

NCIIPC Based Toolkit

Enabling Organizations to improve cybersecurity posture through self assessment

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.

Comprehending Workbook

Digital Toolkit

The digital toolkit is an excel based file that automates the functions of workbook 1 and 2. This toolkit enables quick scoring and recommendation checklists based on the self assessed score. This digital toolkit serves as the first step towards improving the cybersecurity posture of organizations through self assessment

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.

Sensemaking Workbook

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.

Reformulating Workbook

4 Implementing
In the fourth phase, the detailed course of action gets implemented. 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.

Implementing Workbook

Scan here to access the Free Toolkit



Change Management Process

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

