IRAP ASSESSMENT REPORTING GUIDE

Australian Government
Department of Defence

IRAP Assessment Reporting Guide

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

Executive Summary

The executive summary should provide an overall summary of the entire report, with all key considerations clearly stated in a concise manner. The executive summary should include all non-compliant Information Security Manual (ISM) controls, with the recommendations for each. Any further additional concerns should be highlighted. Suitability for certification by the Australian Signals Directorate (ASD) should also be stated, including the recommended classification level and time frame for certification (with a maximum of one year as per the ISM).

Introduction

Background

The background should detail all system environment details, including the design, operator, name of key facilities and locations. The customers and users of the system environment should also be identified in order to help define associated risks, however, only when appropriate for the given environment's policies and classification.

IRAP assessment details also need to be included, such as the key dates of the assessment, the ISM version being used, any previous certification issues or ongoing recommendations, and the maximum classification that the environment will be assessed against.

Assessment Scope

Identify the specific systems within the environment that will be under review. Detail any assumptions or constraints.

Documents Reviewed

List all the necessary documents required for the assessment.

Risk Assessment

Provide a copy of the executive summary and overview of findings from the associated risk assessment documentation. Outline any mitigation strategies for any residual risks.

Detailed Findings

The detailed findings should contain all the comprehensive results of the IRAP Assessment, including any notes or documentation produced during the process. Assessments should follow the most recent version of the ISM, with all controls clearly defined as being out of scope, compliant, or non-compliant with relevant justifications. Any observations, recommendations or comments should be noted alongside each control as appropriate.