# Workbook for NCIIPC based Transformation of Indian Organizations

Enhancing the Cybersecurity Posture for Critical Information Infrastructures

## How to Use The Worksheets

1. Gather a cross-functional team (e.g., IT, legal, compliance, and engineering).
2. The CISO should facilitate the session and ensure all security perspectives are captured
3. Print this worksheet in a large format (A1 to A3) so everyone has room to contribute
4. Hang the worksheet on a wall or lay it flat on a large table
5. Discuss the ideas as a team, use sticky notes, markers and map out your next action steps

## Hands-on Worksheets

Vivek Kant, Soham Mohanty

HFSS 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.

This workbook is an output of a project funded by IHUB-NTIHAC Foundation

© 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

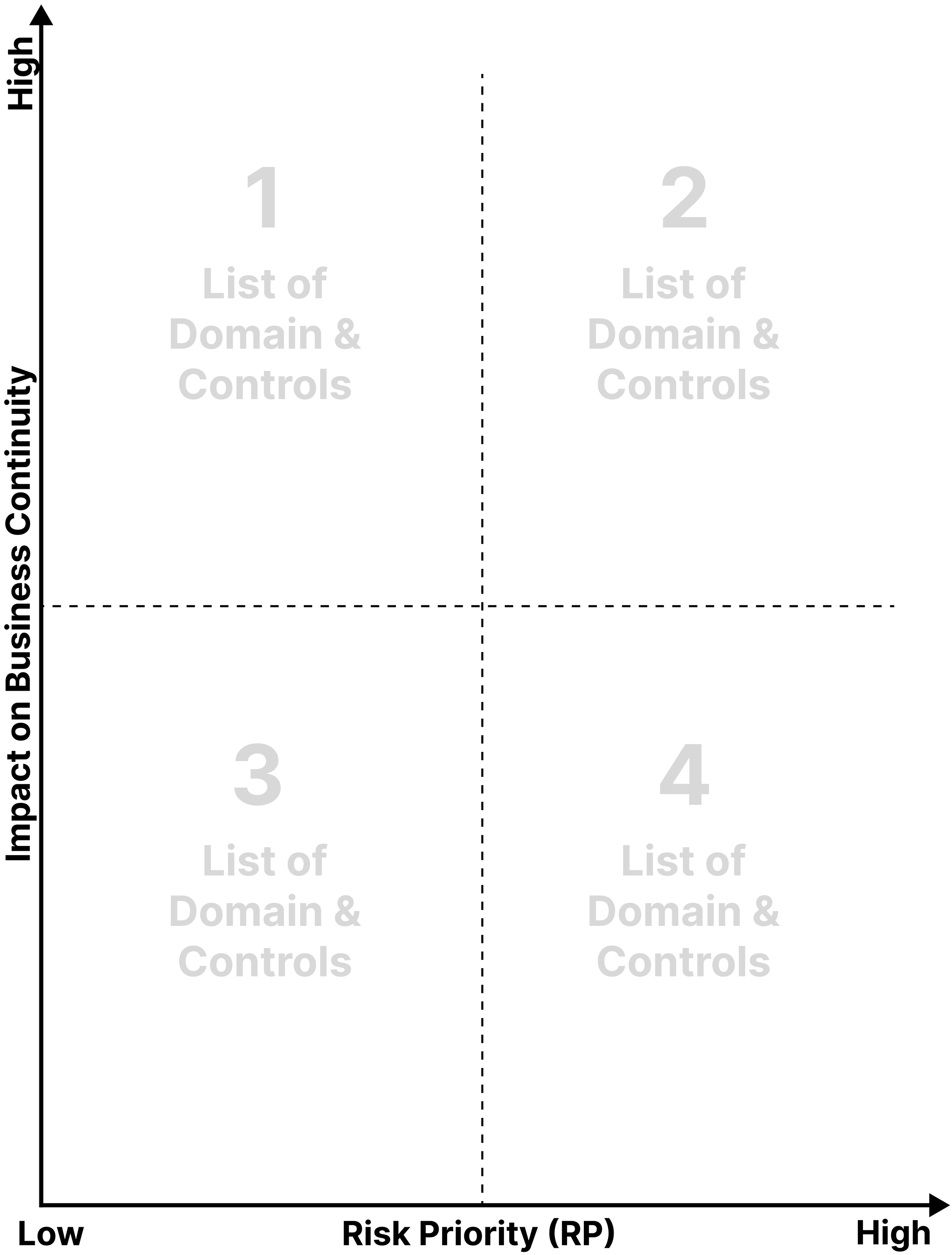
| | Planning Control | Implementation Control | Operational Control | Disaster Recovery/ Business | Reporting and Accountability |
|---|---|---|---|---|---|
| 1. Governance | | | | | |
| 2. Risk Management | | | | | |
| 3. Asset Management | | | | | |
| 4. Identity & Access Mgmt | | | | | |
| 5. Secure 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 | | | | | |

# 1 Domain & Control Comparison Matrix

Refer workbook 3, Pg. 12

Participants:

Date:



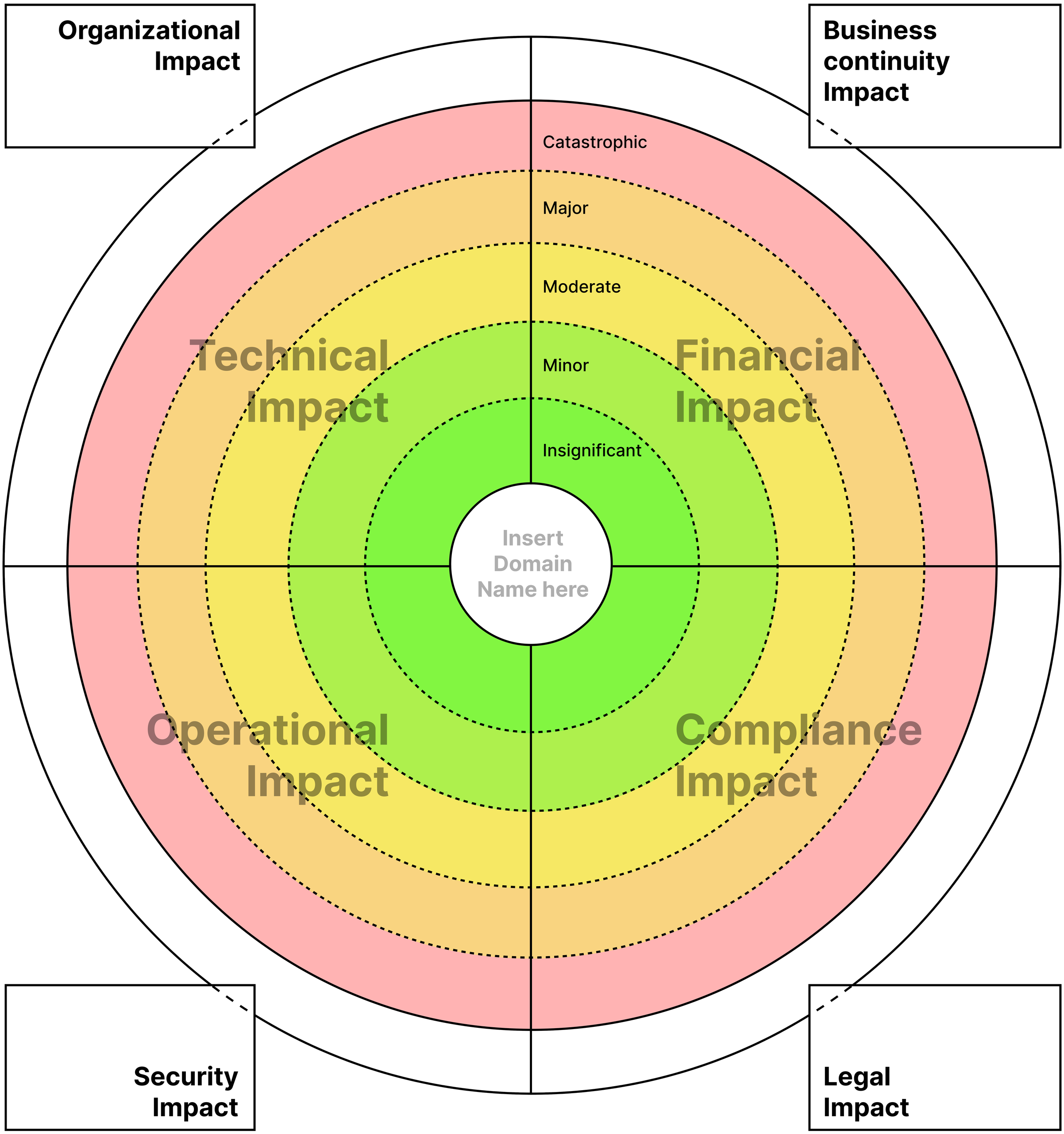

Michael E. Whitman, & Herbert J. Mattord (2019). Management of information security. Cengage Learning.

## 2 Risk Priority & Business Continuity Impact

Refer workbook 3, Pg. 14

Participants:

Date:

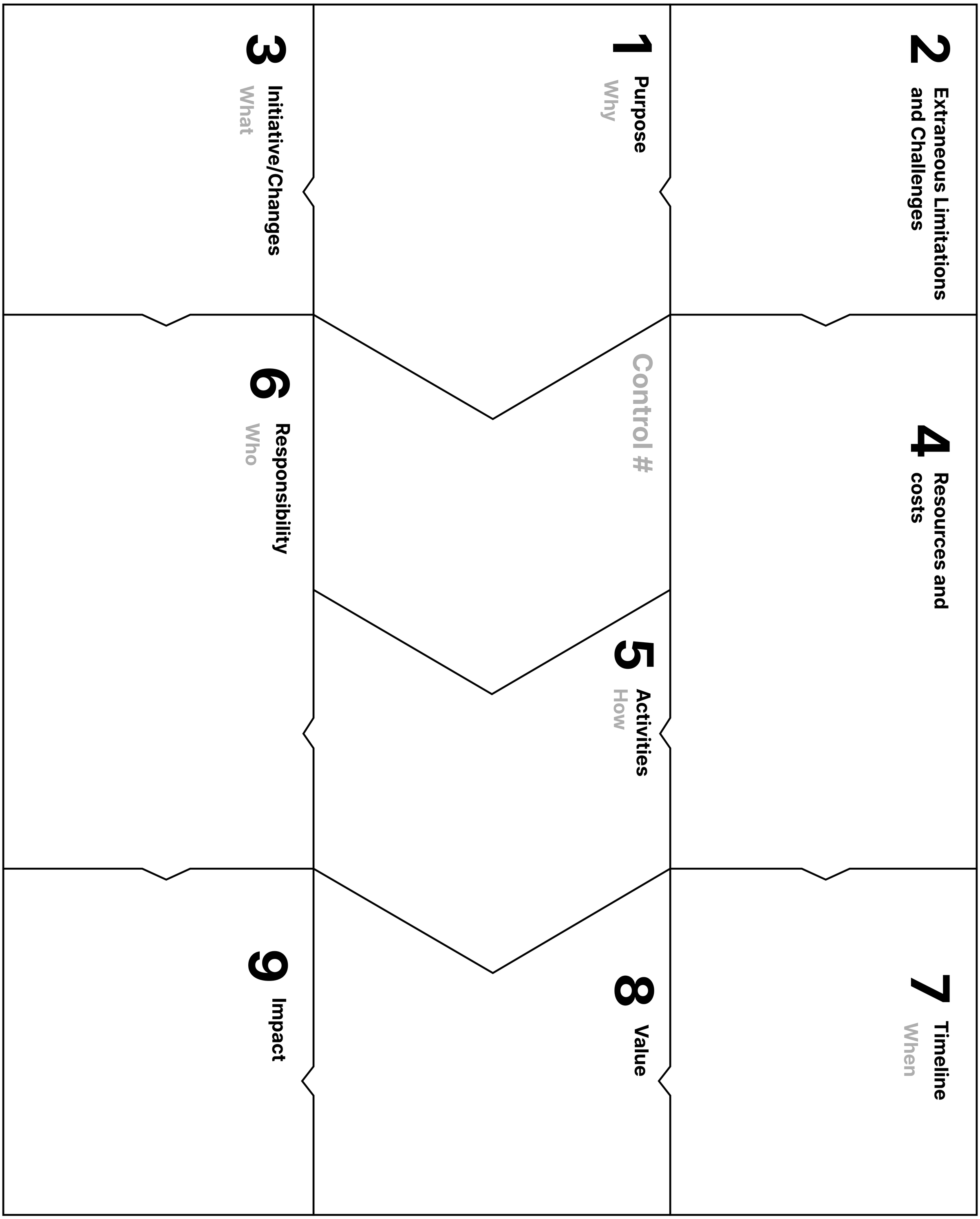



Michael E. Whitman, & Herbert J. Mattord (2019). Management of information security. Cengage Learning.



Participants:

Date:




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.



Participants:

Date:

## 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

**Target Domain & Control**

Domain #

Control #

E.g.

List relevant product changes that are required to achieve the target domain and control

## Product

List relevant procedure changes that are required to achieve the target domain and control

## Procedure

# 5 Resource Mapping: Current Scenario

Refer workbook 3, Pg. 20

Participants:

Date:

## 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

### Existing Scenario (Domain and associated Controls)

Domain #
Controls #

E.g.

- Detail out the existing scenario
- List the existing resources
- List the shortcomings in terms of the resources

*Desirable*

*Likely*

*Could*

*Might*

- 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

- 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


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.


## 6 Resource Mapping: Alternative Scenarios

Refer workbook 3, Pg. 22

Participants:

Date:

| Present | Interventions | | Vision (Ideal future) |
|---|---|---|---|
| Processes | Planned | Envisioned | Processes (Improvement) |
| 1 | 2 | 4 | 3 |
| Technologies | Planned | Envisioned | People (Training) |
| 5 | 6 | 8 | 7 |
| People | Planned | Envisioned | Technologies (Design) |
| 9 | 10 | 12 | 11 |

**Unfreezing** **Changing** **Refreezing**

## Structural Changes


Leavitt H J. (1965). Applied organizational change in industry: structural, technical and humanistic approaches, in March, J. G. (ed.), Handbook of Organizations. 1144-1170.ll

Bill Sharpe (2020).*Three horizons: Patterning of Hope*. UK:Triarchy Press.


# 7 Mapping for Human Systems Integration

Refer workbook 3, Pg. 24

Participants:

Date:

**Resource Planning for Inclusive Change**

Refer workbook 3, Pg. 26

Participants:

Date:

| | 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 | |

John A. Zachman, (2011). *Zachman Framework Version 3.0*. https://zachman-feac.com/the-zachman-framework-evolution(Accessed:16/3/25)

| | Less Certain | More Certain |
|---|---|---|
| More Agreement | **Inquire**<br>Go to Workbook 2<br>*Sensemaking* | **Implement**<br>Go to Workbook 4<br>*Implementing* |
| Less Agreement | **Investigate**<br>Go to Workbook 1<br>*Comprehending* | **Ideate**<br>Go to Workbook 3<br>*Reformulating* |

Stacey, R.D. (1993). *Strategic management and organizational dynamics: The challenge of complexity*. Pitman



Participants:

Date:

# 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

HFSS Studios

ISBN 978-93-6128-253-9
9 789361 282539