# Policy and Procedures

11/2020

Australian Signals Directorate
Information Security Registered Assessors Program

# Information Security Registered Assessors Program

The Information Security Registered Assessors Program (IRAP) is an Australian Signals Directorate (ASD) initiative to provide high quality information and communications technology (ICT) security assessment services to government and industry.

ASD, through IRAP, endorses suitably qualified and experienced cyber security professionals to provide relevant security services which aim to secure broader Industry and Government information and associated systems.

## Purpose and Rationale

1. Cyber and information security is a top national security priority for government. Cyber intrusions on government systems, critical infrastructure and other information networks are a real threat to Australia's national security and national interests.
2. IRAP is a key initiative that provides assurance that ICT systems meet the Government's cyber security standards such as the Australian Government Information Security Manual (ISM) and provides a framework by which individuals are endorsed by ASD. IRAP assessors are employed across the private and public sectors to provide information security assessment services. Endorsed IRAP assessors are engaged to provide an independent assessment of ICT security, suggest mitigations and highlight associated residual risks.
3. This policy outlines the conditions for membership of IRAP, the requirements to maintain membership, and conditions that would rescind membership. In addition, this policy outlines the IRAP Administrator's responsibilities. A strong focus is placed on governance requirements throughout this policy to create a culture that reinforces an IRAP assessor's independence, competency and professionalism.

## Application

4. This policy applies to:
    a. IRAP applicants – A cyber security professional who applies to ASD to be endorsed as an IRAP assessor.

    b. IRAP assessors – A cyber security professional endorsed by ASD through the IRAP application process to conduct independent security assessment services. Also referred to as an IRAP member.

    c. IRAP training providers – Organisations recognised by ASD as providing high quality training and/or technical qualifications that are approved by ASD to delivery IRAP training.

    d. IRAP Administrator – Responsible for the administration and management of the program and available to provide advice and guidance on IRAP related issues.

## Authorisation

5. The First Assistant Director General of Cyber Security Services authorises ASD persons to exercise, from time-to-time, decision making powers on their behalf.

# IRAP Membership

## Pre-requisite qualifications for IRAP assessors

6. To be eligible to join as an IRAP assessor, the IRAP Administrator must be satisfied that an IRAP applicant meets the following minimum requirements listed below.

### Personal qualities

Applicants must:

- be an Australian citizen
- behave professionally and ethically, and
- meet the requirements to apply for a minimum Australian Government Security Agency Negative Vetting Level 1 (NV1) security clearance. Refer to the section on Security Clearances for further details.

### Qualifications

Applicants must be able to provide evidence of a qualification from both Category A and Category B - appropriate evidence includes copies of certificates of attainment, including relevant certification numbers.

Category A:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- GIAC Security Leader Certification (GSLC)

Category B:

- Certified Information Systems Auditor (CISA)
- Payment Card Industry Qualified Security Assessor (PCI QSA)
- ISO 27001 Lead Auditor
- GIAC Systems Network Auditor (GSNA)
- Certified in Risk and Information Systems Control (CRISC)

### Demonstrated security experience

Applicants must provide evidence to substantiate five (5) years of technical ICT experience with at least two (2) years of information security experience securing systems using the Australian Government Information Security Manual (ISM) and supporting publications.

### IRAP training and examination

Applicants must complete IRAP New Starter Training and pass the IRAP assessor examination. Refer to the IRAP assessor examination section for further details.

## Conflict of Interest and confidentiality

Applicants must submit a conflict of interest declaration, and confidentiality deed which are available on cyber.gov.au. Refer to the section on conflict of interest for further details.

## IRAP New Starter Training and assessor examination

7. The IRAP New Starter Training is provided through an ASD endorsed IRAP training provider. As part of the IRAP New Starter Training, applicants will be required to undergo an examination process. IRAP New Starter Training is available for any interested person to complete, however to be endorsed as an IRAP assessor they must meet the IRAP membership requirements.

8. The IRAP New Starter Training is separated into two components:

   a. ISM Fundamentals, and

   b. IRAP Fundamentals.

9. Once attendees have completed and participated in IRAP New Starter Training, they may sit the IRAP assessor examination.

10. The examination may consist of multiple choice and/or short answer questions. IRAP applicants will be given 120 minutes to complete the examination, with an overall pass mark set at 80%. This examination will be updated at ASD's discretion to reflect changes in government policy, the cyber threat landscape and ASD expectations.

11. The IRAP Administrator will mark the examinations and notify applicants of their results within 30 days of completion. ASD does not return completed examinations, nor provide specific feedback.

12. If an applicant does not obtain a pass mark of 80%, the applicant may re- attempt the IRAP examination after waiting for a period of at least four (4) months. During this time, the applicant is expected to gain additional information security experience and knowledge, including the application of the ISM and supporting publications. If the applicant wishes to repeat the IRAP New Starter Training, they may do so only after this four (4) month wait period, subject to course availability. Repeating the IRAP New Starter Training is not a mandatory requirement to re-attempt the IRAP examination. If the applicant does not re-attempt the IRAP examination within 12 months from their first attempt, they must re-apply for entry into the program.

13. If an applicant fails the IRAP examination twice, they must re-apply for entry into the program. Applicants must wait at least 12 months from their exam result notification before re-applying for entry into the program. ASD strongly encourages applicants to re-consider their suitability for entry into IRAP if they fail the examination twice. If an applicant repeatedly fails the IRAP New Starter Training and accompanying examination, ASD reserves the right to refuse to process their application, and by extension refuse the applicant entry to the program. An applicant may appeal the result of an exam by contacting the IRAP administrator (via asd.irap@defence.gov.au) . All appeals will be managed in line with the IRAP conflict resolution process.

14. Further information regarding the content and structure of the IRAP examination can be found in the IRAP Entry Examination Guide.

## Security clearance

15. IRAP applicants must hold a NV1 security clearance prior to being endorsed as an IRAP assessor.

16. If necessary, ASD will initiate and sponsor the IRAP applicant's NV1 security clearance, once an IRAP applicant has passed the New Starter Training and examination and meets the pre-requisite conditions. Additionally, the initiation and/or sponsorship of an NV1 security clearance prior to entry into IRAP may be arranged through other entities requiring the engagement and the respective IRAP applicant, or through the Defence Industry Security Program (DISP).

17. All costs relating to the application and maintenance of a security clearance will be the responsibility of the IRAP applicant. No financial compensation will be provided for costs incurred by an IRAP applicant or assessor related to security clearances.

18. If requested, ASD will sponsor existing security clearances above NV1 held by an IRAP applicant.

19. If a member leaves the program for any reason, ASD will cease sponsorship of the individual's security clearance.

20. For further details see the Australian Government Security Vetting Agency guidelines at: [www.defence.gov.au/security/clearances](www.defence.gov.au/security/clearances).

## Membership requirements to become an IRAP assessor

21. In order to be endorsed by ASD, IRAP applicants must:

    a. submit an IRAP application form and conflict of interest declaration which can be found on the IRAP website at cyber.gov.au

    b. ensure all supporting documentation is complete and accurate

    c. currently hold a certification from both Category A and Category B

    d. completed IRAP New Starter Training and passed examination within the last 12 months

    e. be granted their NV1 security clearance, and

    f. allow 10 business days for ASD to begin processing the application.

22. Once the IRAP Administrator has reviewed the application for the above criteria, applicants who meet the above criteria will be endorsed by ASD as an IRAP assessor and provided with a registration number.

23. Once ASD officially endorses an applicant, they will be notified in writing. Applicants must not identify themselves as IRAP assessors until they have received official endorsement from ASD.

24. A successful applicant becomes a registered IRAP assessor when their details are published on cyber.gov.au.

## Maintaining IRAP assessor membership

To maintain IRAP membership, assessors are required to meet the following requirements. Failure to comply with membership conditions could result in the suspension or revocation of IRAP membership as deemed appropriate by the IRAP administrator.

## Personal qualities

IRAP assessors must:

- adhere to the IRAP Policy and Procedures and behave professionally and ethically when representing ASD
- inform the IRAP Administrator if any conflicts arise relating to the program as soon as possible
- maintain a minimum NV1 security clearance
- pay for security clearance, qualification maintenance and training requests. No financial compensation will be provided for costs incurred by an IRAP applicant or assessor related to IRAP Membership
- notify the IRAP Administrator of any change of circumstances that may impact endorsement, including when unavailable to undertake assessments, and
- notify IRAP Administrator of all IRAP engagements (commencement, delays, and conclusion) via asd.irap@defence.gov.au.

## ICT security knowledge maintenance

IRAP assessors are required to maintain and demonstrate an in depth understanding of the ISM and IRAP by meeting the following elements:

1. At all times, maintain pre-requisite professional qualifications as identified in Category A and B of the application process.
2. Maintain an up-to-date knowledge of changes ISM.
3. Annually, demonstrate maintenance of ISM and IRAP assessment knowledge through completion of either:
   - Submission of an IRAP assessment report – identifying assessments completed within the previous 12 months

     OR
   - IRAP examination.
4. As directed, undertake IRAP-related learning and development activities.

## IRAP assessment requirements

When preparing for and completing an IRAP assessment, IRAP assessors must:

- provide conflict of interest declaration to the IRAP Administrator when engaged to complete an IRAP assessment via asd.irap@defence.gov.au
- produce objective and accurate IRAP assessments in line with the ASD IRAP assessment Reporting Guide
- not agree to terms that would impede ASD's ability to review the assessment or evidence for quality assurance, and
- 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.

## IRAP community

IRAP assessors are expected to be active participants within the IRAP community to provide consistency and uplift of IRAP assessments. To achieve this IRAP assessors are expected to:

- maintain an understanding of government advice and policy through the ACSC Communications Portal at cyber.gov.au
- contribute to events, forums, workshops and general correspondence, and
- notify the IRAP Administrator of any changes that may impact the IRAP assessor availability lists.

25. Membership requirements will be reviewed at ASD's discretion to ensure IRAP assessors continue to have the necessary training and skills to perform IRAP assessments, meet changing technology security requirements, and understand the security threat landscape. ASD will take every reasonable step to ensure all assessors have time and access to meet any change in requirements.

## Transitional arrangements to IRAP policy

26. Some membership requirements have changed. Existing IRAP members will have a twenty-four month grace period from the effective date of the updated policy to fulfil the new requirements. This will include completion of the new starter training and attainment of an NV1 security clearance.

27. This policy will apply to new IRAP assessments prospectively, assessments underway will be grandfathered under the previous policy.

## IRAP assessors

28. IRAP assessors are endorsed by ASD to conduct independent assessments to assess security controls for a system and its environment to determine if they have been implemented effectively and are operating as intended in accordance with the ISM, Attorney-General's Department's Protective Security Policy Framework (PSPF) and other cyber security related guidance.

29. IRAP assessors will be required to apply for their own work.

30. An assessment typically includes, but is not limited to, the following activities:

    a. Informing the IRAP Administrator (via asd.irap@defence.gov.au) of engagements by submitting a conflict of interest declaration.

    b. Coming to an agreement with the system owner on :

        i. the version of the ISM to be used

        ii. the intended security classification of the data the system will handle

        iii. how new ISM guidance will be considered in the assessment

        iv. scope, type, extent, timings and milestones of the assessment

        v. appropriate use and marketing of the completed assessment, and

        vi. availability of the security assessment report and evidence to ASD for quality assurance purposes.

    c. Full system documentation review.

    d. Onsite inspection.

    e. Interview(s) with key staff, including system owners, operations staff and stakeholders.

    f. Evidence gathering and verifying technical configurations to confirm effectiveness of security controls.

    g. Production of a security assessment report that:

        i. outlines the scope of the security assessment

        ii. the system's strengths and weaknesses

        iii. security risks associated with the operation of the system

        iv. the effectiveness of security controls

        v. any recommended remediation actions, and

        vi. enables the reviewer of the report to make an informed risk-based decision about the system's suitability for their security needs and risk appetite.

31. Answering further questions following assessment activities from ASD or other Australian Government entities.

## IRAP assessment reporting

32. ASD expects all IRAP assessors to provide quality services to clients. All IRAP assessments are expected to uphold the quality outlined in the IRAP Assessment Reporting Guidelines.

33. Where appropriate, ASD recommends the use of assessment templates that are available on the IRAP website and the ACSC Communications Portal.

34. Where mutiple IRAP assessors has been actively involved in an assessment, those assessors may each sign off on the IRAP assessment report. This may be used as evidence to demonstrate maintenance of ISM and IRAP assessment knowledge on an annual basis.

35. On an annual basis, ASD will request a sample of IRAP assessments to perform a quality assurance review. The IRAP assessment and any relevant evidence must be provided if requested by ASD. This may be provided by the IRAP assessor or the owner of the report.

36. If an IRAP assessment that has been reviewed by ASD is deemed poor quality, in the first instance, ASD will support the assessor and their client to uplift the IRAP assessment to an acceptable standard as outlined in the IRAP assessment Reporting Guidelines. If the assessment is not improved to an acceptable standard, ASD may revoke the IRAP status of the assessment. This uplift process will be managed in line with the IRAP conflict resolution process.

37. Reasons for revocation of an IRAP assessment could include, but are not limited to:

    a. IRAP assessment does not meet the minimum standard of the IRAP Assessment Reporting Guidelines

    b. scope of IRAP assessment does not provide acceptable visibility of risk management for a system

    c. IRAP assessment evidence is unavailable or unacceptable, or

    d. an undeclared conflict of interest is identified with the IRAP assessor.

38. If received IRAP assessments are of consistently low quality or accuracy, or if the IRAP Administrator receives complaints relating to either behaviour or ability:

    a. ASD will inform the assessor in the first instance to address the matters, and

    b. reserves the right to revoke ASD’s endorsement of the individual as an IRAP assessor.

## IRAP assessment customers

39. A government agency or commercial organisation that is procuring an IRAP assessment should meet the following guidelines:

    a. Seek at least three (3) quotes from the list of available assessors at cyber.gov.au.

    b. Allow a reasonable timeframe to complete an IRAP assessment.

    c. Provide relevant documentation and evidence of technical configurations to the IRAP assessor in a timely manner.

    d. Understand potential conflicts of interest.

    e. Marketing information related to the IRAP assessment of a system must meet requirements outlined in the Marketing policy section, or the Branding Guidelines available on the IRAP website.

    f. If requested, make IRAP assessments and their supporting evidence available to ASD for quality assurance review.

    g. On completion of an IRAP assessment, complete the IRAP Assessment Feedback Form to assist in continually improving IRAP.

40. It is the responsibility of the IRAP assessor to ensure that the customer is aware of these guidelines.

## Conflicts of interest

41. IRAP assessors are often entrusted to sensitive information. Additionally, they may be responsible for contributing toward the information security of a Government entity. 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.

42. The following requirements exist in relation to declaring potential conflicts of interest:

a. Prior to endorsement by ASD, IRAP applicants must complete an IRAP conflict of interest declaration.

b. Upon engagement, IRAP assessors must send an IRAP conflict of interest declaration before undertaking each IRAP assessment, or as soon as they become apparent.

c. An IRAP assessment may not proceed if a related conflict of interest is under review by ASD.

43. ASD will respond to all conflict of interest declarations within 5 business days with either an acceptance of declaration or, a notification that further review and/or information is required relating to a declared conflict.

44. The conflict of interest declaration can be obtained from cyber.gov.au and declared to asd.irap@defence.gov.au.

45. Conflict of interest circumstances are those which affect an IRAP assessor's ability to perform their work or fulfil their responsibilities with impartiality. Circumstances that might influence the IRAP assessor's provision of services includes:

a. personal relationships

b. interests, or

c. corporate affiliations.

46. It is also considered a conflict of interest, should an IRAP assessment be performed on a system where the IRAP assessor, or another party (with a personal relationship, interest or corporate affiliation to the IRAP assessor) 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.

47. 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.

48. ASD takes any perceived or actual conflicts of interest seriously and will handle all declarations with sensitivity. ASD will review a sample of declarations to provide assurance that conflicts of interest are being managed appropriately, ethically and that the independence of the program is being maintained. No further action may be undertaken by the IRAP Assessor until the conflict of interest has been discussed and resolved with ASD.

49. The non-declaration of a conflict of interest reflects a poor compliance culture and is a breach of the conditions of IRAP membership, and may result in removal from the program. Conflicts of interest may also be declared by other parties involved with an IRAP assessment.

## Marketing

50. Ensuring references to IRAP are accurate is integral to the reputation and function of the program.

51. Government or commercial entities employing IRAP assessors may promote employee involvement in the program. IRAP Customers may also promote the completion of an IRAP assessment and the accompanying letter of completion. To assist guide IRAP assessors and industry:

    a. the approved ASD IRAP marketing copy is: 'IRAP assessed on <date> against <classification level> controls. A copy of the IRAP assessment is available from <client email>.'

    b. ASD IRAP logos are available to IRAP assessors via the IRAP secure portal.

52. Publishing statements referring to IRAP accreditation, certification, endorsement, registration or authorisation to operate will result in ASD requesting the removal or recall of marketing materials, or statements that improperly promote an association with IRAP.

53. The IRAP name and logo are owned by ASD and may only be used in material that meets the above requirements and adheres to the requirements detailed in the IRAP Branding Guidelines found on the ASD IRAP website under 'Toolkit'.

## IRAP training providers

54. Only training providers endorsed by ASD can provide IRAP training services. All ASD endorsed IRAP training providers are required to meet the following:

    a. achieve teaching IRAP learning objectives

    b. consult with ASD on all IRAP training course changes or updates

    c. provide adequate facilities for training, and

    d. incorporate any changes to course material as requested by ASD.

## Gateway Security – Commercial or Government

55. Gateway providers holding government information must document their implementation and effectiveness with the scoped ISM controls, the PSPF and the Australian Security Intelligence Organisation's (ASIO) T4 Physical Accreditation requirements.

56. A gateway provider must engage an IRAP Assessor to conduct an independent IRAP Assessment from the list of ASD endorsed IRAP Assessors which can be found at cyber.gov.au.

57. ASD must be informed when certification is being sought. ASD recommends gateway providers allow at least three (3) months for IRAP Assessment and certification activities to occur before certification.

58. Gateway providers must prepare all system documentation prior to an IRAP Assessment. The gateway providers may engage an IRAP Assessor to assist in the development of the documentation suite, however, the same Assessor cannot provide final IRAP Assessment services. To avoid conflicts of interests, all issues or concerns must be referred to ASD as soon as possible for clarification and approval.

59. A gateway providing services to multiple Australian Government agencies must be IRAP Assessed at least every 24 months.

60. The gateway provider will be expected to supply the IRAP Assessment Report on request to the respective government entities (or other customers) who are looking to procure their services.

61. ASD reserves the right to revoke an assessment and to inform gateway clients of security risks or concerns. Reasons for revocation could include, but are not limited to:

    a. the lapse of assessment expiration dates without consultation with IRAP Management

    b. the discovery that controls are not operating effectively

    c. inappropriate management of a cyber incident

    d. a change to location, architecture or design

    e. a change to the residual risk occurs or a new risk is introduced, or

    f. a new or emerging threat is identified.

62. For the list of ASD certified gateway services see: https://www.cyber.gov.au/acsc/view-all-content/programs/irap/asd-certified-gateways.

## Cloud Security – Commercial or Government

63. In accordance with the Australian Government Secure Cloud Strategy, entities are able to self-assess cloud service providers and cloud services using the risk-based approach to cyber security outlined in the ISM. Entities are strongly recommended to use the ACSC's guidance on cloud security when performing a security assessment to determine the suitability of a particular cloud service provider and its cloud services. The ISM recommends that cloud service providers and their cloud services undergo a security assessment by an IRAP assessor at least every 24 months.

## The Australian Signals Directorate’s responsibilities

64. The IRAP Administrator oversees the daily running, clearances and management of the program and provides advice, assistance and support to IRAP applicants, assessors, IRAP training providers, and Government and Commercial entities using IRAP assessment services.

65. Where possible, the IRAP Administrator 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.

66. ASD will respect the intellectual property created by IRAP assessors and will not share IRAP assessments outside ASD without the expressed consent of the report owner. ASD reserves the right to evaluate IRAP assessments and provide the assessor and assessed client with associated security advice and support. If an IRAP assessor’s report quality is consistently low, ASD reserves the right to revoke membership to the program.

67. ASD will not recommend any IRAP assessor to potential clients. As best practice ASD will recommend all clients seek at least three (3) quotes from the list of available assessors at cyber.gov.au

68. To support this process, ASD will maintain two lists of current IRAP assessors:

    a. available for potential clients, and

    b. engaged and unavailable for potential clients.

69. Assessors may request to move between the Available/Engaged list by contacting asd.irap@defence.gov.au

70. ASD reserves the right to make changes to IRAP at any time, including the administration of the program and the introduction of new membership requirements. ASD will inform all IRAP assessors of any changes as soon as possible and allow reasonable time for assessors to achieve the changed requirement(s).

## Conflict resolution process

71. Feedback in relation to the operation of IRAP is valued, and will be used to stimulate improvements, and address weakness in program or administration.

72. For formal complaints and disputes concerning IRAP or arising from the operation of IRAP shall be managed by the IRAP Administrator. The complainant should notify the IRAP Administrator in writing, with supporting evidence, via asd.irap@defence.gov.au

73. The IRAP Administrator will acknowledge the complainant on receipt of the formal notification, and the time frame for resolution will be agreed. Where the complaint concerns the activities of an IRAP assessor or their general competency, the assessor against whom the complaint has been made will be advised in writing from the IRAP Administrator of the allegations and will be requested to submit a response.

74. The IRAP Administrator will consider the factual issues, and consider options to resolve the complaint.

75. The IRAP Administrator will advise all parties of the resolution in writing. Should any party be dissatisfied with the resolution of a complaint, an appeal may be made to the First Assistant Director General Cyber Security Services who will arbitrate the complaint. Following an appeal, the decision of the First Assistant Director may be reviewed by the Inspector-General of Intelligence and Security (IGIS).

76. Complaints or disputes arising from commercial arrangements between 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.

## Related Legislation, Directives, Policies and Processes

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

## Getting Help

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

## Version History

| Version | Date | Comment |
|---|---|---|
| 1.0 | 2 Dec 2020 | |