Australian Government
Australian Signals Directorate

Australian Cyber Security Centre

ASSESSMENT PROCESS GUIDE

AUSTRALIAN SIGNALS DIRECTORATE INFOSEC REGISTERED ASSESSORS PROGRAM

cyber.gov.au

Guidance on the IRAP assessment process

Purpose

1. The purpose of this document is to provide guidance on the IRAP assessment process and key considerations during each stage of an assessment. This document should be read in conjunction with other IRAP guidance including:
   - *IRAP Policy and Procedures Manual*
   - *IRAP Assessment Reporting Guidance*
   - *Anatomy of a Cloud Security Assessment and Authorisation*
   - *System Security Plan Annex Template*
   - *Cloud Security Assessment Report Template*
   - *IRAP Assessment Report Template.*

Table of Contents

Overview

2. An IRAP assessment is an independent assessment of the implementation, appropriateness and effectiveness of a system's security controls. IRAP assessment outcomes are documented within a security assessment report (commonly referred to as an IRAP report), which is used by consumers to conduct their own assessment and authorisation of a system's suitability for their security needs and risk appetite.

3. While the approach taken to conducting an IRAP assessment may depend on the size and complexity of a system, there are foundational assessment stages and principles which should be applied to each assessment.

4. IRAP assessors should incorporate the guidance within this document to help ensure IRAP assessments meet their objectives and the expectations of the consumers of security assessment reports.

The Australian Cyber Security Centre (ACSC), as part of the Australian Signals Directorate (ASD), provides cyber security advice, assistance and operational responses to prevent, detect and remediate cyber threats to Australia. The ACSC is here to help make Australia the most secure place to connect online.

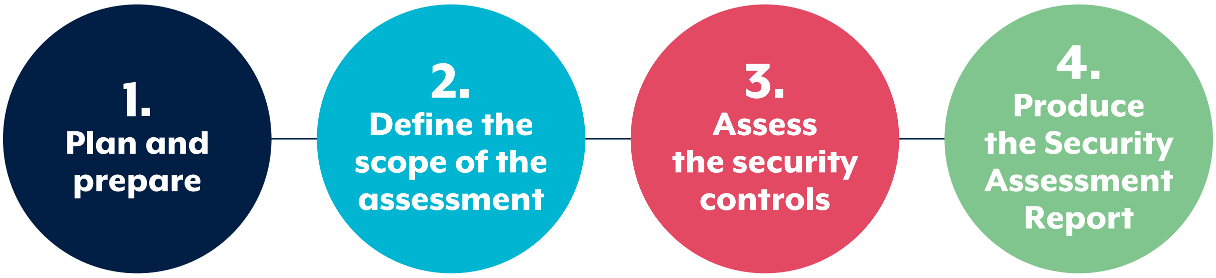
For more cyber security information, guides and advice visit the ACSC's website cyber.gov.au.

If you think you're a victim of cybercrime report it through ACSC's ReportCyber on cyber.gov.au or call our Cyber Security Hotline on 1300 CYBER1 (1300 292 371).

Keep up to date on the latest cyber threats: Sign up to the ACSC's free alert service online at cyber.gov.au.

Stages of an IRAP assessment

5. The IRAP assessment process contains four key stages as shown in the figure below.



1. Plan and prepare

2. Define the scope of the assessment

3. Assess the security controls

4. Produce the Security Assessment Report

6. Detail on the activities and considerations within each stage are as follows:

Stage 1: Plan and prepare

7. The plan and prepare phase consists of the following activities:

8. The IRAP assessor informing the ASD IRAP Administrator, via asd.irap@defence.gov.au of the IRAP engagement by submitting a Conflict of Interest (COI) declaration form.

9. The IRAP assessor conducting engagement planning activities. These activities require the assessor to determine in consultation with the client organisation the:

   - assessment start date, duration and milestones
   - access to resources required to undertake the assessment including documentation, systems, tools, personnel and facilities
   - system and control testing activities
   - evidence collection process and evidence protection
   - approach to stakeholder engagement and consultation
   - version of the ISM that will be used for the assessment
   - appropriate use and marketing of the security assessment report
   - availability of the security assessment report and evidence to ASD for quality assurance purposes.

10. IRAP assessors may develop a security assessment plan to document this information and share it with the client organisation.

Stage 2: Define the scope of the assessment

11. The scope of an IRAP assessment includes both the authorisation boundary of the system under assessment, as well as the security controls applicable to the assessment of that system. The scope of an IRAP assessment should be defined early in the assessment by the IRAP assessor coming to an agreement with the System Owner on:

    - The system version and environment under assessment (e.g. PROD or TEST, and the implications of the latter).
    - The intended security classification of the data stored, processed or communicated by the system.
    - The authorisation boundary of the system (i.e., the system components under assessment as well as the people, processes, technologies and facilities that the system relies on or impact its security posture).

12. The client organisation may already have a view of the scope of an assessment, however it is the IRAP assessor's responsibility to validate the accuracy of the scope. To help define the scope of an assessment, IRAP assessors can:

    - Gain an understanding of the system including its function, processes, data, users, architecture and technology stack.
    - Identify the parties (including suppliers) involved in delivering or maintaining the system and its security controls. This includes identifying the shared responsibility model and security control inheritance.
    - Use the system security plan annex and logical system diagrams to identify the security controls in scope for the system.

13. The scope of the assessment should be clearly articulated within the security assessment report. Any system components or environments deemed out-of-scope should also be documented and accompanied by a justification for its exclusion from the assessment.

Stage 3: Assess the security controls

14. In this phase, the IRAP assessor reviews evidence provided by the client organisation to determine the implementation status of security controls. Security control review activities are typically divided into two categories:

    - Design effectiveness review:
        - The assessor reviews the documented system (i.e. system architecture, security policies, procedures, plans, etc.) and determines whether relevant controls have been scoped for the system and unique risks to the system have been addressed.
        - Personnel interviews may also be required at this stage to confirm the accuracy of documentation and/or fill gaps in poor documentation.
        - The design effectiveness review provides the assessor with an understanding of the system and its security controls, and provides the foundation for further control validation activities.
    - Operational effectiveness review:
        - The assessor conducts control validation activities to determine whether the documented security controls have been implemented and are operating effectively. The determination of operational effectiveness requires a combination of personnel interviews, live demonstrations of systems and security controls, system testing and site inspections (if applicable).
        - Operational effectiveness review provides a higher level of assurance on the implementation of a security control and whether it can be assessed as effective.

15. IRAP assessors must consider the quality of evidence provided during an assessment and its impact on assessment outcomes. The goal is to review evidence that provides a high level of assurance on the implementation of a security control. If an IRAP assessor cannot obtain sufficient evidence during an assessment, this limitation should be documented within the security assessment report. For additional guidance and considerations, see the Quality of Evidence section at paragraphs 21 and 22.

Stage 4: Produce the security assessment report and security controls matrix

16. Upon the completion of the assessment, the assessor produces a security assessment report to document the outcomes of the assessment. At a high-level, a security assessment report describes:

    - The scope of the security assessment.
    - The effectiveness of the implementation of security controls.
    - Security risks associated with the operation of the system.
    - Any recommended remediation actions.

17. IRAP assessors are not required to undertake a risk assessment of ineffective controls, only identify security risks and risk mitigating controls so that the consumer of the report can undertake their own assessment of those risks. IRAP assessors should only describe identified risks and should not rate risks on behalf of report consumers. It is up to the consumer of the report to determine the level of risk exposure within their environment.

18. In addition to the security assessment report, the IRAP assessor documents the security controls matrix (SCM) or cloud SCM (CSCM). The SCM contains assessment observations against each ISM control.

19. IRAP deliverables are required to follow the guidance provided by ACSC on ACSC IRAP Resources. The guidance covers deliverable content requirements and the appropriate language for describing security control implementations.

20. It is important that IRAP assessors do not include any marketing materials, biased or misleading statements within IRAP deliverables. This includes language that states or implies that the IRAP assessment provides certification, accreditation, endorsement, approval or authorisation to operate for a system.

Quality of Evidence

21. Access to evidence as well as the quality of evidence provided during an IRAP assessment impacts an IRAP assessor's ability to determine the implementation status of a security control. IRAP assessors should consider the following examples of poor, fair, good and excellent evidences:

    - **Poor evidence:** A policy statement that repeats the ISM control in an internal document, irrespective of the amount of boilerplate included. Another example of poor evidence is verbal confirmation that a control has been implemented.
    - **Fair evidence:** Reviewing a copy of the relevant system's configuration to determine if it should enforce the expected policy.
    - **Good evidence:** Reviewing the technical configuration on the system (through the systems' interface) to determine it should enforce the expected policy.
    - **Excellent evidence:** Testing the control with a simulated activity designed to confirm it is in place and effective (e.g. attempting to run an application to check for application control, or attempting to access an external website using a privileged account).

22. IRAP assessors should use strong sources of evidence for an IRAP assessment and should discuss evidence expectations with the client organisation. IRAP assessors are encouraged to apply better practice to evidence collection. If sufficient or quality evidence cannot be provided during an assessment, the IRAP assessor should document this limitation within the security assessment report and SCM. Security assessment report consumers should be informed of the lack of information necessary to make a risk-based decision to use a system.

Related Legislation, Directives, Policies and Processes

1. Protective Security Policy Framework (PSPF)
2. Information Security Manual (ISM)
3. Essential Eight and Strategies to Mitigate Cyber Security Incidents
4. IRAP Policy and Procedures
5. IRAP Assessment Reporting Guidance
6. Anatomy of a Cloud Security Assessment and Authorisation
7. Security Assessment Report Template
8. Cloud Security Assessment Report Template

Getting Help

9. For further assistance, please contact asd.irap@defence.gov.au

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

ACSC Australian **Cyber Security** Centre