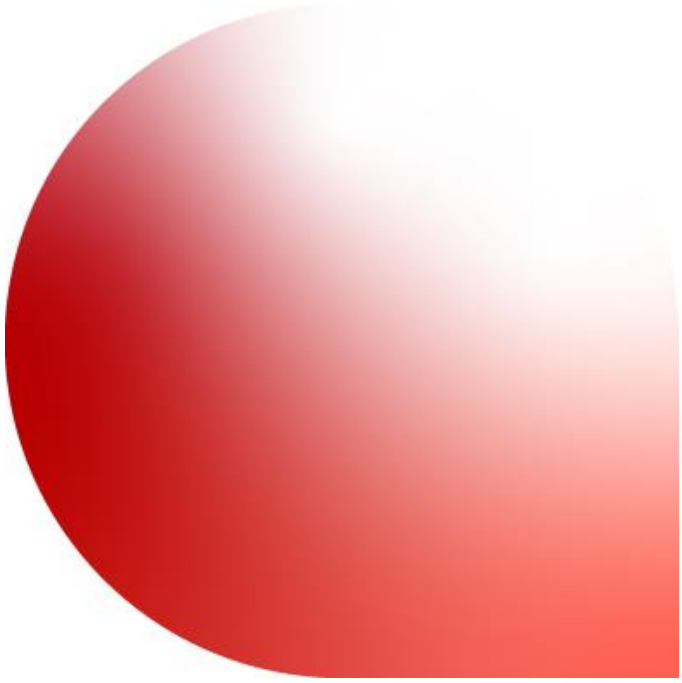

IRAP Assessment Reporting Guide

08/2021

Australian Signals Directorate
Infosec Registered Assessors Program

IRAP Assessment Reporting Guide

This document is designed to assist you when writing IRAP assessment reports.

Executive summary

The executive summary should provide an overview of the engagement and the system's security posture. This includes a description of the scope of the security assessment, the effectiveness of assessed security controls, key risks associated with the operation of the system and recommendations for improvement where required.

The dates of the assessment, the ISM version used and the maximum security classification that the system was assessed against should also be noted.

The report should not impinge on the Authorising Officer's remit to make a risk-based decision on whether or not to authorise the system to operate.

Introduction

Background

Describe the context of the organisation and the system under assessment, including any previous security assessments, issues or ongoing recommendations.

System overview

Provide a description of the system's function, users, technologies and architecture. Any other relevant details including the location of the system, location of operations and support, service providers and dependencies, and shared responsibilities should also be described.

Approach and methodology

Identify the system boundary and system components covered by the security assessment. Detail any assumptions or constraints.

Describe how security controls were reviewed for their effectiveness. Describe any sampling used and evidence collection techniques.

Evidence

List all documents reviewed, personnel interviewed and other evidence reviewed as part of the assessment.

Detailed findings

Articulate the findings of the assessment. Security control implementations should be described in a structured manner and supported by objective evidence. Consider the following structure:

- description of the finding
- description of evidence supporting the finding
- implication of the finding (or security risk)
- concluding statement on security control effectiveness.

If a security control was considered ineffective, and presents a security risk, provide a recommendation for improvement.

Appendices

Appendices can be used to provide any other relevant information about the security assessment. For example, physical security certifications, assessment evidence and assessment outcomes for each ISM security control.