IRAP

Implementation & Assessment Capabilities

Independent. Conflict-Free. Government-Ready.

Cybernion

www.cybernion.com | info@cybernion.com

What is IRAP?

An IRAP assessment is an independent validation of the effectiveness of an organisation's information security posture, conducted by ASD-endorsed assessors. It evaluates whether security controls genuinely work against the Australian Government ISM (Information Security Manual) and PSPF (Protective Security Policy Framework).

PSPF Policy 11 Requirement

Outsourced IT, cloud service providers, and gateway providers must be IRAP-assessed before processing or storing classified Government data.

Assessments must be repeated at least every 24 months, or after significant system changes.

1 **Effectiveness, Not Just Presence**

Controls must be shown genuinely working — reliable evidence is required, not a checklist tick.

2 **Systems Are Assessed, Not Organisations**

Only a specific information system can claim IRAP status. An organisation cannot.

3 **Reports Only, No Certification**

IRAP assessors produce reports. They do not accredit, certify, or endorse systems on behalf of the ASD.

Why IRAP?

Compliance & Risk

Mandatory for information systems handling classified Federal Government data

Government Contracts

Required to meet procurement rules and unlock agency and Defence business

Security Maturity

Structured uplift of Confidentiality, Integrity, and Availability

Competitive Advantage

Expected by central and state agencies and most Defence partners

Credibility & Trust

Demonstrates commitment to protecting sensitive Government data

Our IRAP Services

A holistic, conflict-free service across Advisory, Readiness, and Assessment with mutual exclusivity between readiness and assessment roles.

IRAP Advisory

- ISM & PSPF gap analysis
- Security architecture review
- Control design and guidance
- Scope definition support
- Regulatory interpretation

IRAP Readiness

- Control implementation
- Evidence collection & management
- Documentation (SSP-A, SRMP, SOPs)
- Staff training and awareness
- Continuous compliance monitoring

IRAP Assessment

- ASD-endorsed assessor delivery
- Technical testing & verification
- Risk analysis across all layers
- IRAP Assessment Report
- Cloud Controls Matrix (CCM)

IRAP Assessment Process

Four stages, required at least every 24 months, or when significant changes occur.

1 Plan & Prepare

- Define scope, objectives & timeline
- Identify key security personnel
- Establish communication process
- Review existing documentation

2 Scope Definition

- Map system boundaries & data flows
- Identify classified data touchpoints
- Agree assessment layers & interfaces
- Define evidence requirements

3 Assess

- In-depth technical testing
- Control verification against ISM
- Risk analysis across each layer
- Shared-responsibility review

4 Report

- IRAP Assessment Report
- Cloud Controls Matrix (CCM)
- Detailed findings & recommendations
- Pathway to ongoing compliance

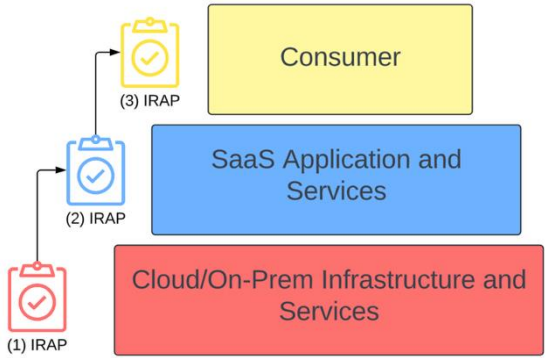
Case Study 1 - IRAP Assessment

An Australian Federal Agency managing sensitive citizen data engaged us to conduct an IRAP assessment of their multi-layered information system, including AWS cloud infrastructure, a government-specific SaaS application, and an external user portal.

Requirements

- Assess the effectiveness of security controls deployed to AWS cloud infrastructure and hosted application and databases based on ISM and PSPF requirements for handling sensitive citizen data
- Assess the security of the external user portal that provides citizens an interface to manage their personal information
- Provide recommendations to uplift security maturity and compliance with PSPF and ISM

Our Solution



By assessing each layer independently and in relation to the others, we helped the Federal Agency identify and address specific opportunities, ensuring that the entire system meets relevant security requirements while effectively sharing responsibilities among the involved parties.

Key Highlights

- **Plan and Prepare:** Define clear objectives, timeline, and comms process
- **Define the Scope:** Scope the assessment to cover AWS infrastructure, SaaS application security, and user access controls on the portal
- **Assess:** Conduct in-depth technical testing, control verification, and risk analysis for each layer
- **Report:** A detailed assessment report and Cloud Control Matrix (CCM) to highlight strengths and opportunities for improvement to appropriately protect data and comply with PSPF and ISM

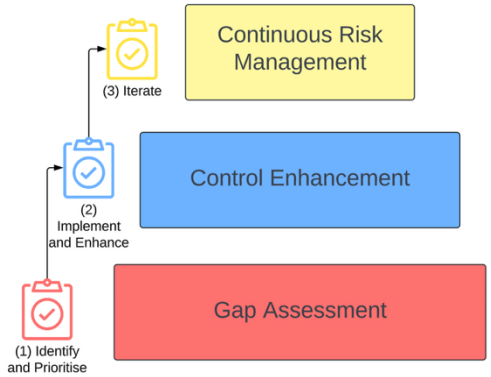
Case Study 1 - IRAP Readiness

A major service provider bidding for Government and Defence contracts needed to uplift internal security controls in line with PSPF and ISM standards to ensure compliance across all layers, including infrastructure, applications, and data management.

Requirements

- Align security controls with PSPF and ISM standards to uplift maturity and prepare for an IRAP assessment
- Ensure compliance across multiple layers, including infrastructure, applications, and data management, to protect sensitive government information
- Facilitate a smooth IRAP assessment by implementing robust security practices and ensuring ongoing compliance
- Establish repeatable evidence collection and management process to support multiple assessments

Our Solution



A comprehensive gap analysis to identify areas where current practices did not align with ISM and PSPF requirements, followed by implementation of security controls and establishment of continuous compliance monitoring to ensure the organisation was fully prepared for the IRAP assessment.

Key Highlights

- **Gap Analysis:** A comprehensive assessment to identify gaps between existing practices and PSPF/ISM requirements
- **Control Implementation:** Strengthen security controls across infrastructure, applications, and data management systems to meet requirements
- **Continuous Monitoring:** Monitoring mechanisms to ensure ongoing compliance and readiness for IRAP assessments
- **Documentation and Training:** Detailed documentation and training to staff to support the new security protocols and ensure alignment with PSPF and ISM

Important IRAP Artefacts

The documents your assessor will examine, and what you receive in return.

Input: What You Provide

SSP-A	System Security Plan Annex
SOD	System Overview Document
SRMP	Security Risk Management Plan
SOPs	Standard Operating Procedures
IRP	Incident Response Plan
DRP	Disaster Recovery Plan
BCP	Business Continuity Plan
PMP	Patch Management Plan
ELP	Event Logging Plan
KMP	Key Management Plan

+ Other policy and process documents as agreed during scoping.

Output: What You Receive

1 IRAP Assessment Report

A comprehensive evaluation of security control effectiveness against ISM and PSPF requirements, covering identified risks, gaps, and their severity, with remediation guidance.

2 Cloud Controls Matrix (CCM)

A structured mapping of cloud security controls assessed against PSPF/ISM, enabling clear shared-responsibility analysis across service layers (infrastructure, platform, application).

Thank You

Ready to start your IRAP journey? Let's talk.



Web www.cybernion.com.au

FAQs www.cybernion.com.au/insights

Email info@cybernion.com

Phone 0404 760 923

A Trusted Cyber Companion