SmartSuite

Framework / Cybersecurity / Other

Australian Government Information Security Manual (ISM)

The ISM is ASD's cyber security framework of principles, guidelines, and controls for IT and OT systems. It is advice, not law, unless legislation or a lawful direction compels compliance.



What it is

The Information security manual (ISM) is a cyber security framework produced by the Australian Signals Directorate (ASD) that an organization applies, through its own risk management framework, to protect information technology (IT) and operational technology (OT) systems from cyber threats. The current edition is the September 2026 edition, published on 7 September 2026.

The ISM is ASD's considered advice under its functions in the Intelligence Services Act 2001, not law. An organization is not required to comply with it unless legislation, or a direction given under legislation or by another lawful authority, compels it, and the ISM does not override legal obligations. It is written for chief information security officers, chief information officers, cyber security professionals, and IT and OT managers.

At a glance

PUBLISHER Australian Signals Directorate (ASD)	TYPE Framework	VERSION Information security manual (September 2026 edition)
EFFECTIVE 7 September 2026	DOMAIN Cybersecurity	FAMILY Other
REGION Australia	INDUSTRY Government & Public Sector	ADOPTION MODEL Voluntary
IMPLEMENTATION COMPLEXITY High		

Source: cyber.gov.au/ism

Why it matters

- **Controls marked by classification** Each security control carries an applicability marking: NC for non-classified systems, OS for OFFICIAL: Sensitive, P for PROTECTED, S for SECRET, and TS for TOP SECRET.
- **A defined authorization path** Systems move through define, select, implement, assess, authorize, and monitor, and the authorizing officer accepts the security risk of operating the system.
- **A documented authorization package** The package contains the system security plan, incident response plan, change and configuration management plan, continuous monitoring plan, security assessment report, and plan of action and milestones.
- **Flexible assessment** Non-TOP SECRET systems can be assessed by an organization's own assessors or Infosec Registered Assessors Program (IRAP) assessors, and TOP SECRET systems by ASD assessors.

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

How SmartSuite supports ASD ISM

ISM control catalog
Record guideline chapters and security controls with their NC, OS, P, S, and TS markings.

System security plans
Hold each system's boundary, criticality, objectives, and selected and implemented controls against its plan and annex.

Authorization records
Track the authorization package, the authorizing officer's decision, constraints, and any expiry date for each system.

Control assessment
Plan assessments, record results and recommended remediation, and track the plan of action and milestones.

Continuous monitoring
Log the events that trigger reassessment, such as new threats, ineffective controls, major incidents, and architecture changes.

Authorization reporting
Use Enterprise Reporting to show systems by authorization status, open actions, and assessment dates.

Common framework mappings

ASD Essential Eight | CIS Controls v8.1 | ISO 27001:2022 | ISO 27002:2022 | ISO 27701 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-53 Rev.5

Official resources

Australia Information Security Manual (ISM)
Provides detailed cybersecurity controls and guidance for securing Australian government systems.

cyber.gov.au/acsc/view-all-content/ism

ISM Guidelines
Outlines procedures and recommendations for implementing ISM cybersecurity measures effectively.

cyber.gov.au/ism

ISM Releases
Lists each quarterly ISM release, with downloadable archives for the last 24 months.

cyber.gov.au/ism/archived-ism-releases

Frequently asked questions

Is the ISM mandatory?
Not as a matter of law. ASD states that an organization is not required to comply with the ISM unless legislation, or a direction given under legislation or by another lawful authority, compels it. The ISM does not override legal obligations, and if it conflicts with legislation the legislation takes precedence.

What do the markings NC, OS, P, S, and TS mean?
They show which classification of system a security control applies to: NC for non-classified systems, OS for OFFICIAL: Sensitive, P for PROTECTED, S for SECRET, and TS for TOP SECRET. They help organizations select and tailor controls for each system.

What are the steps in the ISM risk management framework?
Define the system, select security controls, implement them, assess them, authorize the system, and monitor the system. The framework draws from NIST SP 800-37 Rev. 2, and the selection of controls is approved by the system's authorizing officer.

Who authorizes a system to operate under the ISM?
For non-classified, OFFICIAL: Sensitive, PROTECTED, and SECRET systems the authorizing officer is the organization's CISO or a delegate. For TOP SECRET systems it is the Director-General of ASD or a delegate. For services from commercial providers it is the CISO of the supported organization.

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

How does the ISM relate to the Essential Eight?

ASD publishes a mapping between the Essential Eight maturity model and the ISM. The ISM is a wider framework covering principles, guidelines, and controls across IT and OT systems, while the Essential Eight is a minimum set of eight mitigation strategies.

License included / downloadable: Yes The Australian Information Security Manual is published by the Australian Signals Directorate and is publicly available through the Australian Cyber Security Centre.

Full framework page and mappings: smartsuite.com/frameworks/australia-information-security-manual-ism

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