Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

IRAP consumer guide

Content Complexity
MODERATE ● ● ○

cyber.gov.au

Executive summary

Purpose

The purpose of this document is to provide guidance for customers and consumers of Infosec Registered Assessors Program (IRAP) assessments and services.

Intended audience

This document is intended for:

- consumers who are trying to engage an IRAP assessor for an IRAP assessment
- consumers managing an IRAP assessment, such as system owners, program managers and project managers
- decision-makers who will use an IRAP security assessment report as part of an authorisation package.

Authority

This document represents the considered advice of the Australian Signals Directorate (ASD).

IRAP objective

The objective of IRAP is to enhance Australia's cyber security posture by providing organisations access to highly-skilled cyber security professionals who can help inform their cyber risk assessments.

IRAP assessors provide independent quality assessments on the security of an organisation's systems and services to support consumer's decision making on whether to authorise a systems use.

Table of contents

Executive summary 2

Purpose 2

Intended audience 2

Authority 2

IRAP objective 2

Consumer guidance for IRAP 4

Infosec Registered Assessors Program 4

Value of IRAP 4

Government requirements 4

IRAP assessors 5

Entity assessor versus IRAP assessor 6

Engaging an IRAP assessor; preparing for an IRAP assessment 7

Engaging an IRAP assessor 7

Conflict of interest 7

Preparing for an IRAP assessment 7

Consumer guidance on IRAP assessments 8

The IRAP assessment process 8

IRAP assessment timeframes 8

Consumer guidance for post-IRAP assessment 9

IRAP feedback 9

IRAP security assessment report 9

Authorisation package 9

Multiple service providers 10

Marketing an IRAP assessment 10

Appendix A 11

IRAP RFQ Template 11

Appendix B 12

IRAP Checklist 12

Consumer guidance for IRAP

Infosec Registered Assessors Program

The Australian Signals Directorate (ASD), via the Infosec Registered Assessors Program (IRAP), provides organisations with access to high-quality, independent security assessment services using suitably qualified and endorsed cyber security professionals, known as IRAP assessors.

An IRAP assessor will:

- work to understand the system and the system owner's security requirements
- identify applicable controls from the *Information Security Manual* (ISM)
- assess the effectiveness of those controls, and
- provide an IRAP security assessment report that outlines the system's security strengths and weaknesses, the outcomes of the controls assessment, and recommendations to improve the system's security posture.

A completed IRAP assessment does not imply that a system is compliant, endorsed or approved by ASD, or indeed 'secure'. Rather, it is an important tool for customers to read and understand in order to determine the effectiveness of controls and decide whether the residual security risks associated with operating the system are within their organisation's security risk appetite.

An IRAP assessor will not accredit, certify, endorse or register a system on behalf of ASD.

Value of IRAP

IRAP assessments are high-quality risk-based security assessments conducted by an IRAP assessor. As such, they play a key role in an organisation's decision to authorise a system for use or operation. Specifically, they assist an authorising officer in identifying and understanding the security risks associated with the use of the system.

Government requirements

The *Directive on Security of Government Business* establishes the Protective Security Policy Framework (PSPF) as Australian government policy. The PSPF is owned and developed by the Department of Home Affairs. Non-corporate Commonwealth entities that are subject to the *Public Governance, Performance and Accountability Act 2013* must apply the PSPF (to the extent consistent with legislation).

Under PSPF Policy 11: Robust ICT systems, outsourced information technology, cloud service providers, and gateway providers must be IRAP-assessed prior to processing and storing government data.

On-premises government systems at SECRET and below can have a security assessment conducted by either an IRAP assessor or an entity assessor. In addition, Requirement 1 of PSPF Policy 11: Robust ICT systems requires that 'an ICT system is authorised to operate by the relevant determining authority based on the acceptance of any residual security risks associated with its operation'.

A summary of the determining authority (authorising officer), the security assessor, and the type of ICT system to which they apply is provided at Table 1.

Table 1 - Security assessor and determining authority for authorisation of an ICT system

Type of ICT system	Security assessor	Determining authority (Authorising Officer)
TOP SECRET system	Australian Signals Directorate assessor (or their delegate)	Director-General ASD (DGASD) or their delegate
TOP SECRET sensitive compartmented information system	Australian Signals Directorate assessor (or their delegate)	DGASD or their delegate
SECRET system	Entity assessor or IRAP assessor	Accountable Authority or Chief Security Officer or their delegate
PROTECTED and OFFICIAL: Sensitive systems	Entity assessor or IRAP assessor	Accountable Authority or Chief Security Officer or their delegate
Multinational and multi-entity system	Determined by agreement between the parties involved	Determined by a formal agreement between the parties involved
Outsourced information technology and cloud services (with the exception of a TOP SECRET system)	IRAP assessor	Accountable Authority or Chief Security Officer or their delegate
Gateways	IRAP assessor	Accountable Authority or Chief Security Officer or their delegate

IRAP assessors

Cyber security professionals endorsed by ASD as IRAP assessors must meet the minimum prerequisite requirements outlined in the IRAP Policy and Procedures. This ensures that the assessors have the appropriate skills and experience to provide IRAP services.

An IRAP assessor's experience may vary across a range of systems and environments. When engaging an IRAP assessor, consumers should seek adequate assurance that the assessor has the appropriate experience and knowledge to provide an effective assessment for the type of system or environment requiring assessment (e.g. cloud service, gateway, critical infrastructure).

IRAP assessors must ensure that they remain independent of the system or environment they are assessing. IRAP assessors cannot have contributed to the design and implementation of a system if they are to assess it. This includes drafting the system's documentation, conducting an initial gap assessment, providing design recommendations or having a material interest in the system (e.g. an IRAP assessor that works for a service provider cannot conduct an IRAP assessment of their services, unless specifically hired for that purpose under contract).

In addition, IRAP assessors who are permanent employees of an organisation cannot conduct IRAP assessments for that organisation, regardless of the level of involvement in the design of the system.

Due to the required independence of an IRAP assessment, IRAP assessors do not provide a recommendation on whether a system is suitable for authorisation. Decisions to accept residual security risk and authorisation of the system to operate are the responsibility of the authorising officer.

Entity assessor versus IRAP assessor

An entity assessor is someone who is employed or contracted on an ongoing basis to conduct security assessments of systems.

Entity assessors follow the procedures and processes defined by the organisation and are not bound by IRAP requirements, such as independence and adherence to the IRAP assessment process. There are no mandatory experience or skills requirements to be an entity assessor. It is up to the individual organisation to appoint an entity assessor as they see fit.

Conversely, IRAP assessors have demonstrated that they meet the skills and knowledge requirements set by ASD; including a combination of industry certifications, work experience, IRAP training and passing the IRAP exam. IRAP assessors conducting IRAP assessments must follow the IRAP policies, processes and procedures outlined by ASD.

If an IRAP assessor is unable to fulfil the independence requirements of IRAP, but they conduct an assessment regardless, they would be performing this function as an entity assessor for that assessment, rather than as an IRAP assessor.

IRAP assessment outcomes

Consumers will receive an IRAP security assessment report, which is based on the IRAP security assessment report templates, at the end of the assessment process.

They will also receive an assessment control matrix (a derivative of the System Security Plan Annex Template), which outlines an assessment of the implementation status of each applicable ISM control as well as a justification for that assessment.

The IRAP security assessment report outlines the findings of the assessment, including the system's security strengths and weaknesses. A plan of action and a 'milestones' document support the uplift of the system by detailing control recommendations. This can be used as part of an organisational security program or uplift project.

Engaging an IRAP assessor; preparing for an IRAP assessment

Engaging an IRAP assessor

ASD provides a comprehensive list of IRAP assessors on cyber.gov.au website. Although all IRAP assessors have met the standard as required by ASD, some may possess additional experience and expertise; making them more suitable to conduct an IRAP assessment on a specific system or environment.

Consumers seeking to engage an IRAP assessor should exercise due diligence during the hiring process to ensure the IRAP assessor engaged has the relevant experience and expertise to assess the system or environment in question.

Conflict of interest

An IRAP assessor is required to maintain independence at all times and must not have been involved in any capacity in the design or development of the system being assessed.

IRAP assessors are required to complete a conflict of interest form prior to any IRAP assessment engagement. A conflict of interest form is submitted via ASD's Partner Portal. IRAP assessors must outline and manage any perceived or actual conflicts of interest, and specify the mitigations that are in place.

Consumers should be aware of these requirements when engaging and working with an IRAP assessor.

More information on conflict of interest requirements for IRAP assessors can be found in the IRAP Policy and Procedures.

Preparing for an IRAP assessment

Planning for an IRAP assessment differs depending on the organisation type, structure and system.

The following activities are recommended to allow for a smooth assessment:

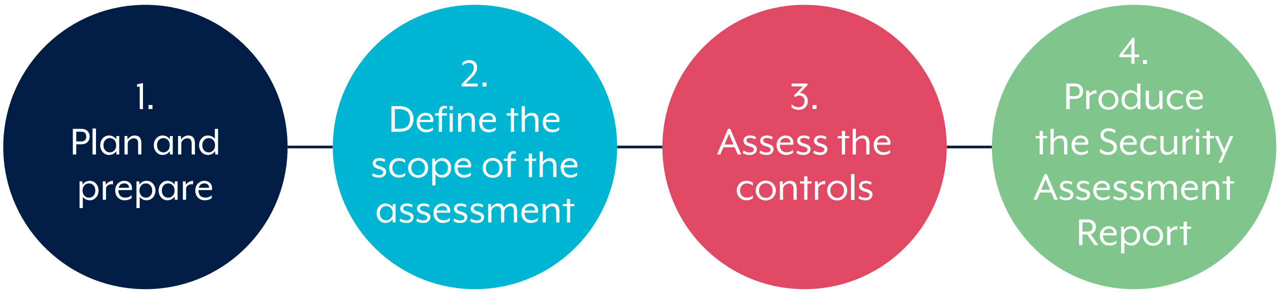
- Ensure that the required system documentation has been developed, is accurate and has been approved by the relevant authority. Documentation may include:
    - a security risk management plan
    - system design documents
    - a system security plan
    - a system security plan annex
    - a cyber security incident response plan
    - a continuous monitoring plan
    - the system security policies, processes and procedures.
- Ensure availability of relevant system personnel, such as the system owner, system administrators and security operations personnel, in order to support the assessment and evidence gathering.
- Where possible, begin to plan and collect evidence to support control assessments (request an initial list from the IRAP assessor, using the system security plan annex as a guide).
- Be prepared to provide any other relevant information that will provide additional context to the IRAP assessor, such as previous security assessment reports.

Consumer guidance on IRAP assessments

The IRAP assessment process

During an IRAP assessment, the IRAP assessor will leverage several Australian government frameworks, policies and guidelines, such as the PSPF and ISM. IRAP assessors may consider additional frameworks as input for IRAP assessments, such as the Department of Home Affair's Hosting Certification Framework certification reports and other physical security certification reports.

IRAP assessments include 4 key stages, as outlined in the IRAP Assessment Process Guide:



1. Plan and prepare

2. Define the scope of the assessment

3. Assess the controls

4. Produce the Security Assessment Report

During an IRAP assessment, and when determining control implementation and effectiveness, IRAP assessors will use the standardised assessment outcomes:

- **Effective** – The organisation is effectively meeting the control's objective.
- **Ineffective** – The organisation is not adequately meeting the control's objective.
- **Alternate Control** – The organisation is effectively meeting the control's objective through an alternative control.
- **Not Assessed** – The control has not yet been assessed.
- **Not Applicable** – The control does not apply to the system or environment.
- **No Visibility** – The assessor was unable to obtain adequate visibility of a control's implementation.

IRAP assessment timeframes

IRAP assessments vary in length based on several factors, including the size and scope of the assessment; the complexity of the system; the availability of key security personnel and evidence to support the assessment; and the assessor's familiarity with the type of organisation, environment and system under assessment.

To reduce the length of an IRAP assessment, thorough planning and preparation should be conducted beforehand by the organisation.

Consumer guidance for post-IRAP assessment

IRAP feedback

Consumers of IRAP services are encouraged to submit feedback to ASD about their experience with their IRAP assessor, the assessment process and the quality of the service.

IRAP security assessment report

An IRAP security assessment report should provide an organisation with information relating to the security risks associated with the use of a system or service. It should inform the authorisation decision and include:

- an overview of the system and types of environments; e.g. administration, test, development
- the assessment details, including the assessment boundary
- the system's security strengths and weaknesses
- the governance arrangements
- the detailed findings, with supporting information and evidence
- the recommended remediation activities
- the completed assessment controls matrix as an annex.

IRAP assessors are encouraged to use the Cloud Security Report Template or the IRAP Assessment Report Template.

What is considered an acceptable level of risk for an organisation will differ depending on their objectives, culture and operating environment. Therefore, it is important to consider the information in an IRAP security assessment report within the context of your organisation's objectives and risk tolerances. Likewise, it is important that IRAP assessment information is made available to other entities considering the use of your services to inform their risk-based decision-making.

When authorising a system, the authorising officer should seek an appropriate balance between system functionality and security risk.

IRAP assessors do not provide a recommendation to authorise, or not authorise, a system. It is not the role of an IRAP assessor to determine the acceptable level of security risk on behalf of the organisation.

Authorisation package

The IRAP security assessment report will form a key component of the authorisation package for a system. The authorisation package is the suite of reports and documents provided to the authorising officer to support their decision to authorise the system, or not.

The authorisation package should consist of the following documents at a minimum:

- a system security plan
- a cyber security incident response plan
- a continuous monitoring plan
- a security assessment report, such as an IRAP security assessment report
- a plan of action, and milestones if applicable.

Multiple service providers

It is important to note that the authorisation package will vary depending on the nature of the management and ownership of a system. For example, if an organisation is looking to use a cloud service, it is likely that the cloud service provider has had an IRAP assessment of that service. Once this has been confirmed, the consuming organisation will conduct an IRAP assessment covering only the aspects of the service they are responsible for designing, configuring or managing.

The following diagram shows the layered approach IRAP takes to support the authorisation decision.

Layer 1 (Cloud infrastructure provider)

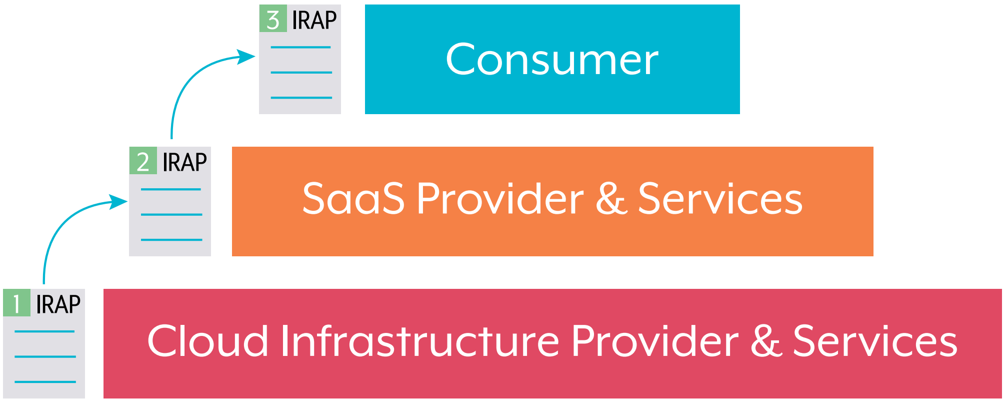
This security assessment covers the infrastructure layer and the responsibilities of the cloud infrastructure provider in managing the infrastructure layer.

Layer 2 (SaaS provider)

This security assessment covers the Software-as-a-Service (SaaS) layer and specifies the responsibilities of the SaaS provider. It should also link to the infrastructure security assessment by including key considerations provided within that layer's IRAP security assessment report.

Layer 3 (Consumer)

This security assessment covers the security responsibilities of the consumer. It should also leverage the IRAP security assessment reports from the preceding 2 layers to provide the relevant information to the authorising officer in a single report.



Marketing an IRAP assessment

Service providers that have completed an IRAP assessment may want to advertise and market this fact. In doing so, there are several considerations that should be made to ensure that the marketing of the IRAP assessment aligns with the intent of the program:

- Under no circumstances should service providers state or imply that their services or systems are certified, authorised or approved by, or compliant with:
  - ASD;
  - IRAP;
  - the Australian Government;
  - any level of Australian government data classification (e.g. PROTECTED).

  Rather, here is an example of appropriate terminology: 'Organisation X has completed an IRAP assessment against the Information Security Manual's PROTECTED level controls.'
- Service providers should make their IRAP security assessment reports readily available to potential consumers to support their decision on whether or not to adopt their service(s). An assessment cover letter alone does not provide the potential consumer sufficient information to understand the security risks associated with consuming a service.

Appendix A

IRAP RFQ Template

The following template provides a typical fit-for-purpose Request for Quote (RFQ) that can be tailored as required when seeking to engage an IRAP assessor.
The template should be adjusted to support any specific requirements.

[Insert organisation name] is seeking an IRAP assessor to conduct an IRAP assessment for our [insert system name]. The purpose of this IRAP assessment is to ensure security risks are identified and understood to support the 'authority to operate' decision.

In accordance with IRAP requirements, the IRAP assessment must be independent and objective; provide an overview of the security posture of the system, including strengths, weaknesses, vulnerabilities and security risks stemming from control deficiencies; and provide recommendations to mitigate security risks.

Scope of work:

The IRAP assessor will be required to perform the following tasks:

- conduct a thorough and independent high-quality assessment in accordance with the IRAP Assessment Process Guide
- prepare a detailed report using either the Cloud Security Report Template or the IRAP Assessment Report Template
- provide an independent and objective view of the security posture of the system, including strengths, weaknesses and vulnerabilities
- identify security risks associated with control deficiencies
- present clear and actionable recommendations to mitigate identified security risks.

Assessor requirements:

The IRAP assessor will be required to have:

- demonstrated expertise in conducting IRAP assessments for systems within [insert environment/system type]
- relevant certifications related to cyber security and the [insert environment/system-related certification]
- proven experience and expertise in assessing systems similar to [insert system name] in size, complexity and sensitivity
- familiarity with Australian government security frameworks, policies and guidelines
- strong communication and reporting skills to effectively convey findings and recommendations.

Timeline and location:

- Estimated start date: [insert estimated start date]
- Initial contract duration: [insert initial contract duration]
- Extension term: [insert extension term]
- Location of work: [insert location of work]
- Security clearance required: [insert security clearance requirements].

Submission of RFQ response:

Interested IRAP assessors are invited to submit their detailed RFQ response by [insert submission deadline].

Responses should include the following:

- an overview of your experience and expertise in conducting IRAP assessments for systems similar to [system name]
- the details of relevant certifications and experience
- a proposed project plan including timelines and milestones
- the proposed team members and their experience
- a breakdown of the costs associated with the assessment
- any contact information for references from previous IRAP assessment customers (if available).

Appendix B

IRAP Checklist

ASD has provided consumers with a baseline checklist to assist in preparing for an IRAP assessment. Consumers should consult with their engaged IRAP assessor for advice on any specific additional evidence requirements.

Item no.	Item description	Prepared
1.	Define assessment timelines (start / end dates and milestones) with IRAP assessor.	□
2.	Define and agree the scope of system and assessment boundary to be assessed with IRAP assessor	□
3.	Complete any on-boarding requirements for IRAP assessor (system access, facility access, clearance check or police checks)	□
4.	Advise and schedule personnel to be available during the assessment period (system administrators, security personnel or system owners).	□
5.	Prepare documentation evidence, including: • system security plan and annex • risk management documents • design and architectural documents • incident response plans and playbooks • organisational policies • standard operating procedures • security test cases and test plans • business continuity plans and disaster recovery plans • configuration and build documents • continuous monitoring plans • service provider security contract (extracts) • previous assessments or penetration tests conducted • hardening guidelines used.	□
6.	Confirm any additional evidence requirements with IRAP assessor, like: • screenshots of system configurations, and cryptographic protocols and algorithms. • automated and manual testing of controls conducted • log files • vulnerability scan results and configurations • personnel prepared to conduct process or control demonstration • History of patching, testing of backup and restoration exercises.	□

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre