

Israel CDMO v1.0

Israel CDMO v1.0 is a national cybersecurity methodology that helps Israeli organizations assess, implement, and manage cyber defense controls.



What it is

Israel CDMO v1.0 — Cyber Defense Methodology for Organizations is a national cybersecurity framework that enables organizations to assess, implement, and manage effective cyber defense controls. The methodology provides a structured approach to safeguarding organizational systems and sensitive data against evolving cyber threats while promoting continuous improvement in security posture.

Developed and published by the Israel National Cyber Directorate (INCD), the framework is intended for organizations operating in Israel across diverse industries, from critical infrastructure to commercial enterprises. Israel CDMO v1.0 covers key focus areas such as cybersecurity risk management, technical and administrative controls, incident response, and regulatory compliance, aligning with international standards and regional requirements.

At a glance

PUBLISHER Israel National Cyber Directorate	TYPE Framework	VERSION CDMO v1.0
EFFECTIVE 2023	DOMAIN Cybersecurity	FAMILY Other
REGION Israel	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: https://www.gov.il/en/departments/israel_national_cyber_directorate

Why it matters

- **Strengthen cybersecurity governance** Establishes clear policies and accountability, supporting executive oversight and effective management of security risks.
- **Enhance regulatory alignment** Ensures organizational practices meet national requirements and international standards, reducing gaps in regulatory compliance.
- **Improve risk management effectiveness** Enables organizations to prioritize, assess, and address cyber risks using a structured, repeatable methodology.
- **Increase audit readiness** Provides documented processes and evidence to simplify audit preparation and support ongoing compliance verification.

How SmartSuite supports Israel CDMO

Cybersecurity Governance and Control Management

Centralize cybersecurity policies, governance documentation, and security control ownership.

Cybersecurity Risk Identification and Remediation

Identify cybersecurity risks, track mitigation actions, and monitor remediation progress.

Security Incident Response Workflows

Track incident detection, investigation, response actions, and recovery processes.

Security Operations Monitoring

Manage threat alerts, investigations, and security operations activities across teams.

Third-Party Cybersecurity Risk Oversight

Monitor vendor cybersecurity posture and track supplier risk mitigation activities.

Security Posture and Program Maturity Reporting

Provide dashboards and reports showing security posture, open risks, and program maturity.

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 Israel CDMO v1.0 used for?

Israel CDMO v1.0 provides a comprehensive methodology to help organizations in Israel assess, implement, and manage cyber defense controls. It is used to protect critical systems and sensitive data, mitigate evolving cyber threats, and ensure compliance with national and international cybersecurity expectations.

Is Israel CDMO v1.0 mandatory or certifiable?

Israel CDMO v1.0 is not currently a certifiable standard, and its implementation is not strictly mandatory unless required by sector-specific regulations. However, adherence may be expected for organizations in critical infrastructure or those subject to regulatory oversight by the Israel National Cyber Directorate.

What organizations does Israel CDMO v1.0 apply to?

The framework is applicable to a wide range of organizations operating in Israel, including those in critical infrastructure sectors, commercial enterprises, and government entities. It is designed to be scalable and adaptable across industries with varying levels of cyber risk exposure.

What are the key concepts and required artifacts in Israel CDMO v1.0?

Key artifacts include a defined cybersecurity governance model, documented risk assessments, mapped control catalogs, incident response plans, and maturity models to evaluate cybersecurity posture. Organizations are expected to maintain records of risk evaluations, implemented controls, incident handling procedures, and ongoing compliance activities.

How is Israel CDMO v1.0 implemented in an organization?

Implementation involves conducting initial and periodic cybersecurity risk assessments, selecting and mapping appropriate security controls, and integrating these controls into existing governance and risk management processes. Ongoing compliance is managed by routinely reviewing controls, executing incident response exercises, and adapting to new threat intelligence.

How does Israel CDMO v1.0 relate to frameworks like ISO 27001 or NIST?

Israel CDMO v1.0 aligns with international standards such as ISO 27001 and NIST SP 800-53, enabling organizations to integrate its controls alongside established frameworks. This alignment supports broader compliance objectives and helps streamline audit and regulatory processes.

What is required to maintain compliance with Israel CDMO v1.0?

Organizations must perform routine compliance assessments, continuously monitor and update their risk posture, and ensure regular review of policies and controls. Maintaining evidence of ongoing improvements and adaptability to new threats is critical for sustained compliance.

How would SmartSuite support Israel CDMO v1.0?

SmartSuite helps organizations operationalize Israel CDMO v1.0 by providing centralized management of the control library, tracking risks and vulnerabilities, and automating evidence collection for compliance assessments. The platform supports effective policy governance, facilitates remediation workflows, and offers reporting dashboards that streamline audit readiness and provide real-time compliance insights.

License included / downloadable: Yes CDMO guidance is publicly available through the Israel National Cyber Directorate.

Full framework page and mappings: smartsuite.com/frameworks/israel-cdmov10-cyber-defense-methodology-for-organizations