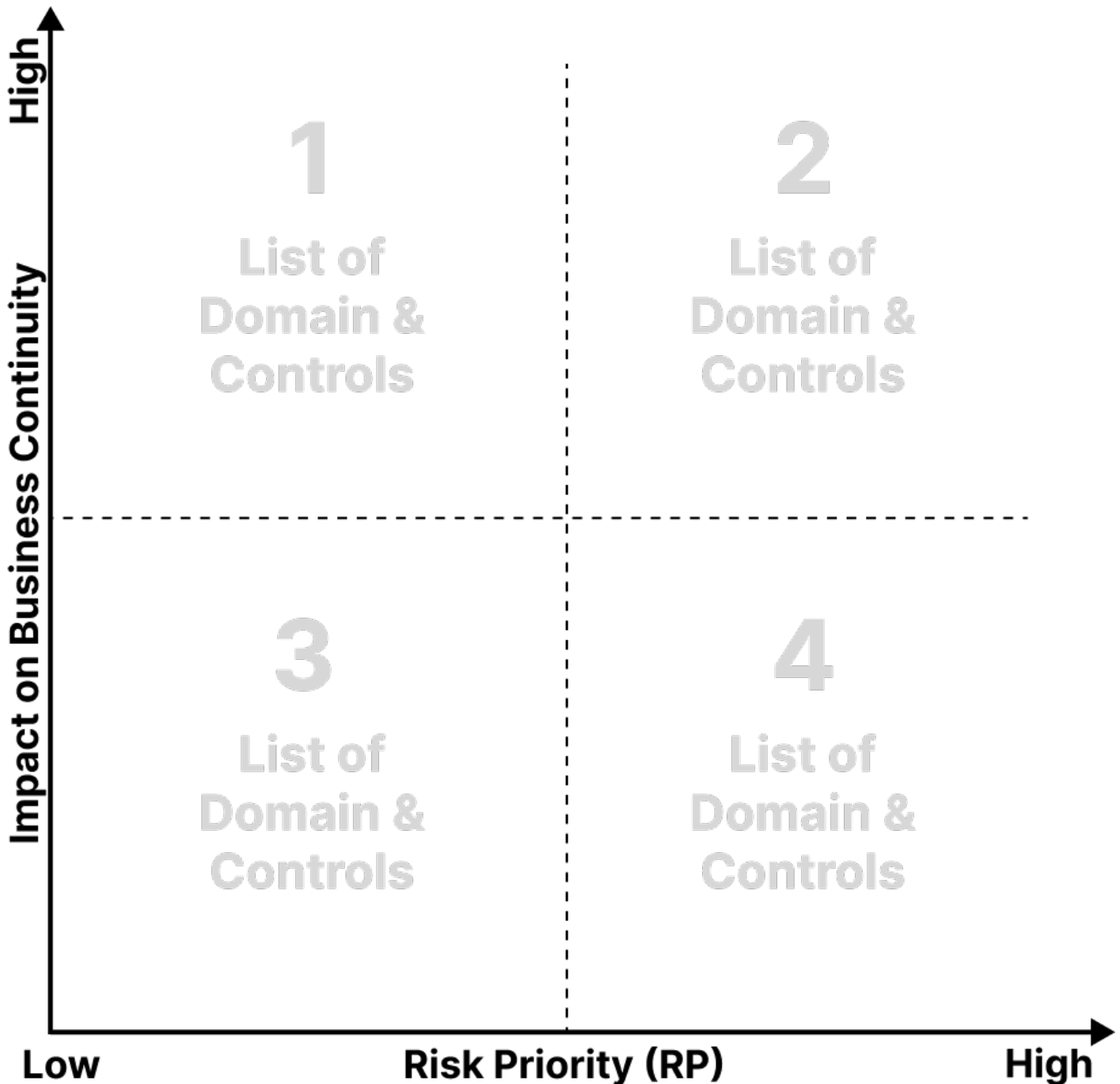
This Worksheet compares the Risk Priority Score (RP) to the Impact on Business Continuity.

- Refer to the scorecard page for each domain
1. Based on the results from Reformulating Worksheet 1, assign quadrants to the identified Domains and its controls
 - Quadrant 1 will consist of identified Domains and Controls that have high impact on business continuity but low Risk Priority Score (RP)
 - Quadrant 2 will consist of identified Domains and Controls that have high impact on business continuity and high Risk Priority Score (RP)
 - Quadrant 3 will consist of identified Domains and Controls that have low impact on business continuity and low Risk Priority Score (RP)
 - Quadrant 4 will consist of identified Domains and Controls that have low impact on business continuity but high Risk Priority Score (RP)
 2. Compare Domains and Controls pairs amongst each other and identify the priority of execution



2 Risk Priority & Business Continuity Impact

Reformulating Worksheet - Template



Michael E. Whitman, & Herbert J. Mattord (2019). Management of information security. Cengage Learning.

3 Strategic Planning for Domains

Reformulating Worksheet - Example

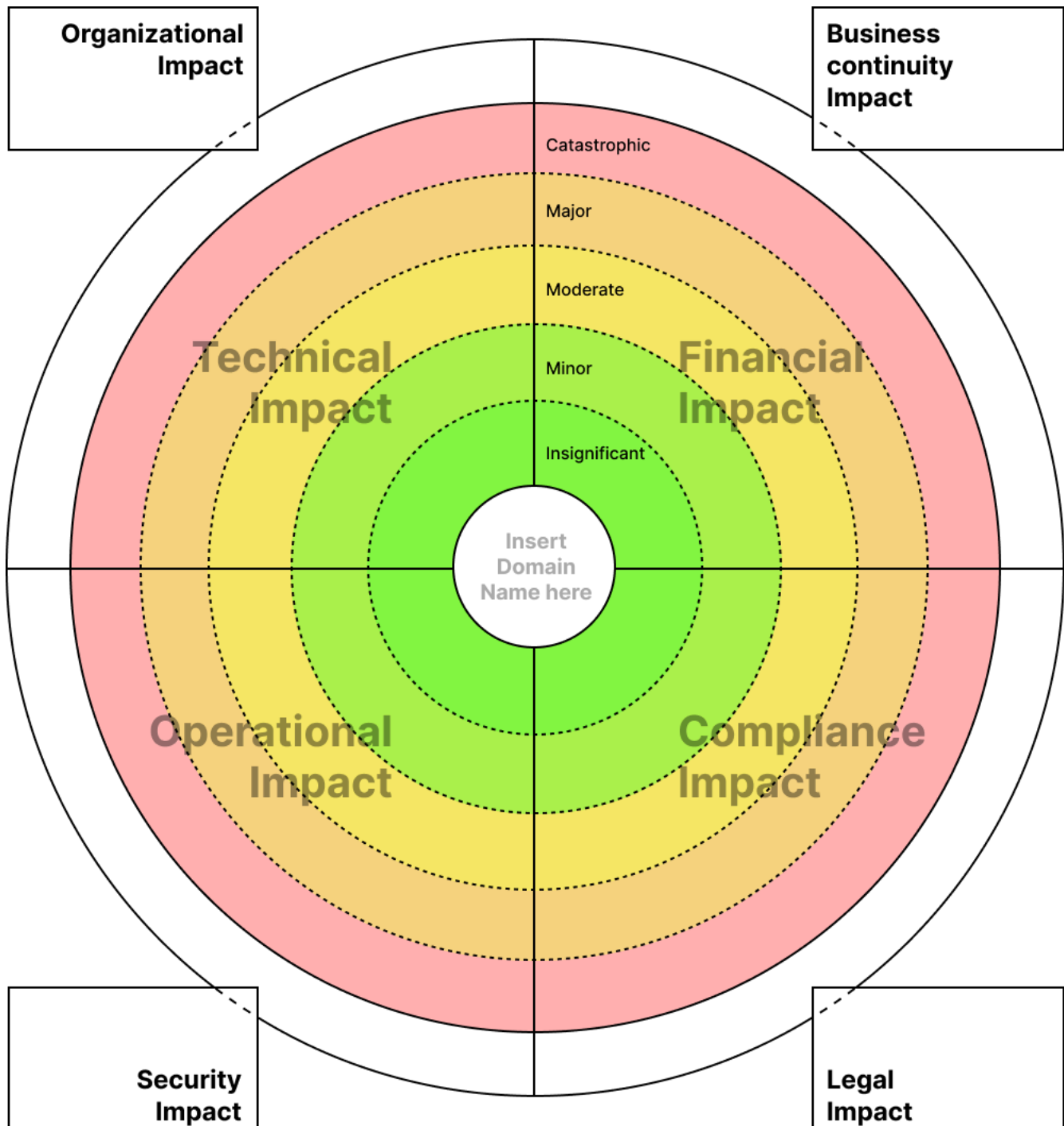
This Worksheet helps in understanding the Domains on a deeper level by identifying various levels of impact that it has in an organization

1. Based on the results from Reformulating Worksheet 2, write your prioritized Domain in the central circle
 - Ideally this exercise should be done for all Domains that need improvement (identified from the Worksheet 1)
2. Using post-it notes, mark the level of impacts (Technical, Financial, Operational, Compliance) and its associated reasons that the particular domain could cause
3. Use post-it notes for the outer circle to write the associated impacts (Organizational, Business continuity, Security, Legal) that the Domain has on the organization



3 Strategic Planning for Domains

Reformulating Worksheet - Template



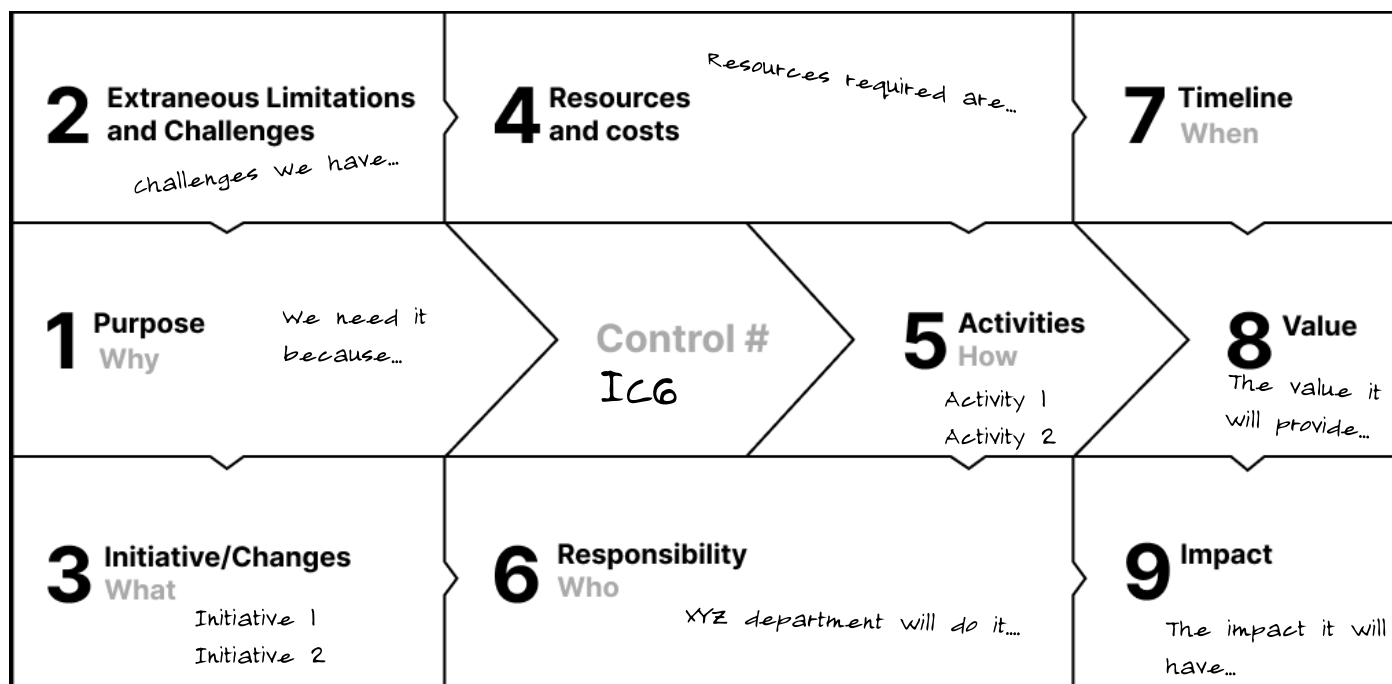
Michael E. Whitman, & Herbert J. Mattord (2019). Management of information security. Cengage Learning.

4 Strategic Planning for Controls

Reformulating Worksheet - Example

This Worksheet helps in understanding the Controls on a deeper level by breaking it down into different components. This diagram is a variant of the SIPOC Diagram/ Turtle Diagram.

- Based on the results from Reformulating Worksheet 2, Write the prioritized Control in the given space
 - Ideally this exercise should be done for all Controls that need improvement (identified from the Worksheet 1)
- Start filling the other sections in a sequential manner
 - Purpose:** Outlines the rationale behind the control. this section explains why it is necessary, including the goals, objectives, or problems it aims to address
 - Extraneous Limitations and Challenges:** External or unforeseen factors that hinder the effective implementation, operation, or assessment of a cybersecurity control within an organization.
 - Initiative/ Changes:** Specifies the main idea or plan being proposed. This aspect summarizes the key approach or project intended to meet the outlined purpose
 - Resources and Costs:** Identifies the tangible and intangible resources technical, human, and otherwise needed to implement the control, along with the associated expenses and budget considerations.
 - Activities:** Breaks down the practical steps and processes for carrying out the initiative. This section details the methods, tasks, and procedures that will be employed to fulfill the plan
 - Responsibility:** Identifies the individual(s) or role(s) in charge of carrying out or overseeing the control. This section clarifies who is in-charge of the action steps and is ultimately accountable for achieving the desired outcomes
 - Timeline:** The structured sequence of events, milestones, or deadlines associated with the implementation, evaluation, and improvement of a cybersecurity control.
 - Value:** The significance or benefit a cybersecurity control brings to the organization in terms of security enhancement, risk reduction, or operational efficiency.
 - Impact:** The measurable effect positive or negative that a cybersecurity control, security event, or threat has on the organization's operations, assets, or compliance posture.



4 Strategic Planning for Controls

Reformulating Worksheet - Template

2 Extraneous Limitations and Challenges	4 Resources and costs	7 Timeline When
1 Purpose Why	5 Activities How	8 Value
3 Initiative/Changes What	6 Responsibility Who	9 Impact

Peter Jones, & Kristel Van Ael (2022). *Design journeys through complex systems: Practice tools for systemic design*. Amsterdam: Bis Publishers, 2022.

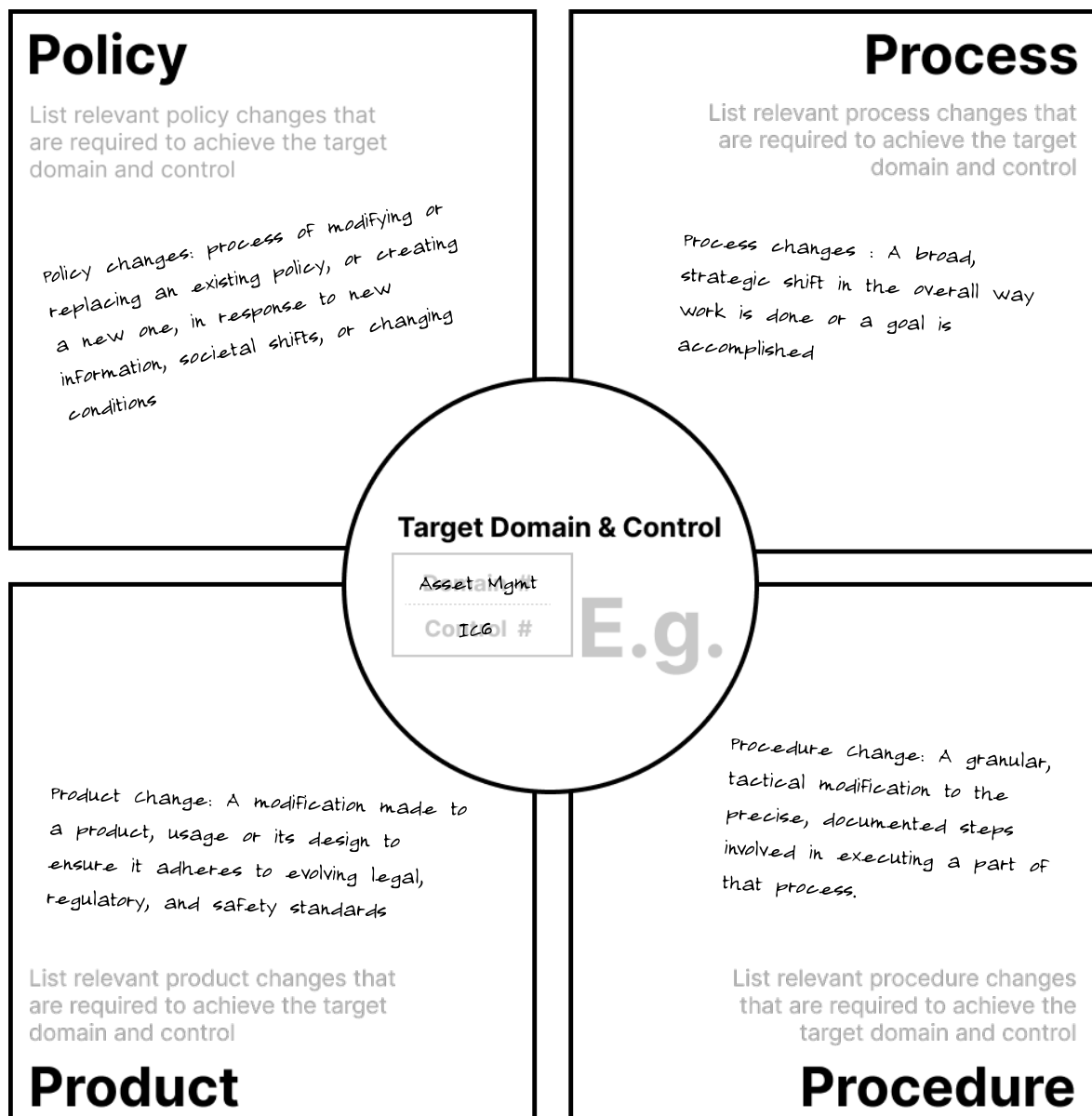
Philip B. Crosby (1979). *Quality is free: The art of making quality certain*. New York: New American Library, 17, 174-83.

5 Resource Mapping: Current Scenario

Reformulating Worksheet - Example

This Worksheet helps in understanding the resources that would be required to successfully execute the target Domain and Control in the current scenario

1. Write the selected Domain and Control in the central circle
2. Write the associated resources required for each sections
 - Policy: List relevant policy changes that are required to achieve the target domain and control
 - Process: List relevant process changes that are required to achieve the target domain and control
 - Procedure: List relevant procedure changes that are required to achieve the target domain and control
 - Product: List relevant product changes that are required to achieve the target domain and control
3. Once completed, the information from this sheet can also be used for enhancing the information in the Resources and Costs section in the Reformulating Worksheet 4



5 Resource Mapping: Current Scenario

Reformulating Worksheet - Template

Policy List relevant policy changes that are required to achieve the target domain and control	Process List relevant process changes that are required to achieve the target domain and control
Product List relevant product changes that are required to achieve the target domain and control	Procedure List relevant procedure changes that are required to achieve the target domain and control

Target Domain & Control

Domain #
Control #

E.g.

6 Resource Mapping: Alternative Scenarios

Reformulating Worksheet - Example

This Worksheet helps in building the alternative scenarios based on the existing scenario and hence provides support to contrafactual thinking while creating cybersecurity plans to handle normal and extreme events of the future

1. Fill the center square with existing scenario from Reformulating worksheet 5
 - Detail out the existing scenario
2. Use contrafactual thinking to develop 4 alternative scenarios to be reached in the future: Preferred; Probable; Plausible; Possible
 - Preferred: preferred futures are those futures that are *desirable* in nature and are what the people involved want a future to be. These preferred futures are highly contested since questions regarding agency and benefits are raised, i.e. preferable according to who and for whom.
 - Probable: probable futures are those futures that would, in all likelihood, manifest unless there are major upheavals in society. These are futures that are *most likely* to happen.
 - Plausible: plausible futures are those futures that are credible or appear acceptable. These provide the realm of those futures that *could* happen.
 - Possible : possible futures are those futures that could be made manifest if there were deviations from existing trends due to the emergence of new unanticipated trends or upheavals. These are futures that *might* happen.

1 Preferred future scenario • Detail out the scenario • List the resources you would require to execute this scenario • List the possible pathways you would take to reach this preferred future scenario	Probable future scenario 2 Please detail out the scenario . Please list the resources you would require to execute this scenario Please list the possible pathways you would take to reach this probable future scenario	
Detailed scenario Required resources Possible pathways <i>Desirable</i>	Existing Scenario (Domain and associated Controls) Asset Mgmt Controls # E.g. Existing scenario Existing Resources Current challenges	Detailed scenario Required resources Possible pathways <i>Likely</i>
Detailed scenario Required resources Possible pathways • Please detail out the scenario • Please list the resources you would require to execute this scenario • Please list the possible pathways you would take to reach this plausible future scenario 3 Plausible future scenario	Detailed scenario Required resources Possible pathways <i>Might</i> Please detail out the scenario . Please list the resources you would require to execute this scenario Please list the possible pathways you would take to reach this possible future scenario Possible future scenario 4	Detailed scenario Required resources Possible pathways

6 Resource Mapping: Alternative Scenarios

Reformulating Worksheet - Template

1 Preferred future scenario • Detail out the scenario • List the resources you would require to execute this scenario • List the possible pathways you would take to reach this preferred future scenario	Probable future scenario 2 Please detail out the scenario Please list the resources you would require to execute this scenario Please list the possible pathways you would take to reach this probable future scenario			
<i>Desirable</i> <i>Could</i> • Please detail out the scenario • Please list the resources you would require to execute this scenario • Please list the possible pathways you would take to reach this plausible future scenario 3 Plausible future scenario	Existing Scenario (Domain and associated Controls) <table border="1"> <tr> <td>Domain #</td> <td rowspan="2">E.g.</td> </tr> <tr> <td>Controls #</td> </tr> </table> • Detail out the existing scenario • List the existing resources • List the shortcomings in terms of the resources <i>Likely</i> <i>Might</i> Please detail out the scenario Please list the resources you would require to execute this scenario Please list the possible pathways you would take to reach this possible future scenario Possible future scenario 4	Domain #	E.g.	Controls #
Domain #	E.g.			
Controls #				

Hannah Kosow, and Robert Gaßner. 2008. *Methods of Future and Scenario Analysis: Overview, Assessment, and Selection Criteria* (vol. 39). Bonn: German Development Institute.

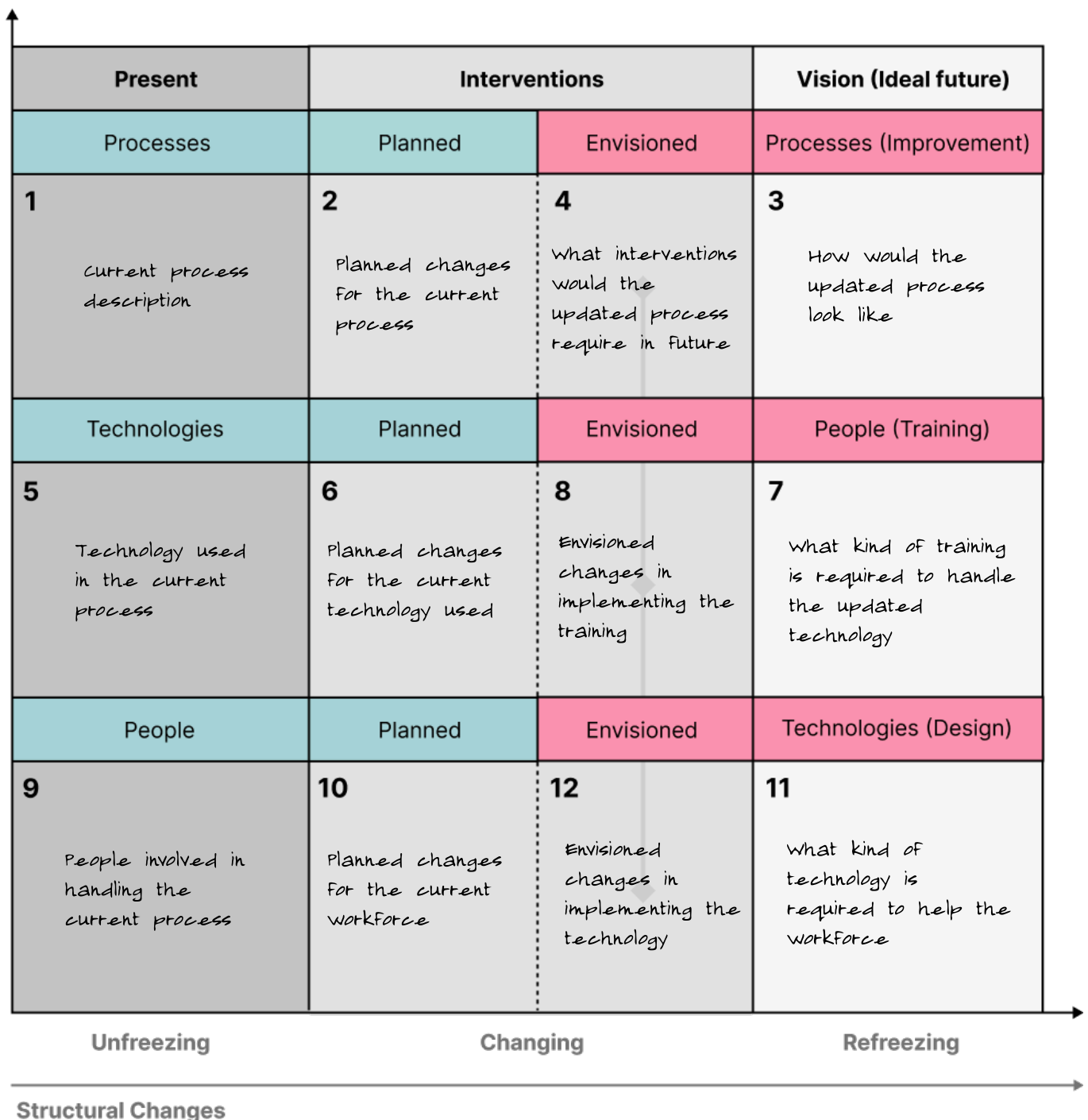
Mats Lindgren, and Hans Bandhold. 2009. *Scenario Planning: The Link Between Future and Strategy*. UK: Palgrave-Macmillan.

7 Mapping for Human Systems Integration

Reformulating Worksheet - Example

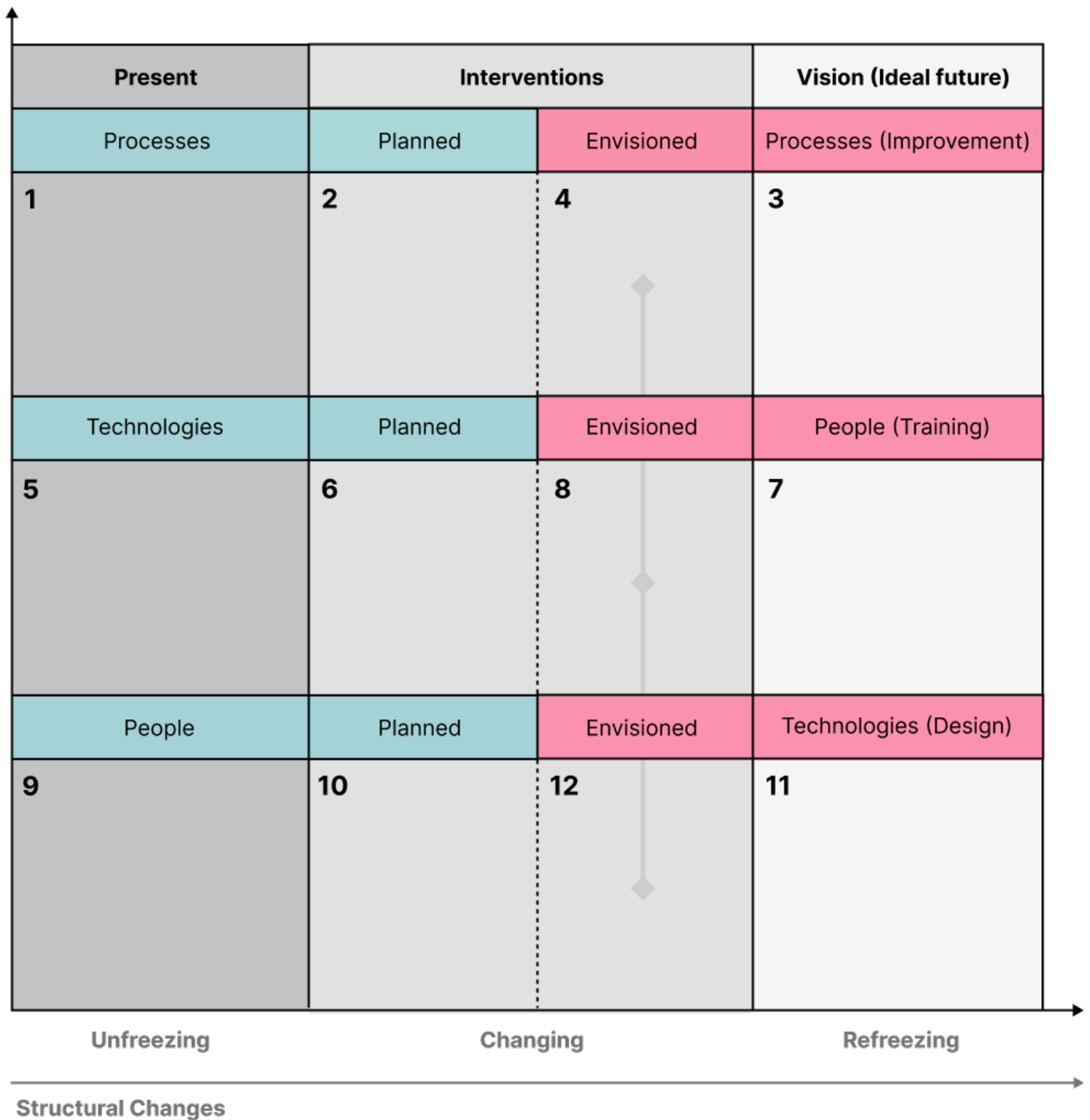
This worksheet will help in mapping the transition between the present posture to an Ideal posture and the required efforts

1. Using post-it notes to fill-in the 12 sections in the requisite numbered order to aid in the transition.
2. First the process improvements need to be charted that will aid in the transition of the future ideal states.
3. Second, the current technological capability is charted along with the required future people capability, followed by the required interventions (5-7)
4. Third, the current people capability are charted along with the required technological capability in the future, followed by the required interventions.



7 Mapping for Human Systems Integration

Reformulating Worksheet - Template



Leavitt H J. (1965). Applied organizational change in industry: structural, technical and humanistic approaches, in March, J. G. (ed.), Handbook of Organizations. 1144-1170.II
 Bill Sharpe (2020). *Three horizons: Patterning of Hope*. UK:Triarchy Press.

8 Resource Planning for Inclusive Change

Reformulating Worksheet - Example

This Worksheet helps in resource planning for cybersecurity by collating various requirements from various stakeholders together

- Rows highlight the breadth in terms of perspectives and associated entities
 - Ideally the CISO and the related teams at each level of the organizational hierarchy should identify stakeholders who can contribute towards (Vertical Dimension):
 - Executive Perspective:** Enabling the identification of Scope
 - Business Perspective:** Clarifying Business Logic
 - System Design Perspective:** Representing System Logic
 - Developer/ OT Engineer Perspective:** Specifying Technology
 - Worker/ Operator Perspective:** Execute through Tools and Components
- Columns indicate the context and the respective physical and temporal entities
 - What:** Entities and Assets based on perspective
 - How:** Process and Operations based on perspective
 - Where:** Entities in Contexts based on perspective
 - Who:** Responsibility Assignments based on perspective
 - When:** Timing/Periodic cycles based on perspective
 - Why:** Motivation and Intention based on perspective
- The matrix is a representation of all the perspectives across the organization and will help towards resource planning for enabling inclusive change management for an enhanced cybersecurity posture.

	What	How	Where	Who	When	Why	
Executive Perspective	Identification of Entities	Identification of Process	Identification of Entities in Contexts	Identification of Responsibility	Identification of Timing/ Periodicity	Identification of Motivation	Scope
Business Perspective	Definition of Entities	Definition of Process	Definition of Entities in Contexts	Definition of Responsibility	Definition of Timing/ Periodicity	Definition of Motivation	Business Logic
System Design Perspective	Representation of Entities	Representation of Process	Representation of Entities in Contexts	Representation of Responsibility	Representation of Timing/ Periodicity	Representation of Motivation	System Logic
Developer/ OT Engineer Perspective	Specification of Assets	Specification of Process	Specification of Entities in Contexts	Specification of Responsibility	Specification of Timing/ Periodicity	Specification of Intention	Technology
Worker/ Operator Perspective	Execution on Assets	Execution of Process	Execution in Contexts	Execution of Responsibility	Execution of Timing/ Periodicity	Execution of Intention	Tools and Components
	Entities and Assets	Process and Operations	Entities in Contexts	Responsibility Assignments	Timing/ Periodic cycles	Motivation and Intentions	

8 Resource Planning for Inclusive Change

Reformulating Worksheet - Template

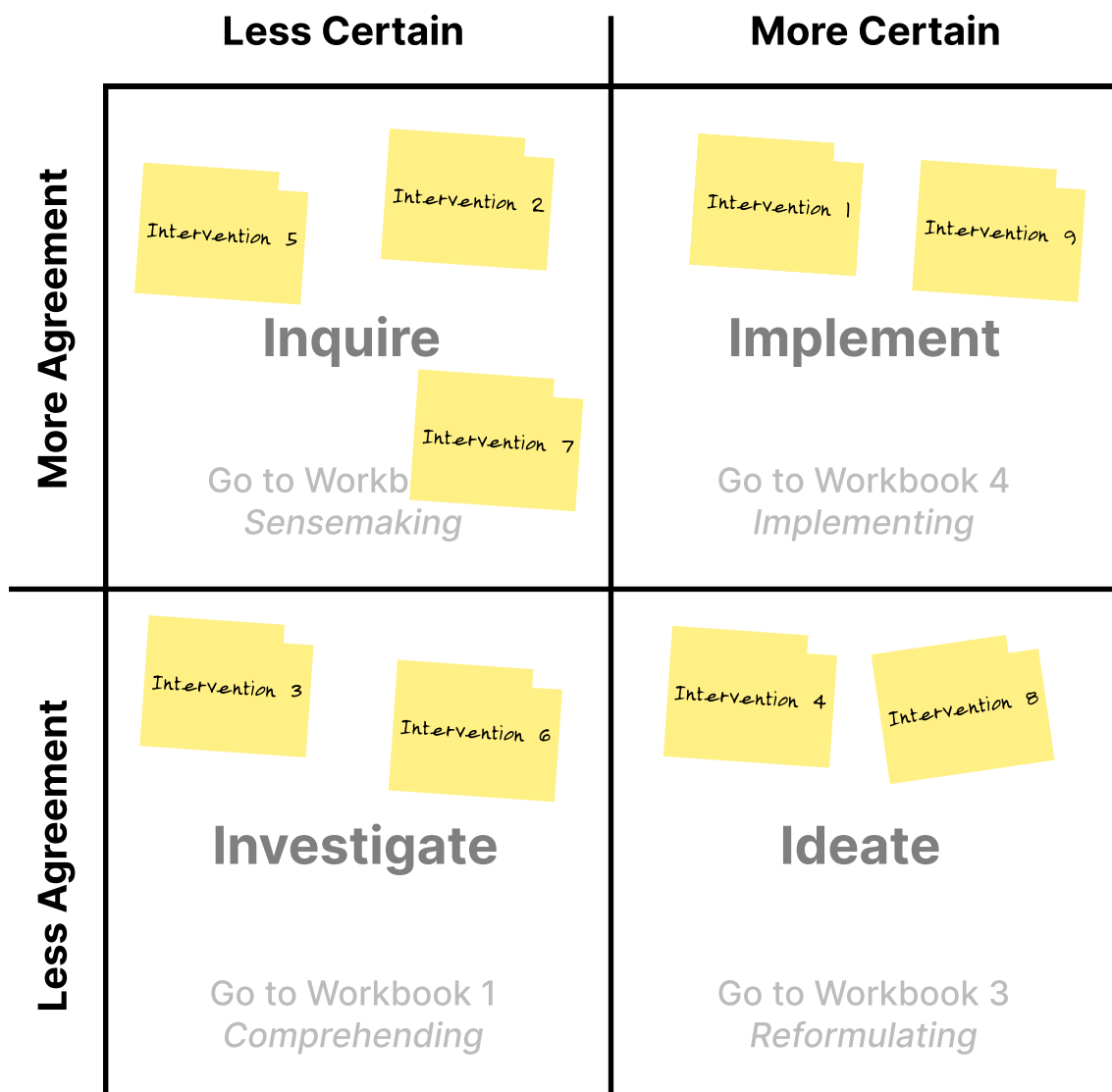
	What	How	Where	Who	When	Why	
Executive Perspective	Identification of Entities	Identification of Process	Identification of Entities in Contexts	Identification of Responsibility	Identification of Timing/Periodicity	Identification of Motivation	Scope
Business Perspective	Definition of Entities	Definition of Process	Definition of Entities in Contexts	Definition of Responsibility	Definition of Timing/Periodicity	Definition of Motivation	Business Logic
System Design Perspective	Representation of Entities	Representation of Process	Representation of Entities in Contexts	Representation of Responsibility	Representation of Timing/Periodicity	Representation of Motivation	System Logic
Developer/OT Engineer Perspective	Specification of Assets	Specification of Process	Specification of Entities in Contexts	Specification of Responsibility	Specification of Timing/Periodicity	Specification of Intention	Technology
Worker/Operator Perspective	Execution on Assets	Execution of Process	Execution in Contexts	Execution of Responsibility	Execution of Timing/Periodicity	Execution of Intention	Tools and Components
	Entities and Assets	Process and Operations	Entities in Contexts	Responsibility Assignments	Timing/Periodic cycles	Motivation and Intentions	

9 Consensus Formation

Reformulating Worksheet - Example

This Worksheet helps in forming of consensus and further action for various stakeholders collectively

1. Horizontal axis highlights the range of certainty of the proposed interventions
2. Vertical axis indicate the stakeholder wide agreement for the implementation of the proposed intervention
3. There are 4 quadrants for this tool
 - a. Quadrant 1 will consist of interventions that have high agreement and high certainty, it is advised that the organization follows the implementing worksheets
 - b. Quadrant 2 will consist of interventions that have high agreement but low certainty, it is advised that the organization follows the sensemaking worksheets again
 - c. Quadrant 3 will consist of interventions that have low agreement and low certainty, it is advised that the organization follows the comprehending worksheets
 - d. Quadrant 4 will consist of interventions that have low agreement but high certainty, it is advised that the organization follows the reformulating worksheets
4. The matrix is a representation of the various interventions formulated until now and will help towards a collective consensus. This will enable inclusive change management for an enhanced cybersecurity posture.



9

Consensus Formation

Reformulating Worksheet - Template

		Less Certain	More Certain
More Agreement		Inquire Go to Workbook 2 <i>Sensemaking</i>	Implement Go to Workbook 4 <i>Implementing</i>
Less Agreement		Investigate Go to Workbook 1 <i>Comprehending</i>	Ideate Go to Workbook 3 <i>Reformulating</i>



Implementing

4



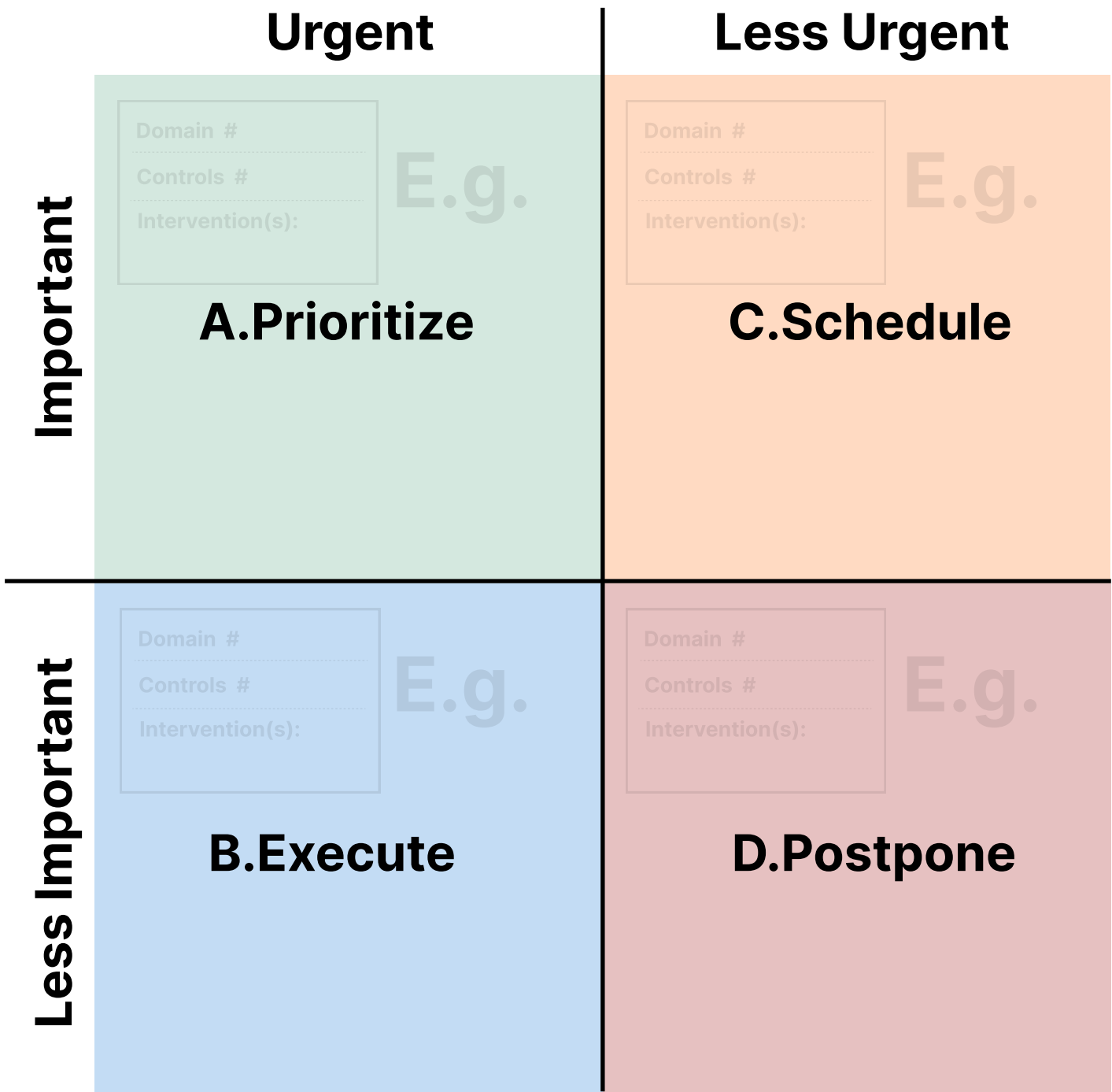
Action Priority Matrix

Implementation Worksheet

This Worksheet helps in categorizing the Interventions in Implement quadrant of reformulation worksheet 9 (Consensus Formulation), based on Importance and Urgency

1. From the Reformulation worksheet 9, categorize the identified Interventions for Domain and Control implementation under each Quadrant

- Prioritize: Interventions that are Important and needs Urgent implementation
- Execute: Interventions that are Less Important but needs Urgent implementation
- Schedule: Interventions that are Important but are Less Urgent
- Postpone: Interventions that are Less Important and are Less Urgent



A Implementation - Prioritze

Implementation Worksheet

This Worksheet helps in keeping track of the implementation of the Controls

1. Refer to A. Prioritize Quadrant of the Implementation Worksheet 0 and fill the table below

- Fill the table with all the Domains and associated Controls identified in the Prioritize Quadrant
- Fill the Domain and Control numbers, assign responsibility, timeline and a completion date, respectively

2. Keep track of the implementation status. Mark the status checkbox once the domain and control is fully implemented

Domain #	Control #	Responsibility	Timeline	Completion Date	Status
E.g. Domain 5	PC2	E.g. Vivek Kant	E.g. 1 week	DD/MM/YY	☒
	IC4	E.g. Soham M	E.g. 1 week	DD/MM/YY	☐
	OC3	E.g. Thomas Raju	E.g. 1 week	DD/MM/YY	☐
					☐

B Implementation - Execute

Implementation Worksheet

- This Worksheet helps in keeping track of the implementation of the Controls
1. Refer to B. Execute Quadrant of the Implementation Worksheet 0 and fill the table below
 - Fill the table with all the Domains and associated Controls identified in the Prioritize Quadrant
 - Fill the Domain and Control numbers, assign responsibility, timeline and a completion date, respectively
 2. Keep track of the implementation status. Mark the status checkbox once the domain and control is fully implemented

Domain #	Control #	Responsibility	Timeline	Completion Date	Status
E.g. Domain 5	PC2	E.g. Vivek Kant	E.g. 1 week	DD/MM/YY	☒
	IC4	E.g. Soham M	E.g. 1 week	DD/MM/YY	☐
	OC3	E.g. Thomas Raju	E.g. 1 week	DD/MM/YY	☐
					☐

C

Implementation - Schedule

Implementation Worksheet

- This Worksheet helps in keeping track of the implementation of the Controls
1. Refer to C. Schedule Quadrant of the Implementation Worksheet 0 and fill the table below
 - Fill the table with all the Domains and associated Controls identified in the Prioritize Quadrant
 - Fill the Domain and Control numbers, assign responsibility, timeline and a completion date, respectively
 2. Keep track of the implementation status. Mark the status checkbox once the domain and control is fully implemented

Domain #	Control #	Responsibility	Timeline	Completion Date	Status
E.g. Domain 5	PC2	E.g. Vivek Kant	E.g. 1 week	DD/MM/YY	☒
	IC4	E.g. Soham M	E.g. 1 week	DD/MM/YY	☐
	OC3	E.g. Thomas Raju	E.g. 1 week	DD/MM/YY	☐
					☐

D Implementation - Postpone

Implementation Worksheet

- This Worksheet helps in keeping track of the implementation of the Controls
1. Refer to D. Postpone Quadrant of the Implementation Worksheet 0 and fill the table below
 - Fill the table with all the Domains and associated Controls identified in the Prioritize Quadrant
 - Fill the Domain and Control numbers, assign responsibility, timeline and a completion date, respectively
 2. Keep track of the implementation status. Mark the status checkbox once the domain and control is fully implemented

Domain #	Control #	Responsibility	Timeline	Completion Date	Status
E.g. Domain 5	PC2	E.g. Vivek Kant	E.g. 1 week	DD/MM/YY	☒
	IC4	E.g. Soham M	E.g. 1 week	DD/MM/YY	☐
	OC3	E.g. Thomas Raju	E.g. 1 week	DD/MM/YY	☐
					☐

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 fourth 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 978-93-6128-253-9



9 789361 282539