Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

IRAP Quality Assurance Framework

Australian Signals Directorate

Infosec Registered Assessors Program (IRAP)

irap

Table of contents

Introduction

This document provides a systematic process for evaluating and improving the quality of Infosec Registered Assessors Program (IRAP) assessments performed by IRAP Assessors.

ASD endorses suitably qualified security professionals as IRAP Assessors. The IRAP Quality Assurance Framework is an important mechanism for ensuring the high standards expected of an IRAP Assessor, are maintained.

The IRAP Quality Assurance Framework also facilitates the identification of opportunities for improvement in the IRAP training course, ongoing IRAP Assessor development, and the program's administration. The implementation of the IRAP Quality Assurance Framework provides additional assurance to ASD that the program reflects ASD's high standard for technical advice and guidance. As per the IRAP Policy and Procedures, all IRAP assessments may be subject to a quality assurance appraisal by ASD.

Background

IRAP is one of ASD's longest running and most public facing programs. This program supports the cyber resilience of the Australian Government by enabling objective security assessments of ICT systems to and for Commonwealth entities, and to private sector entities contracting with the Commonwealth.

The demand for IRAP assessments continues to grow as the emphasis on cyber security across Government and industry increases. There is a need to ensure that IRAP assessments remain of a high standard and consistency, and Assessor conduct is professional and reputable.

ASD sets the standards of the IRAP program and has an obligation to pursue corrective actions related to IRAP assessments and IRAP Assessors, as necessary.

The IRAP Quality Assurance Framework provides IRAP Assessors with guidance on the standard and level of detail expected of them in the conduct of an assessment. It provides ASD with a mechanism for assuring that IRAP Assessors conduct high quality assessments and demonstrate expert knowledge. ASD will communicate any need for adjustment to an Assessor's assessment approach through a Corrective Action Plan.

Supporting documents

This framework is supported by the following ASD publications and guidance:

- IRAP Policy and Procedures;
- IRAP Common Assessment Framework;
- IRAP Assessment Report Template; and
- IRAP Branding and Marketing Guidelines.

IRAP Quality Assurance Appraisals

The IRAP Quality Assurance Framework includes an appraisal of the Assessor's ability to meet the assessment requirements that are outlined in the IRAP Common Assessment Framework. Each of these assessment requirements have been aligned to a technical or non-technical standard to form the IRAP Quality Standards, outlined in Annex A.

During an IRAP Quality Assurance Appraisal, both technical and non-technical Quality Standards will be reviewed. Where deficiencies or risks are determined to be associated with the IRAP engagement or report, corrective recommendations will be provided to the Assessor via a Corrective Action Plan.

Quality Standards terminology

Quality Assurance Reviewers will use the following terminology when reviewing whether an IRAP Assessor has met the IRAP Quality Standards:

- **At Standard (AS)** – The IRAP Assessor has met the Quality Standards specified by ASD.
- **Not At Standard (NAS)** – The IRAP Assessor has NOT yet met the Quality Standards specified by ASD.
- **No Visibility (NV)** – There was insufficient evidence to assess the IRAP Assessor against the Quality Standards outlined by ASD. This could be due to the report being incomplete or in draft, which resulted in the Quality Assurance Reviewer not being able to determine a sufficient outcome.
- **Not Applicable (NA)** – An assessment requirement or Quality Standard was deemed out of scope or not applicable to the IRAP assessment or the Quality Assurance Appraisal process.

Quality rating terminology

In addition to the Quality Standards terminology that a Quality Assurance Reviewer will use in their appraisal, they will also rate the level of any deficiencies against assessment requirements. The ratings used are a reflection of the potential impact on a decision-makers ability to appropriately authorise a system, or to the integrity of the Program, as a result of Quality Standards not being met. Examples of quality ratings used in assessing against IRAP Quality Standards is presented in Annex B.

Quality rating terminology includes:

Severe – The Quality Assurance Reviewer has determined that immediate remediation by the IRAP Assessor is required - adjusting the existing IRAP assessment report or completing an Addendum. A 'Severe' rating may be provided where the deficiencies misrepresent and/or could affect an authorising officer in making a proper risk-based decision, or where an IRAP Assessor has failed to establish assessment independence by lodging a conflict of interest declaration.

Moderate – The Quality Assurance Reviewer has determined that the IRAP Assessor should implement the remediation activities into the existing report if it is reasonable, otherwise remediation activities must be addressed in subsequent assessments. ASD IRAP must be advised of the corrections taken.

Minor – The Quality Assurance Reviewer has determined that remediation activities for the IRAP Assessor are not urgent and can occur within subsequent IRAP assessments. A 'Minor' rating is where minimal discrepancies or deficiencies were present, but are not material to the risk-based decision making of an authorising officer.

Non-technical quality assurance appraisal

A Non-Technical Quality Assurance Appraisal assesses the materials produced, adherence to program governance, and professionalism of an Assessor during an engagement, against the non-technical IRAP Quality Standards. This initial step determines whether the IRAP Assessor has meet the baseline standards expected by ASD. A Non-Technical Quality Assurance Appraisal may identify the need to conduct a Technical Quality Assurance Appraisal.

If required, the findings from the Non-Technical Quality Assurance Appraisal will inform recommendations in a Corrective Action Plan.

Examples of some of the non-technical standards include:

- Terminology used throughout the IRAP assessment report is consistent with ASD's published guidance;
- the IRAP assessment report template is utilised with relevant supplementary sections added, where appropriate;
- the IRAP Assessor does not place a rating on the risk of the system or its operation;
- a conflict of interest declaration is submitted prior to the commencement of the IRAP assessment; and
- the IRAP assessment report does not use language to suggest or recommend any endorsement, certification, authorisation or accreditation of the system.

Technical quality assurance appraisal

The Technical Quality Assurance Appraisal will include an in-depth analysis of IRAP assessment artefacts. The technical IRAP Quality Standards, specified in Annex A, will be used to inform this process.

ASD IRAP may initiate a Technical Quality Assurance Appraisal based on the following criteria:

- An IRAP assessment of a high-risk system is initiated and requires ASD oversight;
- reviewing a new Assessor's first IRAP report;
- as part of ongoing monitoring from previous Corrective Action Plans;
- upon receiving feedback from an assessed entity;
- a concern has been raised by the general community;
- issues were identified during a non-technical quality appraisal;

- at the request of internal ASD stakeholders; or
- at the discretion of ASD IRAP as part of general program governance.

Depending on the severity of the ‘not at standard’ Quality Standards, the findings from the Technical Quality Assurance Appraisal may inform recommendations in a Corrective Action Plan, in which case, a determination will be made on the remediation’s and timeframes required of the Assessor.

Corrective Action Plan

The Corrective Action Plan will define the actions or adjustments that an IRAP Assessor is required to complete to meet the Quality Standards specified in Annex A. The IRAP Assessor is required to respond by providing a remediation plan with appropriate deadlines. ASD IRAP will make a determination on the suitability of remediation activities and the timeframes suggested by the IRAP Assessor. ASD IRAP will also outline any monitoring period that will be put in place to gain assurance that the IRAP Assessor has been able to improve upon and maintain expected Quality Standards. This monitoring period can be in the form of a set period of time and/or a set number of future assessments completed by the Assessor.

The Corrective Action Plan supports ASD IRAP in identifying improvement opportunities within the IRAP Assessor cohort. Common issues and trends seen in Corrective Action Plans will inform future program enhancements, or development of IRAP guidance, publications or training.

Appealing corrective actions

IRAP Assessors that wish to appeal the findings presented within a Corrective Action Plan must respond in writing to ASD.IRAP@defence.gov.au within 10 business days of receiving it. To appeal the findings, the IRAP Assessor must provide a business case as to why they disagree with any specific finding and provide relevant evidence to support their claim.

Once ASD IRAP has received a formal appeal in writing with a business case, a review will be conducted.

Outcomes from the appeal will be communicated to the IRAP Assessor within 30 days.

Assessor participation and compliance with the IRAP Quality Assurance Appraisal process is a condition of ASD endorsement.

IRAP Quality Assurance Management

Roles and responsibilities

ASD IRAP

ASD IRAP maintain, coordinate and oversee IRAP Quality Assurance processes. They approve all Corrective Action Plans developed for IRAP Assessors who have not yet met Quality Standards, as well as approve and manage any revocation or change to an IRAP Assessor's status. In addition, ASD IRAP approves the timeframes and remediation activities recommended by the IRAP Quality Assurance Reviewers.

Quality Assurance Reviewer

The Quality Assurance Reviewer assess IRAP assessments based on the assessment requirements as defined by ASD IRAP in the IRAP Common Assessment Framework. Assessment requirements are categorised into either non-technical or technical Quality Standards:

- **Non-technical Standards:** Ensuring appropriate use of terminology and adherence to program governance and reporting standards (as outlined in the 'Supporting Documents' listed in this Framework). This includes identifying instances of incorrect language, such as assigning risk ratings or mischaracterising the IRAP assessment as certification or accreditation.

- **Technical Standards:** Evaluating the Assessor's understanding and application of the Information Security Manual (ISM) controls, and verifying the accuracy and detail of technical assessments.

ASD IRAP may delegate Quality Assurance Reviewer responsibilities to suitably experienced ASD personnel, when appropriate. ASD personnel assessing against technical Standards must be an active IRAP Assessor, unless explicitly authorised by ASD IRAP.

Technical or Non-Technical Reviewers may recommend changes to an IRAP Assessor's status, based on the outcome of an appraisal.

IRAP Assessors

IRAP Assessors are required to meet the Quality Standards specified in Annex A. An IRAP Assessor must respond to ASD IRAP's requests for IRAP assessment artefacts within the requested timeframe. The Assessor must provide, at a minimum, the IRAP assessment report and security controls matrix for the assessment.

IRAP Assessors must complete and return any Corrective Action Plan received as part of a Quality Assurance Appraisal, within 10 business days. IRAP Assessors must complete the specified remediation activities within the timeframe outlined in the Corrective Action Plan. An IRAP Assessor must provide ASD IRAP with a business case, and obtain ASD's agreement on a new delivery timeframe, if they are unable to complete the remediation activities within the specified period.

IRAP Assessors that are in the monitoring period of a Corrective Action Plan must advise ASD of any other concurrent assessment activities. This is in addition to their normal conflict of interest declaration requirements.

Breaches of program governance or failure to participate and comply with the IRAP Quality Assurance Appraisal process, may result in a change in Assessor status or revocation of ASD endorsement/membership from the program.

Customers and consumers

Customers and consumers having direct interactions with IRAP Assessors and their work product, are encouraged to provide ASD with feedback relating to the IRAP Assessor's performance, conduct, or the quality of the IRAP assessment.

Customers and consumers should send all feedback to the IRAP mailbox at asd.irap@defence.gov.au.

Customers and consumers should be aware that IRAP Assessors are required to provide IRAP assessments to ASD for quality assurance activities upon request, and must not force an Assessor to sign any non-disclosure agreement or similar, to inhibit this process.

IRAP Assessor status

ASD reserves the right to change an IRAP Assessor’s status to any of the following:

- **Active** – The IRAP Assessor has produced IRAP reports at an acceptable standard, and has adhered to the program’s Policy and Procedures. The IRAP Assessor is able to conduct IRAP Assessments. Active IRAP Assessors may be required to provide IRAP assessment artefacts to ASD IRAP for general quality assurance purposes.
- **Assessor of interest** – The Assessor is new to the program, or the Assessor has produced IRAP reports that are not yet at standard when reviewed against ASD’s IRAP Quality Standards (Annex A). ASD IRAP will automatically designate new Assessors to ‘Assessor of interest’ status to ensure we provide appropriate support and feedback on their first IRAP assessment.

  Minor or moderate issues that may lead to the ‘Assessor of interest’ status for ongoing Assessors include, incomplete testing, poor document quality or inaccurate reporting.

  - As an Assessor of interest the IRAP Assessor is still able to conduct IRAP assessments and designate themselves as an IRAP Assessor, however for a designated period, they are required to submit all IRAP assessment material to ASD IRAP for monitoring and review.
  - An Assessor of interest as a result of a Corrective Action Plan must resolve any rectification activities in the timeframe specified. They must also demonstrate continuous improvement and quality to ASD.
- **Revoked** – The IRAP Assessor has repeatedly produced IRAP reports with severe quality deficiencies and/or there are substantial governance breaches or professionalism concerns. The IRAP Assessor may have failed to complete or effectively remediate Corrective Action Plans and/or meet program policy requirements. The IRAP Assessor has been afforded procedural fairness (including reasonable opportunity to respond to claims / evidence), but the matter is unresolved and is deemed an unacceptable risk. A letter from ASD will be sent to the IRAP

Assessor notifying of their decision to discontinue endorsement and the change in IRAP status.

- An Assessor who is revoked from the IRAP program is ineligible for future ASD IRAP endorsement.

IRAP Quality Assurance Management Cycle

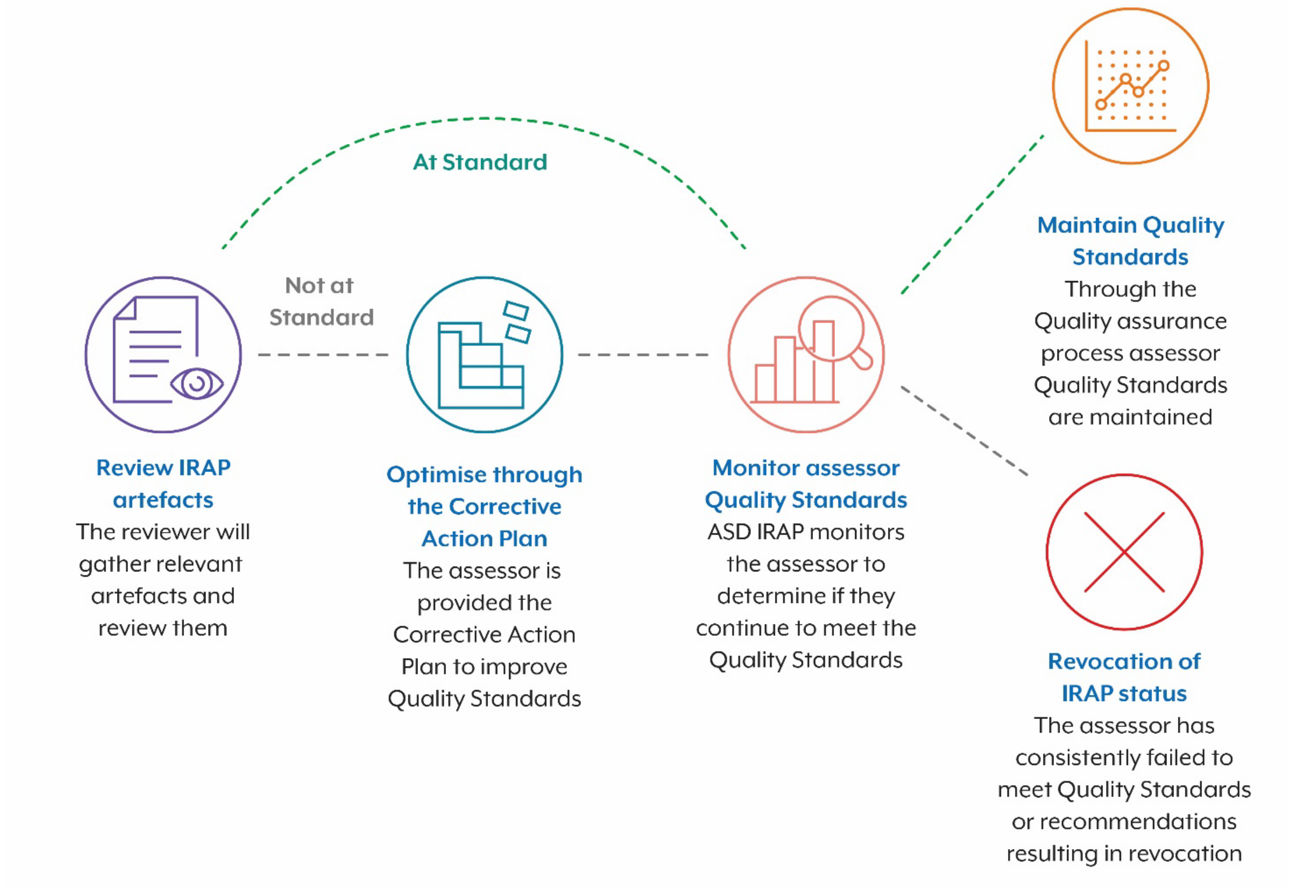
At Standard
Not at Standard
Review IRAP artefacts
The reviewer will gather relevant artefacts and review them
Optimise through the Corrective Action Plan
The assessor is provided the Corrective Action Plan to improve Quality Standards
Monitor assessor Quality Standards
ASD IRAP monitors the assessor to determine if they continue to meet the Quality Standards
Maintain Quality Standards
Through the Quality assurance process assessor Quality Standards are maintained
Revocation of IRAP status
The assessor has consistently failed to meet Quality Standards or recommendations resulting in revocation

Figure 1: IRAP Quality Assurance Management Cycle

Review

The Quality Assurance Reviewer evaluates the supplied IRAP artefacts against the Quality Standards specified in Annex A and relevant IRAP publications (listed under Supporting Documents). The reviewer will assess the quality of the report artefacts and the terminology used throughout.

An IRAP Assessor identified as having no, or only minor deficiencies in their assessment through the review process, will receive feedback from ASD IRAP on assessment strengths and weaknesses. Assessors will be expected to maintain IRAP Quality Standards.

Optimise

An IRAP Assessor identified as having moderate or severe deficiencies in their assessment through the review process will be required to conduct remediation activities. Areas requiring remediation will be provided in the form of a Corrective Action Plan. The IRAP Assessor will then be required to review the identified deficiencies, work with ASD IRAP to agree on corrective actions and implement the remediation actions specified.

ASD IRAP will provide the IRAP Assessor with detailed information on Quality Standard expectations and maintain communications with Assessors undertaking a Corrective Action Plan, so they are clear on the remediation activities required.

Monitor

The Assessor will be moved to an 'Assessor of interest' status for the duration of Corrective Action Plan remediation, or a period specified by ASD IRAP. The Corrective Action Plan will outline the monitoring period for the Assessor.

The Assessor will be given reasonable opportunity to demonstrate they have made adjustments to their assessment approach or report format, to meet IRAP Quality Standards.

The Assessor must provide ASD IRAP with a copy of all assessment reports from IRAP assessments conducted while they are at 'Assessor of interest' status. ASD will review subsequent reports completed by the IRAP Assessor to determine whether Quality Standards have improved and are being maintained.

Maintain

If the IRAP Assessor successfully meets the required Quality Standards during the monitoring period specified in the Corrective Action Plan, they will revert to 'Active' status and be required to participate in general quality assurance governance processes.

IRAP Assessors are required to complete the Conflict of Interest declaration form, as normal.

Revoke

ASD reserves the right to revoke endorsement of an IRAP Assessor that repeatedly has severe deficiencies in their assessments and fails to lift to meet the Quality Standards, despite feedback and instruction from ASD. This includes a failure to comply with IRAP Policy and Procedures or ignoring/refusal to participate in the IRAP Quality Assurance process, as well as a demonstrated lack in technical proficiency expected of an IRAP Assessor.

Annex A: IRAP Quality Standards

Overview of Quality Standards

Quality Standard	**Note:** *The details below are representative descriptions of IRAP's Quality Standards. ASD maintains the right to update and implement Quality Standards, as needed.*
Report artefacts quality and terminology	• The output of an IRAP assessment includes artefacts, terminology and language defined by ASD. • The flow of the IRAP assessment report aligns to the structure and outline of the IRAP Assessment Report template and includes supplementary sections, as necessary, to provide a thorough assessment.
Assessment process and frameworks	• The IRAP assessment follows the processes and stages outlined in the IRAP Common Assessment Framework and demonstrates consideration of other related Australian Government frameworks and policies that are required to ensure a holistic approach to security.
Evidence gathering	• The evidence made available/gathered during an assessment is of appropriate quality (as per the IRAP Common Assessment Framework). • Where the findings presented in an IRAP assessment cannot be substantiated by an appropriate level of evidence, the report clearly articulates the constraints and limitations, and specifies which controls are affected. • The sample size of testing is proportionate to the system size. • The IRAP Assessor uses various assessment objects and methods to enable sufficient depth and coverage.
Coverage	• The IRAP assessment has full coverage of the assessment scope and boundary; ensuring that it is appropriate and that the assessment does not miss components that could affect an authorising officer's decision to make an informed risk-based decision. • The IRAP Assessor understands the assessment boundary clearly and articulates it in the report. • The rationale for security controls, systems, services and architecture that are out of scope, is clearly articulated.
Objectivity	• The IRAP Assessor presents evidence-based findings substantiated with the highest quality of evidence available.

Quality Standard	**Note***: The details below are representative descriptions of IRAP's Quality Standards. ASD maintains the right to update and implement Quality Standards, as needed.*
	• The Assessor does not use language that would consider the assessment as a compliance, certification or accreditation report to authorise a system. • The IRAP Assessor does not 'rate' risks and subvert an authorising officer's ability to make risk-based decisions.
Technical accuracy and completeness	• The IRAP assessment considers the various technologies, systems and services in place and can clearly explain and articulate its use, purpose and implementation to technical and non-technical stakeholders. • References to control implementation that are meant to meet an ISM control, properly satisfy the intent of that control. • The IRAP Assessor understands how to test technical systems to provide the greatest assurance.
Assessment Integrity	• The IRAP Assessor acts as an independent Assessor and must report anything that may affect this independence. • The IRAP Assessor fulfils their administrative requirements, such as timely submission and maintenance of the Conflict of Interest declaration form and notifications to relevant stakeholders.

Annex B: Example IRAP Quality Ratings

Example of quality ratings used in assessing against IRAP Quality Standards

Quality Standard	Rating guideline **Note:** *The details below are representative examples of IRAP's Quality Standards and are not all-inclusive of assessment requirements.*
Report artefacts and terminology	**Severe** The IRAP Assessor assessed a control as 'Effective' when the provided evidence and statement leads to the control being 'Ineffective'
	Moderate The IRAP Assessor failed to specify that there were limitations and constraints during the assessment, which resulted in not being able to gather highest level of evidence possible.
	Minor The IRAP Assessment report was reviewed by the stakeholder and security professional but the Assessor failed to specify this in the report.
Assessment process and frameworks	**Severe** The IRAP Assessor failed to utilise the IRAP Common Assessment Framework and the Information Security Manual during the IRAP assessment.
	Moderate The IRAP Assessor failed to conduct a delta assessment utilising the latest version of the Information Security Manual.
	Minor The IRAP Assessor failed to articulate the activities conducted during each phase of an IRAP assessment within the report.
Evidence gathering	**Severe** The IRAP Assessor only gathered poor quality evidence throughout the assessment to support the control status.
	Moderate The IRAP Assessor did not gather an appropriate sample size of evidence to support the control status.
	Minor The IRAP Assessor miscategorised the evidence supplied.
Coverage	**Severe** The IRAP Assessor omitted systems, services or technologies within the assessment boundary.

Quality Standard	Rating guideline **Note***: The details below are representative examples of IRAP's Quality Standards and are not all-inclusive of assessment requirements.*
	Moderate The IRAP Assessor outlined weakness around data sovereignty but failed to outline them within the key strengths and weaknesses section.
	Minor The image of the assessment or the boundary is not sufficiently clear or is blurry within the IRAP assessment report.
Objectivity	**Severe** The IRAP Assessor made assumptions with no evidence to support the claim.
	Moderate The IRAP Assessor has made assumptions based on the evidence provided, instead of presenting factual findings.
	Minor The IRAP Assessor marked a control 'Not implemented' without specifying technical or business constraints when the control should instead be marked as 'Ineffective'.
Technical accuracy and completeness	**Severe** The IRAP Assessor has assessed an alternate control as being 'Effective' when the provided statement or evidence does not appropriately meet or exceed the intent of the ISM control, making it 'Ineffective'.
	Moderate The technical accuracy of information detailed within the report is ambiguous or confusing.
	Minor The IRAP Assessor utilised overly technical jargon to explain certain aspects of the system or service being assessed.
Assessment integrity	**Severe** The IRAP Assessor fails to submit a conflict of interest declaration form, impacting program assurance of assessment independence.
	Moderate The primary IRAP Assessor failed to add any secondary assessors to the IRAP assessment record to enable all conflicts of interest to be declared.
	Minor The IRAP Assessor did not clearly articulate the nature of the conflict of interest within the IRAP assessment report.

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

Australian Government
Australian Signals Directorate

ASD
AUSTRALIAN
SIGNALS
DIRECTORATE

ACSC
Australian
Cyber Security
Centre