SmartSuite

Framework / Cybersecurity / Other

Cyber Defense Methodology for an Organization, version 1.0

Israel's Cyber Defense Methodology for an Organization (CDMO) from the INCD: v1.0 (June 2017) sorts organizations into Category A or B; v2.0 (2021) builds on NIST CSF 1.1.



What it is

Israel CDMO is the Cyber Defense Methodology for an Organization, a recommendation for all organizations in Israel issued by the Israel National Cyber Directorate (INCD), which grew out of the Cyber Bureau created in the Prime Minister's Office in 2012. Version 1.0, dated June 2017, sorts organizations into two categories and groups its controls under the five functions of the NIST Cybersecurity Framework. Version 2.0, published in 2021, adopts NIST Cybersecurity Framework 1.1 and NIST SP 800-53 Rev. 5 and is the latest version found; this page describes version 1.0 in detail and records what NIST has published about version 2.0.

Version 1.0 turns on one question: if a cyber incident occurred, would handling it cost more than NIS 500,000? An organization that answers no is Category A and works through ten categories of protection. One that answers yes is Category B, maps its assets, rates each from 1 to 4 and applies the controls up to that level. The document says it presents minimum protection requirements in line with the potential for damage and that organizations are required to perform a risk assessment.

At a glance

PUBLISHER Israel National Cyber Directorate (INCD)	TYPE Framework	VERSION Version 1.0 (June 2017); version 2.0 published 2021
EFFECTIVE June 2017	DOMAIN Cybersecurity	FAMILY Other
REGION Israel	ADOPTION MODEL Voluntary	IMPLEMENTATION COMPLEXITY High

Source: gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf

Why it matters

- **Defense scaled to damage** Controls carry levels from 1 to 4, and an asset needs every control at or below its own value level (clause 5.2, stage 3).
- **A lighter path for Category A** Smaller-exposure organizations follow ten categories of protection (Appendix C) instead of the full control chapters.
- **A common language with NIST** Controls sit under Identify, Protect, Detect, Respond and Recover, so they line up with the NIST Cybersecurity Framework (clause 3.2).
- **Mapped to NIST and ISO** Appendix D says INCD mapped the controls to equivalent controls in NIST SP 800-53 and ISO 27001.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Israel CDMO

Asset Inventory

Keep the asset inventory that the mapping stage starts from in IT Asset Management (ITAM), with owner and lifecycle.

Asset Value and Risk Register

Record each asset's value level, exposure and resulting risk in Cyber & IT Risk, with the controls it requires.

Control Library by Level

Hold the controls in Compliance Management with their level from 1 to 4, owner, status, testing and evidence.

Gap-Based Work Plan

Turn the gap list into remediation actions in Cyber & IT Risk, ranked by risk, cost and speed of implementation.

Supplier Requirements

Assess and monitor suppliers in Third Party Risk Management against the requirements the organization sets for them.

Review and Board Reporting

Plan control reviews in Internal Audit Management, track remediation and report risk and gaps to management.

Common framework mappings

CIS Controls v8.1 · COBIT 2019 · ISO 27001:2022 · ISO 27002:2022 · MITRE ATT&CK · NIST CSF 2.0 · NIST 800-53 Rev.5 · SOC 2

Official resources

Israel CDMO v1.0 Framework

Provides the official methodology for organizations to implement comprehensive cyber defense strategies.

gov.il/en/departments/israel_national_cyber_directorate

Israel National Cyber Directorate Homepage

Outlines responsibilities and initiatives of Israel's main cybersecurity authority.

gov.il/en/departments/about/national_cyber_directorate

Cyber Defense Methodology Guidelines

Details guidelines for applying the Israel CDMO framework in organizational contexts.

gov.il/en/departments/general/cyber-defense-methodology-guidelines

Frequently asked questions

What is the Cyber Defense Methodology for an Organization (CDMO)?

It is the Israel National Cyber Directorate's methodology for organizations in Israel, a recommendation that boards, managements and cyber defense managers can use freely. Version 1.0 is dated June 2017 and organizes controls under the five functions of the NIST Cybersecurity Framework; version 2.0 followed in 2021. The aim stated in its Executive Summary is to minimize cyber risks for organizations in Israel.

How do Category A and Category B differ in version 1.0?

Clause 5 asks whether handling a cyber incident would cost more than NIS 500,000. If not, the organization is Category A and follows ten categories of protection from Appendix C. If so, it is Category B and maps its assets, rates each from 1 to 4 and implements all controls whose level is at or below the asset's score (clause 5.2). Existing regulation can move an organization from A to B.

How does version 1.0 calculate an asset's risk level?

Impact is the highest of three damage scores for confidentiality, integrity and availability, on a scale from 1 to 4. Probability is the average of ten exposure questions covering users, interfaces, remote access, update level and physical security. The risk level is impact multiplied by three plus probability (clause 5.2), and the work plan is ranked by risk level, cost and speed of implementation.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What changed in version 2.0?

NIST records that INCD published version 2.0 in 2021 and that it adopts NIST Cybersecurity Framework 1.1, NIST SP 800-53 Rev. 5 and further NIST standards, plus threat-informed defense and zero-trust. Each control is layered with its requirement, an organizational maturity model, explanations and examples, links to best practices, templates and compatibility with standards. Version 1.0 was built on NIST Cybersecurity Framework 1.0.

Is the methodology mandatory?

The document describes itself as a recommendation for all organizations in Israel. NIST records that the whole Israeli government adopted version 2.0 in 2021 as the required cyber risk methodology for its offices, that many organizations in the market adopted it voluntarily, and that INCD was working with sector regulators on adoption. Whether a particular sector regulator requires it should be checked with that regulator.

License included / downloadable: Yes The INCD document states that it constitutes a recommendation for all organizations in Israel and can be used freely to enhance the cyber resilience of the economy; the platform links to the INCD copy.

Full framework page and mappings: smartsuite.com/frameworks/israel-cdmo-v1-0-cyber-defense-methodology-for-organizations