

IRAP Assessor Agreement

For participation in the ASD Infosec Registered Assessors Program (IRAP)

Last updated: June 2026

Agreement Details

Date:

Assessor:

Name:

Address:

Phone number:

Email:

1. Background

- 1.1 ASD manages and administers IRAP with an aim to enhance the security of broader industry and Australian Government systems and data.
- 1.2 Once individuals have successfully completed the IRAP training course, they receive a formal endorsement by ASD to provide independent, high quality information security assessment services to both public and private organisations.
- 1.3 Without ASD's endorsement, an individual will not be considered an IRAP Assessor and will not be able to undertake IRAP assessments.
- 1.4 The Assessor wishes to participate in IRAP as an IRAP Assessor.
- 1.5 ASD is willing to accept the Assessor into IRAP as an IRAP Assessor on the condition that the Assessor acts in accordance with this Agreement and any other document incorporated herein by reference..

2. Definitions

In this Agreement:

ACSC Partner Portal means the online platform provided to IRAP Assessors and used by ASD to share relevant cyber security advice and information.

Agreement means the agreement set out in this document.

ASD means the Commonwealth of Australia as represented by the Australian Signals Directorate (ABN 22 323 254 583).

Agreement Commencement Date means the date on which this document is signed by the Assessor.

Conflict of interest has the same meaning as specified in section 4.4 of the *IRAP Policy & Procedures*.

IRAP means the InfoSec Registered Assessors Program.

IRAP Assessor means an individual who has been endorsed by ASD under IRAP.

IRAP Team means the individuals within ASD who are responsible for overseeing the management and administration of IRAP.

3. Agreement and Term

- 3.1 The parties agree that the promises made to each other in this Agreement constitute good and valuable consideration.

3.2 This Agreement takes effect from the Agreement Commencement Date and continues for the period of time that the Assessor remains endorsed by ASD or superseded by a new IRAP Assessor Agreement following the IRAP renewal process.

3.3 The following obligations will survive the termination or expiry of this Agreement:

the Assessor's obligations of confidentiality arising under the *IRAP Policy & Procedures*, the *IRAP Confidentiality Deed* and *IRAP ACSC Partner Portal Deed*

3.4 The following obligations will survive the termination or expiry of this Agreement:

3.4.1 the Assessor's obligations of confidentiality arising under the *IRAP Policy & Procedures*, the *IRAP Confidentiality Deed* and *IRAP ACSC Partner Portal Deed*;

4. Conditions for ASD endorsement in IRAP

4.1 In order to obtain and maintain ASD's accreditation as an endorsed IRAP Assessor, the Assessor agrees to comply with the endorsement requirements set out in the *IRAP Policy & Procedures*, including, but not limited to:

4.1.1 Completing and complying with the *IRAP Confidentiality Deed* and *IRAP ACSC Partner Portal Deed*.

4.1.2 Demonstrating behaviours aligned to the IRAP Code of Conduct and Values.

4.1.3 Ensuring that all conflict of interest declarations are submitted to ASD on time.

4.1.4 Abiding by applicable Australian laws and the IRAP Code of Conduct and Values.

4.1.5 Holding an active NV1 or higher security clearance.

5. General agreement

5.1 The Assessor acknowledges and agrees that a breach or breaches of the *IRAP Policy & Procedures* may result in the suspension or revocation of their

membership as set out in that document. Without limitation, the actions by an IRAP Assessor that may constitute the grounds for the suspension or revocation of membership include:

5.1.1 a breach of IRAP policy or IRAP Assessor Agreement

5.1.2 a failure to comply with ongoing membership requirements

5.1.3 a failure to comply with the IRAP quality assurance process

5.1.4 unprofessional behaviour towards ASD, the IRAP program, the IRAP Assessor community or external parties

5.1.5 behaviour which gives rise to a concern for national security

5.1.6 a failure to maintain an NV1 minimum security clearance

5.1.7 a failure to declare or manage a conflict of interest or integrity concern

5.1.8 misrepresentation of ASD or the IRAP brand

5.1.9 any behaviour inconsistent with the IRAP Code of Conduct

5.2 The Assessor acknowledges and agrees that any breach or breaches of the *IRAP Confidentiality Deed* and *IRAP ACSC Partner Portal Deed* may result in the suspension or revocation of their IRAP membership.

5.3 The Assessor acknowledges that if revocation occurs, the Assessor will lose their membership as an IRAP Assessor and, as a result, will no longer be able to undertake or complete IRAP assessments.

5.4 The Assessor acknowledges that the obligations outlined in the *IRAP Confidentiality Deed* and *IRAP ACSC Partner Portal Deed* for access to the ACSC Partner Portal will continue to apply to them after ceasing their role as an IRAP Assessor.

5.5 The Assessor acknowledges that ASD reserves the right to make changes to IRAP at any time, including the administration of the program and the introduction of new reasonable and necessary membership requirements to ensure the quality, effectiveness and integrity of the program.

5.6 The Assessor

5.6.1 agrees that ASD and its officers, employees and agents will not be

liable for any financial, reputational or vocational impact resulting from the revocation of IRAP endorsement or making changes to IRAP; and

5.6.2 releases ASD and its officers, employees and agents from all claims whatsoever arising out or connected with a decision to revoke an IRAP endorsement or making changes to IRAP.

X

Print name:

Date:



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre

IRAP policy and procedures

Australian Signals Directorate

InfoSec Registered Assessors Program

First published: December 2020

Last updated: June 2026

Table of contents

1. InfoSec Registered Assessors Program.....	1
1.1 About.....	1
1.2 Purpose	1
1.3 Rationale	1
1.4 Intended audience & definitions	1
1.5 Supporting documents.....	2
1.6 IRAP code of conduct and values.....	3
2. IRAP: Training course	5
2.1 Enrolment prerequisites	5
2.2 Training course content and assessments.....	5
3. IRAP: Membership	7
3.1 Membership prerequisites.....	7
3.2 Security clearance	8
3.3 Endorsement requirements for an IRAP assessor	8
3.4 Denial of endorsement	9
3.5 Membership maintenance.....	10
4. IRAP: Assessors	14
4.1 IRAP assessment reporting	14
4.2 Supporting information security guidance	14
4.3 Confidentiality.....	15
4.4 Conflict of interest.....	15
4.5 Quality assurance	17
4.6 Revocation of IRAP endorsement	18
5. IRAP: Consumers	20
5.1 IRAP assessment customers & consumers	20
5.2 Applicable policy	20

6. IRAP: Brand and marketing	21
6.1 IRAP assessment customers & consumers	21
6.2 IRAP assessors	21
7. IRAP: Training providers	22
7.1 About.....	22
8. ASD	23
8.1 Responsibilities.....	23
8.2 Conflict resolution process.....	23
9. Appendix.....	25
9.1 Related legislation, directives, policies and procedures.....	25
9.2 Getting help.....	25
9.3 Version history	25

1. InfoSec Registered Assessors Program

1.1 About

- 1.1.1 The InfoSec Registered Assessors Program (IRAP) is Australia's premier cyber security assurance program - providing high-quality information security assessment services to government and industry under the Australian Signals Directorate (ASD).
- 1.1.2 ASD, through IRAP, endorses suitably qualified cyber security professionals to provide independent security assessment services, with the aim of securing the information systems and data of Commonwealth Government and related industry. IRAP assessments can only be conducted by ASD-endorsed IRAP assessors.
- 1.1.3 The *Protective Security Policy Framework* (PSPF) outlines the requirements and responsibilities for IRAP assessors to conduct independent security assessments. Table 21 of the PSPF details the security assessments required for technology systems. Cloud, ICT outsourced service providers and gateway systems (up to SECRET) *must* be assessed by ASD-endorsed IRAP assessors.

1.2 Purpose

- 1.2.1 The *IRAP policy and procedures* outlines the conditions for IRAP membership, the requirements to maintain ASD endorsement, the responsibilities of the ASD IRAP team, and the conditions under which membership may be denied or revoked.

1.3 Rationale

- 1.3.1 Cyber security is a top national security priority for the Australian Government. Cyber security threats on government, critical infrastructure and other information systems are a real threat to Australia's national security and interests.
- 1.3.2 IRAP provides independent security assessment services to ensure that security strengths and weaknesses are appropriately identified and communicated to the authorising officer, in order to support their decision to authorise the operation of a system. An IRAP assessment includes determining the effectiveness of relevant security controls outlined within the Information Security Manual (ISM).

1.4 Intended audience & definitions

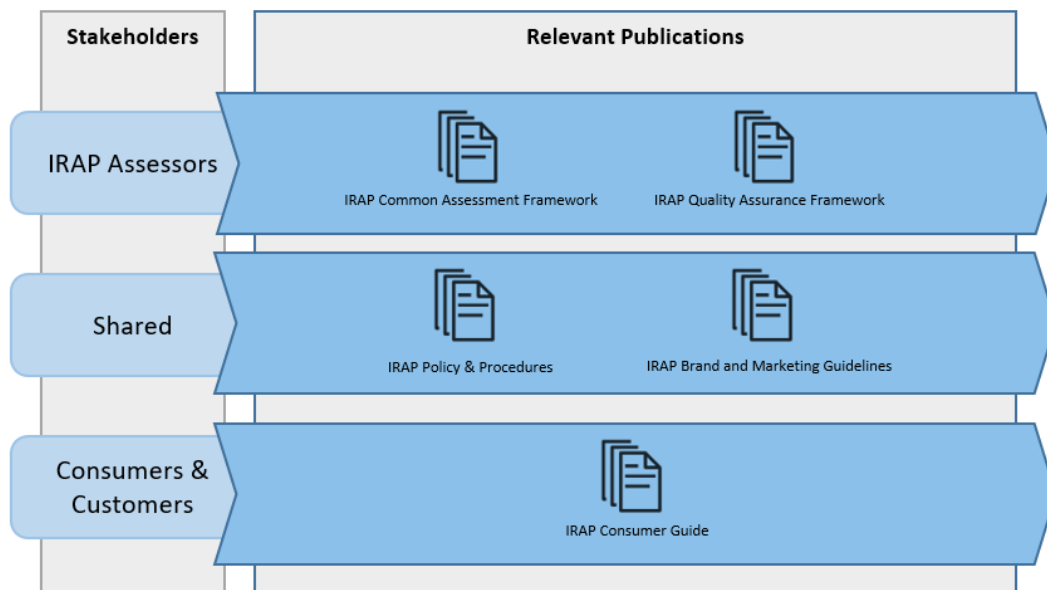
- 1.4.1 This information is intended for the following stakeholders:
 - (a) **ASD IRAP team** – The team in ASD responsible for the management, governance and strategic delivery of the IRAP (including the provision of advice and guidance to the IRAP community).
 - (b) **IRAP applicant** – A cyber security professional that is applying, or has applied for endorsement by ASD, to become an IRAP assessor.
 - (c) **IRAP course participant** – An individual who is seeking to enrol, or who has enrolled in the IRAP training course.

- (d) **IRAP assessor** – A cyber security professional that has received ASD endorsement to conduct an independent security assessment service, hereafter referred to as an IRAP assessment. IRAP assessors are not employees or contractors of ASD.
- (e) **IRAP consumer** – A person that is using an IRAP assessment as part of an information security authorisation package.
- (f) **IRAP customer** – Organisations who are engaging, or looking to engage an IRAP assessor to conduct an IRAP assessment, and that may advertise or promote the completion of an IRAP assessment on their products or services.
- (g) **IRAP training provider** – An organisation engaged by ASD through a formal tender process, to deliver the ASD-developed IRAP training course.

1.5 Supporting documents

1.5.1 The following publications have been developed to supplement and provide additional clarity to, this document. IRAP applicants, assessors, customers, and consumers should read these publications where further clarity is required.

- (a) **IRAP policy and procedures:** The *IRAP policy and procedures* (this document) outlines the core requirements that all stakeholders included in the intended audience must follow.
- (b) **IRAP brand and marketing guidelines:** The *IRAP brand and marketing guidelines* set out the requirements for IRAP assessors, consumers, and customers on the appropriate marketing terminology and usage of the IRAP brand.
- (c) **IRAP Quality Assurance Framework:** The *IRAP Quality Assurance Framework* sets out the quality standards that IRAP assessors are required to meet. IRAP assessors will be assessed against this framework during quality assurance appraisal.
- (d) **IRAP Common Assessment Framework:** The *IRAP Common Assessment Framework* provides IRAP assessors with a standardised methodology for conducting IRAP assessments and assessing the implementation of security controls, regardless of the system type (On-premise, cloud or gateways). Additionally, it outlines Assessment Requirements (AR) that align with the quality standards outlined in the *IRAP Quality Assurance Framework*.
- (e) **IRAP Consumer Guide:** The *IRAP Consumer Guide* assists IRAP consumers and customers in preparing for and ensuring a streamlined and efficient, IRAP assessment.



1.6 IRAP code of conduct and values

- 1.6.1 IRAP applicants and IRAP assessors have a responsibility to uphold the elements of the Code of Conduct (Code) outlined in Section 1.6.4, and adhere to and model the values outlined in Section 1.6.5. If further clarity is required, IRAP applicants and IRAP assessors must consult the ASD IRAP team and/or the supporting documents listed in Section 1.5.1.
- 1.6.2 IRAP assessors provide an independent assessment of an information system’s security controls, and evaluate compliance with the ISM and PSPF to best assist and help organisations identify risks and strengthen security. The ASD IRAP team, Australian Government and public therefore expect high standards of performance, ethics and personal behaviour from IRAP applicants and IRAP assessors.
- 1.6.3 The IRAP Code of Conduct and IRAP Values address these requirements and public expectations while also supporting the specific needs of the ASD and ASD IRAP team - they set a framework of enduring principles of good public administration.

1.6.4 IRAP code of conduct

- (a) An IRAP applicant or IRAP assessor:
- i. must behave honestly and with integrity in connection with the IRAP.
 - ii. must act with care and diligence in connection with the IRAP.
 - iii. when acting in connection with the IRAP, must treat everyone with respect and courtesy, and without harassment.
 - iv. when acting in connection with the IRAP, must comply with all applicable Australian laws and policies. For this purpose Australian law means an Act, or any instrument made under an Act, or any law of a State or Territory, including any instrument made under such a law.
 - v. must comply with any lawful and reasonable direction given by the ASD IRAP team or by someone in ASD who has authority to give the direction.

- vi. must take reasonable steps to avoid any conflict of interest (real, potential or apparent) in connection with the IRAP, and disclose details of any material personal interest in connection with the IRAP or an IRAP assessment.
- vii. must use IRAP resources in a proper manner and for a proper purpose.
- viii. must not improperly use inside information or their duties, status, power or authority to gain, or seek to gain, a benefit or an advantage for themselves or any other person, or to cause, or seek to cause, detriment to the ASD or any other person.
- ix. must at all times behave in a way that upholds the IRAP Values, and the integrity and good reputation of ASD.
- x. must comply with any other requirement outlined in this document.

1.6.5 IRAP values

- (a) An IRAP applicant or IRAP assessor is:
 - i. **accountable.** IRAP applicants and IRAP assessors are open and accountable to the Australian community and ASD under applicable laws and within the framework of this document.
 - ii. **committed to service.** IRAP applicants and IRAP assessors are professional, objective, innovative and efficient, and work to achieve the best results for the Australian community, Government and national interest.
 - iii. **ethical.** IRAP applicants and IRAP assessors demonstrate leadership, are trustworthy, and act with integrity, in all that they do.
 - iv. **impartial.** IRAP assessors will provide IRAP customers with advice that is honest, timely and based on the best available evidence.
 - v. **respectful.** IRAP applicants and IRAP assessors respect all people, including their rights and their heritage.

2. IRAP: Training course

2.1 Enrolment prerequisites

- 2.1.1 To be eligible for enrolment into the IRAP training course, and to undertake the training and assessments of the IRAP training course, the ASD-recognised training provider must be satisfied the individual meets the requirements outlined in Section 2.1.3, 2.1.4 and 2.1.5.
- 2.1.2 An individual who is not eligible for enrolment into the IRAP training course, or who is not able to undertake the training assessments of the IRAP training course, will not be eligible for endorsement as an IRAP assessor.

2.1.3 Citizenship

- (a) An individual must be an Australian citizen.

2.1.4 Qualifications

- (a) An individual must hold at least one qualification from **both** Category A and B.
- i. Recognised Category A qualifications include:
 - (a) Certified Information Systems Security Professional (CISSP);
 - (b) Certified Information Security Manager (CISM); and
 - (c) GIAC Security Leader Certification (GSLC).
 - ii. Recognised Category B qualifications include:
 - (a) Certified Information Systems Auditor (CISA);
 - (b) Payment Card Industry Qualified Security Assessor (PCI QSA); and
 - (c) Certified in Risk and Information Systems Control (CRISC).

2.1.5 Demonstrated ICT experience

- (a) An individual must provide evidence to substantiate at minimum five (5) years of experience in information security roles utilising relevant Australian security frameworks such as the ISM and PSPF and supporting publications. This experience must include examples where the individual is currently, or was recently, responsible for:
- i. implementing or assessing security controls and principles as per the ISM; and
 - ii. using supporting frameworks and publications such as the PSPF and the Strategies to Mitigate Cyber Security Incidents.

2.2 Training course content and assessments

- 2.2.1 The IRAP training course is facilitated through ASD-recognised training providers and is delivered in face-to-face or virtual modes. An individual is required to complete the IRAP training course and pass all assessment components in order to be eligible for endorsement as an IRAP assessor.
- 2.2.2 The IRAP training course is based on real-life assessment scenarios in a lab-based environment, with an assumed knowledge approach to the ISM and PSPF. The pre-requisites outlined in Section 2.1 are required to enrol in the IRAP training course. Individuals will be vetted by the training provider to ensure they meet the entry requirements, including verification of qualifications and experience.

- 2.2.3 There are three (3) assessment components required to successfully pass the IRAP training course. All three assessment components must be passed to successfully complete the IRAP training course. This includes the:
- (a) IRAP exam, which consists of multiple-choice and short answer questions;
 - (b) daily learning reflections; and
 - (c) the completion of a condensed IRAP report assessment.
- 2.2.4 The pass mark for the exam is 80%. The daily reflections and IRAP report assessment components must meet a minimum standard for demonstrating sufficient evidence of control testing from the course environment.
- 2.2.5 ASD-recognised training providers will mark the assessments and may provide the outcomes to ASD for quality assurance review. The ASD-recognised training providers will notify individuals of their results. This will occur within thirty (30) business days of completion of the final assessment.
- (a) Neither ASD-recognised training providers nor ASD will return completed examinations, or provide feedback to an individual regarding specific exam questions.
- 2.2.6 From the date of results notification, individuals have a period of three (3) months to apply to ASD to become an IRAP assessor by submitting the IRAP Application form on cyber.gov.au.
- 2.2.7 If an individual receives a mark between 75% and 80% on the exam, **and** passes the other assessment components, they will be eligible to sit a second-chance supplementary examination, at their own expense. The supplementary examination has a pass mark of 80%. The supplementary examination must be sat within three (3) months of receiving the initial assessment results.
- 2.2.8 If an individual fails the IRAP training assessments and still wishes to enter the IRAP program, they will be required to re-apply for entry to the IRAP training course, at their own expense.
- (a) Individuals must wait at least six (6) months from the date of results notification before re-enrolling into the IRAP training course. During this time, IRAP applicants are expected to gain additional information security knowledge, including of the ISM and supporting IRAP publications.
 - (b) If an individual fails the IRAP training course and the accompanying assessments two (2) or more times, ASD reserves the right to refuse to process their endorsement application and, by extension, refuse membership to IRAP.
- 2.2.9 Any contest of assessment results should be directed to the applicable training provider in the first instance. Training providers may escalate an individual's contest to ASD when appropriate. Contests will be managed in line with the IRAP Conflict Resolution Process (see Section 8.2).
- 2.2.10 The IRAP course and assessments are updated at ASD's discretion to reflect changes in security frameworks, government policy, the cyber threat landscape, and ASD expectations.
- 2.2.11 Further information regarding the level and format of the IRAP training can be found in the *IRAP Course & Assessment Guidance*.

3. IRAP: Membership

3.1 Membership prerequisites

- 3.1.1 To be eligible for endorsement as an IRAP assessor, the ASD IRAP team must be satisfied that the IRAP applicant meets the requirements outlined in Section 2.1.3, 2.1.4, 2.1.5, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.1.7, and 3.1.8.
- 3.1.2 An IRAP applicant who is not able to meet the necessary requirements will not be eligible for endorsement as an IRAP assessor.

3.1.3 Security requirements

- (a) An IRAP applicant must:
- i. be an Australian citizen; and
 - ii. meet the requirements to apply for, and maintain, at minimum an Australian Government Security Vetting Agency (AGSVA) Negative Vetting Level 1 (NV1) security clearance. For further detail or information on security clearances, refer to Section 3.2.

3.1.4 IRAP training and assessments

- (a) An individual must complete the IRAP training course and pass all the training assessments in order to be eligible for endorsement as an IRAP assessor. For further detail or information on the IRAP training course, refer to Section 2.2.
- (b) An individual must submit an IRAP application to ASD within three (3) months of passing the training course.

3.1.5 Endorsement suitability

- (a) An IRAP applicant must adhere to the IRAP Code of Conduct and IRAP Values outlined in Section 1.6.

3.1.6 IRAP ACSC Partner Portal Deed

- (a) An IRAP applicant must complete and submit an IRAP ACSC Partner Portal Deed, which is available on cyber.gov.au, before being granted access to the ACSC Partner Portal and being admitted into the IRAP.

3.1.7 IRAP Assessor Agreement

- (a) An IRAP applicant must complete and submit the IRAP Assessor Agreement, which is available on cyber.gov.au, before being endorsed as an IRAP assessor by ASD.

3.1.8 IRAP Confidentiality Deed

- (a) An IRAP applicant must complete and submit an IRAP Confidentiality Deed, which is available on cyber.gov.au, before being endorsed as an IRAP assessor.

3.2 Security clearance

- 3.2.1 To be eligible for endorsement as an IRAP assessor, an IRAP applicant must hold, at minimum, an active Australian NV1 security clearance. Security vetting services are conducted by AGSVA, not by ASD.
- (a) ASD may submit a clearance request on behalf of an IRAP applicant to sponsor their security clearance. An individual / IRAP applicant cannot sponsor their own security clearance.
 - (b) ASD will only initiate sponsorship of an IRAP applicant's NV1 security clearance once an IRAP applicant meets all necessary requirements for endorsement as an IRAP assessor. Once sponsorship of a clearance is requested, ASD is unable to provide further assistance regarding the process or timeframes for clearances.
 - (c) All costs relating to the application and maintenance of a security clearance will be the responsibility of the IRAP applicant or IRAP assessor. No financial compensation will be provided by ASD, for costs incurred by an IRAP applicant or IRAP assessor related to security clearances.
 - (d) An IRAP applicant should expect extended lead times for processing security clearance applications and should refer to AGSVA guidance regarding timeframe and progress.
- 3.2.2 If an IRAP assessor leaves the program for any reason, ASD will cease sponsorship of their security clearance.
- 3.2.3 An IRAP assessor whose security clearance is sponsored by ASD is required to adhere to all current organisational security reporting obligations. ASD IRAP can provide an information pack for IRAP assessors sponsored by ASD.
- 3.2.4 Changes in personal circumstances, reported to the AGSVA via the myClearance portal, must also be provided to ASD Clearance Administration team, if a clearance is sponsored by ASD.
- 3.2.5 ASD reserves the right to deny or withdraw the sponsorship of an applicant's security clearance where the applicant does not meet AGSVAs suitability or character traits and/or IRAP Code of Conduct and Values (Section 1.6).
- (a) If an IRAP applicant is assessed by AGSVA as not suitable to hold a security clearance, a procedural fairness process is initiated.
 - (b) The IRAP applicant will be notified of AGSVA's concerns, and will be provided an opportunity to respond. AGSVA will consider all of the information, including the response provided by the IRAP applicant, before making a final decision on the outcome of the security clearance assessment.

3.3 Endorsement requirements for an IRAP assessor

- 3.3.1 To be endorsed by ASD as an IRAP assessor, IRAP applicants must:
- (a) be an Australian citizen.
 - (b) have completed the IRAP training course and passed all IRAP assessments, within the last three (3) months.
 - (c) demonstrate behaviours aligned to the IRAP Code of Conduct and Values (Section 1.6).
 - (d) submit an IRAP application form via cyber.gov.au.
 - (e) submit a signed IRAP Confidentiality Deed, IRAP Assessor Agreement and IRAP ACSC Partner Portal Deed.
 - (f) hold an active NV1, or higher, security clearance.
 - (g) ensure all supporting documentation submitted to ASD is complete and accurate.

(h) read and understand the requirements set forth by this document.

3.3.2 The ASD IRAP team will review the IRAP applicant's application in-line with the above endorsement requirements. IRAP applicants who meet the requirements will be endorsed by ASD as an IRAP assessor and provided with an IRAP certificate and registration number.

3.3.3 Once ASD officially endorses an IRAP applicant, they will be notified in writing. IRAP applicants must not identify themselves as an IRAP assessor until they have received official endorsement and an IRAP registration number from ASD.

3.4 Denial of endorsement

3.4.1 Completion of the IRAP course and assessments does not guarantee program entry. ASD IRAP reserves the right to deny the endorsement of an IRAP applicant at any stage during the endorsement process.

3.4.2 Applicants may be refused endorsement if they:

- (a) fail to meet membership pre-requisite requirements (Section 3.1)
- (b) fail to successfully obtain and maintain a minimum NV1 security clearance
- (c) demonstrate behaviour or act in a way that causes concern for ASD's sponsorship of a security clearance
- (d) are declined sponsorship by ASD personnel security.

3.4.3 Any refusal to sign the IRAP Assessor Agreement, IRAP Confidentiality Deed, and IRAP ACSC Partner Portal Deed will result in denial of endorsement.

3.4.4 Abusive, dishonest or disrespectful behaviour may constitute grounds for the denial of endorsement.

3.4.5 Multiple failed attempts at the IRAP training and assessment course (Section 2.2.8(b))

3.4.6 If an IRAP applicant is assessed as not suitable for endorsement, the Applicant will be advised, and a procedural fairness process will be initiated as follows:

- (a) The Applicant will be advised in writing of ASD's concerns and provided an opportunity to respond; and
- (b) ASD will consider all of the information, including the Applicant's response, before making a final decision concerning the endorsement of the Applicant.

3.4.7 An Applicant can request a review of the decision to deny endorsement by:

- (a) requesting an internal review of the decision by ASD;
- (b) lodging a complaint with the Inspector-General of Intelligence and Security.

3.4.8 ASD will not be liable for any costs incurred related to training or security clearances, if an Applicant is considered not suitable for endorsement.

3.5 Membership maintenance

3.5.1 To maintain IRAP membership, an IRAP assessor is required to adhere to the conditions of the IRAP Assessor Agreement, confidentiality deeds and policies and procedures outlined in this document. Failure to comply with membership conditions may result in the revocation of IRAP membership.

3.5.2 Personal Responsibilities

- (a) IRAP assessors must:
- i. maintain a standard of behaviour that the public would reasonably expect of someone who holds a position of public trust and that meets the requirements of holding a security clearance.
 - ii. adhere to the *IRAP policy and procedures, IRAP Assessor Agreement, IRAP Confidentiality Deed, and IRAP ACSC Partner Portal Deed.*
 - iii. adhere to the IRAP code of conduct and values.
 - iv. inform the ASD IRAP team if any conflicts arise relating to the program, as soon as possible.
 - v. maintain an active NV1 security clearance or higher, at all times.
 - vi. complete any training as instructed by the ASD IRAP team.
 - vii. inform AGSVA and ASD clearance administration (as applicable), of any significant changes to personal circumstances that may affect suitability to hold a security clearance.
 - viii. ensure appropriate marketing of IRAP services, as per *IRAP brand and marketing guidelines.*
 - ix. ensure personal details are managed and up to date at all times, and advise ASD IRAP team of any periods where the IRAP assessor is unavailable to undertake assessments.
 - x. register all IRAP engagements with the ASD IRAP team. Assessment records and Conflict of Interest declarations (COI's) must be submitted a minimum of seven (7) business days before an IRAP engagement commences, and continually updated as required (commencement, delays, and completion), via the ACSC Partner Portal.

3.5.3 ICT security knowledge maintenance

- (a) IRAP assessors are required to maintain and demonstrate an in-depth understanding of Australian security frameworks, and follow IRAP guidance by meeting the following elements:
- (b) Maintain up-to-date knowledge of the ISM and PSPF and apply current versions conducting assessments.
- (c) At all times, utilise current IRAP assessment guidance and resources, including the *IRAP Common Assessment Framework* and report templates provided by ASD.
- (d) Complete any technical competency training requested by ASD IRAP and maintain contemporary technical proficiency.

3.5.4 IRAP Renewal Requirements

- (a) IRAP membership is based on a rolling 24 month cycle. IRAP assessors are required to apply for membership renewal on a 2-yearly basis by submitting the 'IRAP Renewal Application' form on the ACSC Partner Portal. Continued technical proficiency, knowledge of IRAP processes and requirements and active participation towards the programs function, must be demonstrated for

- (b) continued endorsement. Maintenance of current Category A and B certifications are not required as part of the ongoing membership renewal process.

IRAP renewal pathway options			
Within the previous 24 month period:			
Option 1:			
2x Primary IRAP assessments submitted to ASD for QA			✓
Option 2:			
1x Primary IRAP assessment submitted to ASD for QA	1x Secondary IRAP assessments submitted to ASD for QA	Attend 2x IRAP Information evenings (virtual or in-person)	✓
Option 3:			
1x Primary IRAP assessment submitted to ASD for QA	2x Secondary IRAP assessments submitted to ASD for QA		✓
Option 4:			
3x Secondary IRAP assessments submitted to ASD for QA			✓
Option 5:			
2x Secondary IRAP assessments submitted to ASD for QA	Attend 4x IRAP Information evenings (virtual or in-person)		✓

- (c) IRAP membership renewal eligibility will be weighted and determined through the following means/conditions:
- i. Submission of IRAP assessments for quality assurance reviews, in either primary or secondary roles during the previous 24 months.
 - ii. Actively engaging in the IRAP community via attending IRAP Information evenings, maintaining correspondence/reporting to ASD and positively representing the program.
 - iii. The IRAP assessor must not have any outstanding /overdue Corrective Action Plans (CAPs).
- (d) IRAP assessors who are employed by ASD (Commonwealth or Contractors) will be eligible for an alternate renewal pathway contributing to quality assurance activities. ASD-internal IRAP assessors are required to contact the ASD IRAP team to access this renewal pathway.
- (e) IRAP assessors contributing to the facilitation or development of the IRAP training course, will be provided with an alternate renewal pathway; to ensure the integrity of the IRAP training course as a membership renewal pathway. These IRAP assessors will also be required to attend a minimum of 4x IRAP Information evenings within the 24 month renewal period.
- (f) IRAP assessors will be required to sign and submit an IRAP assessor Agreement which aligns to current-day *IRAP policy and procedures*, as part of their membership renewal process.

- (g) If an IRAP assessor is unable to demonstrate contribution to the program, through meeting one of the preceding renewal pathway options within any 24 month period, they may elect to enrol in (and pass) the IRAP training course and assessments, at their own expense. This renewal pathway will only be permitted one time. If the IRAP assessor fails to demonstrate active participation in the program (ie: meet one of the nominated renewal pathway options) for a consecutive 24 months, they will not be eligible for membership renewal.
- (h) If an IRAP assessor's membership is not renewed, they will be ineligible for program re-entry for a period of six (6) months. To re-enter the program, individuals will be required to meet the pre-requisites for enrolment, complete and pass the IRAP training course and assessments, and resubmit and IRAP endorsement application, as per a new applicant.
- (i) The ASD IRAP team reserves the right to make changes to the IRAP renewal process at any time. The ASD IRAP team will inform all IRAP assessors of any changes to the IRAP renewal process as soon as practicable and allow reasonable time for IRAP assessors to achieve the changed requirement(s). Failure or refusal to meet any changed requirements within the specified timeframe may result in removal of IRAP endorsement.

3.5.5 IRAP community

- (a) IRAP assessors are expected to be active participants within the IRAP community. To achieve this IRAP assessors must:
 - i. maintain an understanding of relevant security frameworks and best-practice cyber security guidance provided on cyber.gov.au.
 - ii. regularly access the ACSC Partner Portal to see updates provided by ASD IRAP and ensure contact details remain current. Please note: Portal access is automatically deactivated if not accessed within 90 days.
 - iii. protect and uphold the integrity of the IRAP and its association by reporting any misuse of the IRAP brand, instances of individuals misrepresenting their IRAP status, or concerns regarding an IRAP assessment.
 - iv. contribute to ASD events, forums and workshops, and keep abreast of general community news/correspondence.
 - v. advise ASD IRAP team of any request to represent IRAP at external events or forums.
 - vi. notify the ASD IRAP team of any changes that may affect the IRAP assessor's availability to perform assessments.
 - vii. encourage clients to submit feedback to support improvements to IRAP.
- (b) The IRAP membership requirements will be reviewed at ASD's discretion to ensure IRAP assessors continue to demonstrate proficiency to perform IRAP assessments, meet changing technology security requirements, and understand the security threat landscape. ASD will take reasonable steps to ensure all IRAP assessors have time and access to meet any change in requirements.
- (c) IRAP assessors are required to apply for their own work. ASD is only responsible for the governance and administration of the program and is not involved in any third-party commercial arrangements.

3.5.6 IRAP assessment requirements

- (a) IRAP assessors conducting an IRAP assessment must:
- i. Submit an Assessment Record and Conflict of Interest declaration to the ASD IRAP team at least seven (7) business days prior to commencing an IRAP assessment. This is submitted via the self-service function on the ACSC Partner Portal.
 - ii. Produce objective and accurate IRAP assessments in line with *the IRAP Common Assessment Framework* and *IRAP Assessment Report* template.
 - iii. Not agree to any terms or non-disclosure agreements that would impede ASD's ability to obtain copies of IRAP reports for quality assurance purposes, including the security controls matrix, or any other IRAP documentation produced by the IRAP assessor.
 - iv. Secure all information and electronic devices used in IRAP services, as agreed with the customer and commensurate to the sensitivity and classification of the information.
 - v. Provide a copy of the IRAP assessment report and controls matrix to ASD when requested, and ensure the Assessment Record is closed within the ACSC Partner Portal when completed.
 - vi. Participate in the IRAP quality assurance process, and comply with agreed deliverables and timeframes.
 - vii. Ensure final products align with current *IRAP brand and marketing guidelines* and are distinguishable as an IRAP assessment report.

3.5.7 Removal from the IRAP program

- (a) ASD reserves the right to revoke the endorsement of an IRAP assessor identified as continuously failing to demonstrate adherence to program policy and quality standards, as outlined in this document and the *IRAP Quality Assurance Framework*.
- (b) Where ASD IRAP is made aware of potential breaches in program policy, agreements or deeds, or severe deficiencies in assessment quality standards, the IRAP assessor will be contacted by the ASD IRAP team and provided right of reply and procedural fairness opportunities.
- (c) See Section 4.5 for more information on the quality assurance process.

4. IRAP: Assessors

4.1 IRAP assessment reporting

- 4.1.1 ASD expects all IRAP assessors to provide high-quality services to clients. All IRAP assessments are expected to uphold the high standards of the program and follow the methodologies outlined in the *IRAP Common Assessment Framework*.
- 4.1.2 Metrics and insights collected through the assessment process and Customer feedback, may be used to inform program direction, wider ASD functions, and Whole of Government security advice.
- 4.1.3 IRAP assessors are expected to use and adapt (as relevant) assessment templates provided on the IRAP Resources page on cyber.gov.au and in the ACSC Partner Portal.
- 4.1.4 Multiple IRAP assessors may work on a single IRAP assessment.
- (a) Any IRAP assessor involved in the assessment process must submit an Assessment Record and Conflict of Interest declaration; recording themselves as the primary or a secondary IRAP assessor, at least seven (7) business days before commencing an IRAP assessment.
 - (b) Where multiple IRAP assessors have been actively involved in an assessment, each IRAP assessor must sign-off on the IRAP assessment report. This may be used as evidence to support IRAP membership renewal.
 - (c) Any IRAP assessor listed on an IRAP assessment is responsible for its contents and must engage in the quality assurance process; with any reviews or outcomes being applied to all involved.
- 4.1.5 ASD may request an IRAP assessment report to perform quality assurance review, as per the *IRAP Quality Assurance Framework*. The IRAP assessment report, controls matrix and any relevant documentation, must be provided if requested by the ASD IRAP team. This may be provided by the IRAP assessor or the owner of the report.
- 4.1.6 IRAP assessors that are designated 'Assessors of Interest' (as per the *IRAP Quality Assurance Framework*) must provide copies of all IRAP assessments to ASD IRAP for quality assurance review, on completion. New IRAP assessors are automatically designated 'Assessor of Interest' status upon entry into the program.
- 4.1.7 If an IRAP assessment report has been reviewed by ASD and is deemed 'not at standard' (as per the *IRAP Common Assessment Framework*), in the first instance, ASD will support the IRAP assessor and their client to uplift the IRAP assessment report to an acceptable standard, in accordance with the *IRAP Quality Assurance Framework*.
- 4.1.8 Failure to comply with the quality assurance process may be considered a breach of *IRAP policy and procedures* and may result in action by ASD, as outlined in Section 4.5.

4.2 Supporting information security guidance

- 4.2.1 ASD maintains publications and guidance on specific technologies and security topics on cyber.gov.au. These publications provide valuable advice and IRAP assessors should maintain an awareness of the publications and use them to support their assessments, where appropriate.
- 4.2.2 Some key documents that can be found on cyber.gov.au include:
- (a) IRAP Common Assessment Framework.
 - (b) IRAP Quality Assurance Framework
 - (c) IRAP brand and marketing guidelines.

- (d) IRAP Assessment Report Template.
- (e) Cloud security assessment template.
- (f) IRAP Consumer Guide.
- (g) Information Security Manual.
- (h) Modern defensible architecture
- (i) ASD's Blueprint for Secure Cloud
- (j) Gateway security guidance package

4.3 Confidentiality

- 4.3.1 IRAP assessors are often entrusted to sensitive information. Additionally, they may be responsible for contributing toward the information security of a government entity.
- 4.3.2 All IRAP assessors will be required to sign an IRAP Confidentiality Deed relating to information they may be privy to through the course of undertaking IRAP assessments. IRAP assessors will likewise be required to sign an IRAP ACSC Partner Portal Deed in relation to information produced by ASD they may be privy to once given access to the ACSC Partner Portal.
- 4.3.3 ASD requires IRAP assessors to handle all information collected in the course of their engagements as an IRAP assessor in accordance with the *Privacy Act 1988* (Cth). This means that IRAP assessors must consider the Australian Privacy Principles within the *Privacy Act 1988* (Cth) when collecting, using, disclosing or storing personal information at all stages of an IRAP assessment.
- 4.3.4 More information on the *Privacy Act 1988* (Cth) and the Australian Privacy Principles can be found here: [OAIC Guidelines](#).
- 4.3.5 In addition to the requirements above, an IRAP Customer may require an IRAP assessor to separately agree to internal policies, agreements or applicable laws in relation to confidentiality, before commencing an IRAP assessment. The IRAP assessor should not agree, however, to any terms or non-disclosure agreements that would impede ASD's ability to obtain copies of IRAP assessment artefacts for quality assurance purposes, as per Section 3.5.6.
- 4.3.6 It will be the IRAP assessor's responsibility to ensure they understand, and comply with, the confidentiality arrangements with the IRAP Customer. ASD is not responsible for managing the confidentiality arrangements between the IRAP Customer and IRAP assessor in relation to an IRAP assessment.
- 4.3.7 ASD will investigate any reported or suspected breaches of confidentiality by an IRAP assessor, as per Section 4.6. Any breaches of confidentiality may result in revocation of ASD's endorsement as an IRAP assessor.

4.4 Conflict of interest

- 4.4.1 ASD's ability to manage potential conflicts of interest and uphold the independence of assessments is vital. It is therefore critical that ASD is aware of any potential conflicts of interest, to maintain a high level of confidence and trust in IRAP assessors.
What is a conflict of interest?
- 4.4.2 A conflict of interest arises when there is conflict between an IRAP assessor's duties and responsibilities and their personal interests that could, or could be seen to, influence the decisions they are taking or the advice they are giving in relation to an IRAP assessment. An IRAP assessor's duties and responsibilities includes any activity conducted for, or in connection with, IRAP.

- 4.4.3 IRAP assessors must keep in mind that conflicts of interest may be **real, potential** or **apparent** when assessing whether conflicts of interest exist. These terms are defined as follows:
- (a) **Real** – where a direct conflict exists between current IRAP duties and existing personal interests;
 - (b) **Potential** – where personal interests do not, but could, come into direct conflict with IRAP duties; and
 - (c) **Apparent** – where a third party could reasonably perceive that an IRAP assessor’s personal interest may influence the performance of their IRAP duties, now or in the future. This can occur whether there is a conflict or not.
- 4.4.4 Conflicts of interest can also arise from situations that could allow IRAP assessors to avoid personal losses or detriment, or gain personal advantage, whether financial or otherwise, for themselves or a third party.
- 4.4.5 There is no exhaustive list of conflicts that must be disclosed. It is the responsibility of the IRAP assessor to consider their circumstances and disclose their interests or relationships to ASD. If in doubt, it is recommend the conflict of interest is disclosed for ASD’s assessment.
- 4.4.6 Common circumstances that might influence the IRAP assessor’s provision of services includes:
- (a) personal relationships;
 - (b) material interests;
 - (c) financial interests or corporate affiliations;
- 4.4.7 By way of additional examples, a conflict of interest will arise where:
- (a) An IRAP assessment is performed on a system where the IRAP assessor, or another party with whom they have a personal relationship, interest or corporate affiliation, has direct influence over the system. This influence includes, but is not limited to the development, ownership or update of system components, documentation, mitigation advice, or implementation guidance they may have taken upon the system. This applies even if the work was completed through a separate reporting structure, difference in physical locations, or point in time in which those activities were undertaken.
 - (b) This includes situations involving two parties that are related by corporate mergers, takeovers, subsidiaries or any other affiliation where they are ultimately owned by the same parent organisation, or where staff are employed by both parties. Customers should consider potential conflicts of interest before engaging an IRAP assessor; particularly, if they will be assessing a system that has been outsourced or shaped by an external party.
- When must a conflict of interest declaration be made?*
- 4.4.8 Upon engagement by an IRAP Customer, IRAP assessors must submit an IRAP Conflict of Interest declaration form at a minimum of seven (7) business days before commencing each IRAP assessment. This declaration must be submitted regardless of whether a real, potential, apparent, or no conflict of interest exists.
- 4.4.9 All Conflict of Interest declarations can be made through the ACSC Partner Portal on cyber.gov.au.
- 4.4.10 Conflict of Interest declarations must also be submitted by any secondary IRAP assessor involved in an IRAP assessment, via the ACSC Partner Portal.
- 4.4.11 ASD will then review the declaration and consider any mitigation strategies put forward by the IRAP assessor. An IRAP assessment must not proceed if ASD IRAP advises that the proposed mitigation strategies do not satisfactory mitigate the conflict.
- 4.4.12 If the circumstances of a conflict of interest change during the course of an IRAP assessment, IRAP assessors must immediately update their Conflict of Interest declaration in the ACSC Partner Portal.

For example, if an IRAP assessor declares they have no conflict of interest at the commencement of the assessment but a potential conflict of interest arises part way through the assessment, they must log into the ACSC Partner Portal and disclose the potential conflict of interest immediately.

- 4.4.13 If a 'real' conflict of interest arises during the course of an IRAP assessment, the IRAP assessor must stop work on the IRAP assessment until ASD has considered the declaration and any proposed mitigations. To protect the integrity of the program, ASD reserves the right to require conflicted IRAP assessors to disengage from the assessment, transition the assessment to a non-conflicted IRAP assessor, or cease the assessment altogether.
- 4.4.14 ASD will not be liable for any costs incurred as a result of an IRAP assessor being required to cease, transition or disengage from an assessment due to unacceptable conflicts of interest.

Failing to declare conflicts of interest

- 4.4.15 Declaring all conflicts of interest is a requirement of the program. As such, failure to complete and submit a Conflict of Interest declaration prior to any assessment will be a breach of this document and the IRAP Assessor Agreement.

4.5 Quality assurance

- 4.5.1 ASD IRAP governance provides a systematic process for evaluating and improving the quality of IRAP assessments performed by IRAP assessors. This ensures that IRAP assessments remain of a high standard and consistency, and IRAP assessor conduct is professional and reputable.
- 4.5.2 ASD will perform quality assurance activities by requesting copies of completed IRAP assessments and controls matrices for review and feedback. All IRAP assessors are required to comply with any requests for Assessment reports in a timely manner, or to timeframes outlined by ASD.
- 4.5.3 Quality Assurance activities will review the IRAP assessment requirements as outlined in the *IRAP Common Assessment Framework*. The details of quality standards are outlined in the *IRAP Quality Assurance Framework (QAF)*
- 4.5.4 It is the responsibility of the IRAP assessor to notify the assessed entity of the requirement to provide ASD with copies of IRAP assessments upon request.
- 4.5.5 Any limitations identified through quality assurance activities will be communicated through feedback from ASD. This may include recommended corrective actions through a Corrective Action Plan (CAP).
- 4.5.6 IRAP assessors are required to collaborate and agree to corrective actions and a delivery timeframe for the Corrective Action Plan to be completed.
- 4.5.7 If the remediation activities identified in a Corrective Action Plan are not addressed or not addressed to the acceptable standard agreed upon, a decision may be made by ASD to revoke IRAP assessor membership on the basis of non-compliance. Procedural fairness will be managed in-line with the IRAP Conflict Resolution process (see Section 8.2).
- 4.5.8 If an IRAP assessor is revoked from the program due to Quality Assurance non-compliance, they will be ineligible for program re-entry.

4.6 Revocation of IRAP endorsement

- 4.6.1 ASD is responsible for the governance of the IRAP program and is obligated to ensure IRAP assessors contribute to the program’s function, and provide assessments in line with quality standard expectations. ASD reserves the right to suspend or revoke an IRAP assessor’s membership through removal of their ongoing endorsement.
- 4.6.2 For the purpose of this policy:
- (a) a decision by ASD to suspend IRAP Membership may be employed while ASD conducts an investigation of potential breaches. Suspension includes the removal of the IRAP assessor’s name from the IRAP assessor list. During this time, the IRAP assessor must not engage new assessment activities or market themselves as an IRAP assessor. Individuals who have had their membership suspended may be allowed to re-join the program subject to completion of the investigation and/or the individual complying with such conditions as may be specified by ASD.
 - (b) a decision by ASD to revoke IRAP Membership means the immediate withdrawal of endorsement by ASD. An IRAP assessor must cease all assessment activities from the point of notification and must not market themselves as an IRAP assessor. Any IRAP assessor revoked from the program will be ineligible to re-join the program in the future.
- 4.6.3 Actions by an IRAP assessor that may constitute grounds for the suspension or revocation of a membership include:
- (a) a breach of IRAP policy or IRAP Assessor Agreement
 - (b) a failure to comply with ongoing membership requirements
 - (c) a failure to comply with the IRAP quality assurance process
 - (d) unprofessional behaviour towards ASD, the IRAP program, the IRAP assessor community or external parties, including through inappropriate use of communication channels, such as Slack.
 - (e) behaviour which gives rise to a concern for national security
 - (f) a failure to maintain an NV1 minimum security clearance
 - (g) a failure to declare or manage a conflict of interest or integrity concern
 - (h) misrepresentation of ASD or the IRAP brand
 - (i) any behaviour inconsistent with the IRAP code of conduct
- 4.6.4 Where ASD assesses a minor breach of IRAP policy or program requirements has occurred it may issue a written notice to the IRAP assessor requiring corrective action to be taken within a specified time-frame. A notice issued under this clause may also specify additional reporting conditions to provide ASD with an assurance that the IRAP assessor is meeting their compliance obligations. Compliance with such additional reporting obligations is mandatory for the IRAP assessor’s ongoing endorsement by ASD.
- 4.6.5 For the purposes of this policy, a major breach of IRAP policy or program requirements refers to repeated minor breaches, a failure to comply with one or more fundamental IRAP obligations, or an action or behaviour from which the repercussions could cause a substantial risk to ASD/IRAP’s reputation or Australia’s national interests.
- 4.6.6 Where ASD assesses a major breach of IRAP policy or program requirements has occurred it will adopt the following process:
- (a) ASD will provide the IRAP assessor with a written notice of the issues of concern and the range of actions which may be considered (including revocation), and provide the IRAP assessor with an opportunity submit a response.

- (b) ASD will take into account all relevant information and evidence relating to the decision (including any responses from the parties), and make a decision based on an application of the IRAP Policy and other relevant considerations.
 - (c) ASD will inform the IRAP assessor of its decision in writing.
- 4.6.7 The IRAP assessor can request a review of the decision in writing, including supporting evidence.
- 4.6.8 ASD IRAP will not be liable for any costs or hardship incurred as a result of membership suspension or revocation due to non-compliance with IRAP policy or other program requirements.

5. IRAP: Consumers

5.1 IRAP assessment customers & consumers

- 5.1.1 A government agency or commercial organisation that is procuring an IRAP assessment should refer to the IRAP Consumer Guide which is located on the IRAP cyber.gov.au webpage. IRAP assessment Consumers and Customers are responsible for:
- Asking questions to ensure they engage an IRAP assessor familiar with the type of system being assessed. A list of available IRAP assessors can be found on cyber.gov.au.
 - Ensuring preparations are made in order to provide relevant documentation and evidence of technical configuration to the IRAP assessor in a timely manner.
 - Following ASD guidance when marketing the completion of an IRAP assessment, as per the *IRAP brand and marketing guidelines* found on cyber.gov.au
 - Being aware that IRAP reports must be provided to ASD IRAP team by IRAP assessors if requested, to support IRAP quality assurance activities and inform program direction.
- 5.1.2 An IRAP assessment consists of, at a minimum, an IRAP assessment report and a security controls matrix. Consumers / authorising officers should ensure that they have both the assessment report and security controls matrix to inform their risk-based decision making.
- 5.1.3 ASD strongly encourages vendors to share their IRAP assessment reports and security controls matrices with potential Government customers to inform risk-based authorisation decisions.
- 5.1.4 It is the responsibility of the IRAP assessor to ensure that their customers are aware of the published guidance in relation to marketing.

5.2 Applicable policy

- 5.2.1 In accordance with the *Protective Security Policy Framework (PSPF) Section 13 – Technology Lifecycle Management*, Outsourced information technology systems, cloud services, and Gateways (up to SECRET) must be assessed by an IRAP assessor.
- 5.2.2 As per *PSPF Requirement 0043*, any Government entities providing outsourced services must provide IRAP assessment reports to the government entities consuming, or looking to consume, their services.

6. IRAP: Brand and marketing

6.1 IRAP assessment customers & consumers

- 6.2.1 Entities procuring IRAP assessments are responsible for ensuring references to the program are accurate to uphold the reputation and function of the program.
- 6.2.2 'IRAP' is a registered trademark, which the Australian Signals Directorate owns.
- 6.2.3 The 'IRAP' name and logo may only be used in ways that meet the requirements detailed in the *IRAP brand and marketing guidelines*.
- 6.2.4 Commercial entities who employ IRAP assessors may advertise IRAP assessment services on their behalf. Assessments marked as IRAP assessments must have been conducted by ASD-endorsed IRAP assessor/s.
- 6.2.5 IRAP customers may promote the completion of an IRAP assessment in accordance with terminology and guidance in the *IRAP brand and marketing guidelines*. To guide IRAP assessors and industry, the approved ASD IRAP marketing copy is:
- "<Organisation X> has completed an IRAP assessment for <System X> against the Information Security Manual's <Classification> level controls."*
- (a) Service providers advertising the completion of an IRAP assessment need to include the services or system that was assessed.
- (b) ASD IRAP logos are available to IRAP assessors and Customers via cyber.gov.au.
- 6.2.6 ASD does not accredit, certify, endorse or register any system under IRAP. Publishing statements referring to IRAP or ASD accreditation, certification, endorsement, registration or authorisation to operate a system is a misrepresentation of IRAP's role, and will result in ASD requesting the immediate removal or recall of misleading statements.

6.2 IRAP assessors

- 6.2.1 IRAP assessors must follow the *IRAP brand and marketing guidelines* when producing IRAP reports and promoting IRAP assessment services and their involvement in the program.
- 6.2.2 IRAP assessors should use caution regarding personal profile management in particular on social media platforms and use discretion regarding disclosure of their security clearance, as per AGSVA advice.
- 6.2.3 IRAP assessors must not claim to represent, or speak on behalf of, ASD or ASD IRAP, including at external forums or events, without permission from ASD.

7. IRAP: Training providers

7.1 About

- 7.1.1 Only training providers engaged by ASD through a formal tender process are permitted to provide IRAP training services using ASD-developed resources and use the IRAP brand in promoting this training.
- 7.1.2 All ASD IRAP training providers are required to meet the following:
- (a) deliver only ASD IRAP approved training material as part of the IRAP training course.
 - (b) provide adequate facilities and systems for training.
 - (c) incorporate any changes to course material as requested by ASD.
 - (d) deliver training and assessment material in accordance with the Memorandum of Understanding.
- 7.1.3 Training providers will conduct checks to ensure that the prospective participant meets the necessary pre-requisites to enrol in the IRAP training course, as outlined in Section 2.1.

8. ASD

8.1 Responsibilities

- 8.1.1 The ASD IRAP team oversees the governance, operation, clearances and management of the IRAP program and provides advice, assistance and support to:
- (a) IRAP applicants.
 - (b) IRAP assessors.
 - (c) IRAP training providers.
 - (d) Government and commercial entities using, or interested in, IRAP assessment services.
- 8.1.2 The ASD IRAP team will consult with, and inform, IRAP assessors on IRAP assessment activities, relevant cyber security trends, changes to related Australian government policies, and changes to the program, through focus sessions and information evenings.
- 8.1.3 ASD is responsible for the quality assurance and strategic direction of the program and works to ensure independence of IRAP assessments as per the programs objective.
- 8.1.4 ASD will not recommend any IRAP assessor to potential clients and will not be involved in any third-party commercial arrangements.
- 8.1.5 To support customer access to IRAP services, ASD maintains a list of current IRAP assessors publically available on cyber.gov.au, which includes a list of available and engaged IRAP assessors.
- 8.1.6 ASD is responsible for ensuring continued IRAP program alignment with current policy, legislative advice and Government priorities.
- 8.1.7 ASD reserves the right to make changes to IRAP at any time, including the administration of the program, the training course, and the introduction of new membership requirements.
- 8.1.8 ASD reserves the right to pause IRAP assessor endorsement application and program processes at any time due to changes in Government priorities.
- 8.1.9 ASD will inform all IRAP assessors of any changes as soon as possible and allow reasonable time for IRAP assessors to achieve the changed requirement(s).

8.2 Conflict resolution process

- 8.2.1 Feedback in relation to the operation of IRAP is valued, and will be used to stimulate improvements and address weaknesses in program outputs or administration.
- 8.2.2 For formal complaints and disputes concerning IRAP or arising from the operation of IRAP, the complainant should notify ASD IRAP in writing, with supporting evidence, via asd.irap@defence.gov.au.
- 8.2.3 Complaints regarding the actions or behaviour of an IRAP assessor should be reported to asd.irap@defence.gov.au.
- 8.2.4 ASD IRAP will acknowledge the complainant on receipt of the formal notification, and the timeframe for resolution will be agreed.
- 8.2.5 Complaints or disputes arising from commercial arrangements between IRAP assessors and their clients are outside the scope of this program. ASD, either directly or through IRAP, will not become involved in matters of contractor payment disputes between entities and IRAP assessors.

- 8.2.6 Complaints or disputes arising from commercial arrangements between the IRAP training providers and course participants are outside the scope of this program. ASD, either directly or through IRAP, will not become involved in matters of commercial disputes between training providers and course participants.
- 8.2.7 Complaints or disputes relating to the outcome of the IRAP training course results will be managed with the applicable training provider in the first instance. Where ASD requires involvement, all available and relevant evidence from both parties will be considered, and a decision will be made by IRAP Director.
- 8.2.8 Any system or content issues encountered during the IRAP course and exam, such as connection disruptions or technical issues, must be brought to the attention of the training provider in real-time, or provided in writing the same day. ASD will not accept belated claims of technical disruptions as evidence in result disputes.

9. Appendix

9.1 Related legislation, directives, policies and procedures

9.1.1 Related information: *Protective Security Policy Framework (PSPF)* and *Information Security Manual (ISM)*.

9.2 Getting help

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

9.3 Version history

Version	Date	Comment	Updated by
1.0	Dec 2020	Reformed policy	ASD IRAP
2.0	June 2026	Reformed policy	ASD IRAP

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

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license
<https://creativecommons.org/licenses/by/4.0/>

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license <https://creativecommons.org/licenses/by/4.0/legalcode.en>

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 <https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre