

# Australian Government Information Security Manual (ISM) — June 2024



The Australia Information Security Manual provides mandated cybersecurity controls and guidance to protect Australian government systems and data.

## What it is

The Australia Information Security Manual (ISM) is a cybersecurity framework that guides organizations in implementing effective security controls to protect Australian government systems and data. Its primary purpose is to support agencies in managing information security risks, safeguarding sensitive information, and ensuring the resilience of critical systems.

Published by the Australian Signals Directorate (ASD), the ISM is mandatory for Australian federal government departments and widely referenced by state agencies and contractors handling government information. The framework covers areas such as cybersecurity controls, data protection, risk management, system hardening, incident response, and compliance oversight, aligning with broader national security and privacy requirements.

## At a glance

|                                                                         |                                                               |                                                            |
|-------------------------------------------------------------------------|---------------------------------------------------------------|------------------------------------------------------------|
| <div>PUBLISHER</div> <div>Australian Cyber Security Centre (ACSC)</div> | <div>TYPE</div> <div>Framework</div>                          | <div>VERSION</div> <div>June 2024 Edition</div>            |
| <div>EFFECTIVE</div> <div>June 2024</div>                               | <div>DOMAIN</div> <div>Cybersecurity</div>                    | <div>FAMILY</div> <div>Other</div>                         |
| <div>REGION</div> <div>Australia</div>                                  | <div>INDUSTRY</div> <div>Government &amp; Public Sector</div> | <div>ADOPTION MODEL</div> <div>Regulatory Compliance</div> |
| <div>IMPLEMENTATION COMPLEXITY</div> <div>High</div>                    |                                                               |                                                            |

Source: <https://www.cyber.gov.au/acsc/view-all-content/ism>

## Why it matters

- Strengthen cybersecurity governance** Establish comprehensive oversight mechanisms to ensure effective implementation and maintenance of information security controls across the organization.
- Improve regulatory compliance** Support alignment with national security requirements, easing the burden of demonstrating compliance during internal and external audits.
- Promote operational resilience** Enhance the ability to continue critical operations by minimizing the likelihood and impact of cybersecurity incidents.
- Enhance incident response readiness** Enable prompt detection, containment, and remediation of security threats through structured incident response planning and processes.

How SmartSuite supports ASD ISM

ISM Control Library and Ownership

Organize ISM guidance into controls with owners, scope, and operating cadence.

System Hardening and Configuration Evidence

Centralize baselines, scan outputs, and configuration proof tied to controls.

Identity, Access, and Privilege Governance

Track MFA, privileged access, access reviews, and enforcement evidence.

Vulnerability and Patch Cadence

Schedule scanning, patching, remediation, and retesting with proof of completion.

Monitoring and Incident Response Workflows

Capture logging, alerting, incident timelines, and post-incident improvements.

Audit and Readiness Reporting

Report control coverage, gaps, exceptions, and progress across systems.

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](https://cyber.gov.au/acsc/view-all-content/ism)

ISM Guidelines

Outlines procedures and recommendations for implementing ISM cybersecurity measures effectively.  
[cyber.gov.au/acsc/view-all-content/ism/guidelines](https://cyber.gov.au/acsc/view-all-content/ism/guidelines)

ISM Updates

Describes the latest updates and revisions to the ISM framework.  
[cyber.gov.au/acsc/view-all-content/ism/updates](https://cyber.gov.au/acsc/view-all-content/ism/updates)

Frequently asked questions

What is the Australia Information Security Manual (ISM) used for?

The ISM is used to guide government agencies and associated contractors in implementing effective security controls to protect classified and sensitive Australian government information. It sets out a control-based approach to managing cybersecurity risks, safeguarding data, and ensuring the resilience of government-operated information systems. The ISM supports organizations in fulfilling regulatory and policy obligations for information security.

Is compliance with the ISM mandatory?

Yes, compliance with the ISM is mandatory for all Australian federal government departments and agencies. It is also a common requirement for third-party contractors and service providers who handle government information. State and territory agencies often reference or adopt ISM controls to align with federal security expectations.

What organizations or systems are within the ISM's scope?

The ISM applies to any organization processing, storing, or transmitting Australian government information, including federal departments, state bodies, and third-party contractors. It covers all information systems and environments that interact with government data, regardless of whether they are on-premises or cloud-based.

What key concepts and artifacts are required by the ISM?

The ISM requires organizations to establish and document security policies, risk assessment reports, control implementation records, and incident response plans. Key artifacts include a security risk management plan, system security plan, asset inventory, and evidence of compliance with control requirements. These artifacts support auditability and effective governance.

## How do organizations implement the ISM?

Implementation involves conducting risk and gap assessments, mapping ISM controls to organizational assets and business processes, and configuring technical and procedural safeguards. Organizations must maintain documentation to demonstrate how each control is addressed and regularly review and improve the effectiveness of implemented measures.

## How does the ISM relate to other cybersecurity frameworks?

The ISM aligns with international standards such as ISO 27001 and NIST SP 800-53, and can be mapped alongside them to enhance compliance and governance. Many organizations integrate ISM with other frameworks to streamline control selection, coordinate audit readiness, and meet overlapping requirements for national security and privacy.

## What ongoing compliance requirements does the ISM establish?

The ISM requires continual risk management, regular testing and review of controls, periodic reassessment of system vulnerabilities, and timely remediation of identified weaknesses. Compliance is monitored through internal audits, external assessments, and mandatory reporting to oversight bodies such as the Australian Signals Directorate.

## How would SmartSuite support the Australia Information Security Manual (ISM)?

SmartSuite facilitates ISM compliance by enabling organizations to import and manage the ISM control library, link controls to a centralized risk register and asset inventory, and track policy governance. It supports collection of evidence, ongoing compliance monitoring, workflow-driven remediation, audit preparation, and dashboard reporting to visualize control status and track remediation progress.

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-june-2024](https://smartsuite.com/frameworks/australia-information-security-manual-ism-june-2024)