Australian Government
Department of Defence

Australian Signals Directorate
Cyber and Information Security Division
Information Security Registered Assessors Program

Policy and Procedures
02/2017

irap

Contents

Information Security Registered Assessors Program 2

- Summary 2
- IRAP Overview 2
- IRAP Objectives 2

Policy and Procedures 2

- Roles 2
- Application 3
- Examination 3
- IRAP Membership 4
- IRAP Assessors 5
- Security Clearance 6
- Conflicts of Interest 6
- Marketing 7
- Training Providers 7
- Cloud and Gateway Security – Commercial or Government 8
- The Australian Signals Directorate's Responsibilities 8
- Conflict and Resolution Process 9
- IRAP Assessment Reporting Guidelines 9

Related Documents 10

IRAP Policy and Procedures | February 2017

IRAP Management Team

E asd.irap@defence.gov.au
W asd.gov.au/irap

Australian Signals Directorate

P 1300 CYBER1 (1300 292 371) and select 2 at any time
E asd.assist@defence.gov.au
W asd.gov.au/contact

Information Security Registered Assessors Program

Summary

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.

ASD endorses suitably qualified ICT professionals to provide relevant security services which aim to secure broader Industry and Australian Government information and associated systems.

IRAP Overview

ASD is the Commonwealth authority on information and cyber security with a mandate to provide technical advice and assistance to secure Australian Government information. 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.

IRAP is a defensive step towards improving the security of Australian Government information, including the ICT infrastructure storing, processing and communicating this information.

IRAP Objectives

IRAP provides the framework by which individuals are endorsed from across the private and public sectors to provide information security assessment services for use by, but not limited to, the Australian Government. Endorsed IRAP Assessors are engaged to provide an independent assessment of ICT security, suggest mitigations and highlight associated residual risk.

Policy and Procedures

Roles

IRAP enables the engagement of an IRAP Assessor by any commercial or government entity requesting ICT security assessment services . This policy applies to:

- IRAP applicants – An ICT professional who applies to ASD to be endorsed as an IRAP Assessor
- IRAP Assessors – An ICT professional endorsed by ASD through the IRAP application process to conduct independent security assessment services to the Australian Government. Also referred to as an IRAP member
- IRAP Training Providers – Organisations recognised by ASD as providing high quality training and/or technical qualifications meeting ASD requirements
- ASD IRAP Management – responsible for the administration and management of the program and available to provide advice and guidance on IRAP related issues.

Application

To be eligible to join IRAP, ASD must be satisfied that an IRAP applicant is an Australian citizen, has appropriate technical qualifications and expertise, and must confirm their identity. An IRAP applicant will need to provide original or certified true copies of these documents and meet the following additional requirements:

- A baseline security clearance (minimum). For further details on requirements please see the Australian Government Security Vetting Agency guidelines at *http://www.defence.gov.au/agsva/*
- A qualification from both Category A and Category B - appropriate evidence includes copies of course completion certificates and certificates of attainment, including relevant certification numbers

A	B
CISSP	CISA
CISM	PCI QSA
GSLC	CRISC
	ISO27001 Lead Auditor
	GSNA

- Five (5) years of technical ICT experience with at least two (2) years of information security experience. This must include experience with the application of the *Australian Government Information Security Manual* (ISM) and supporting publications on government systems.
- Contact details of two current and relevant professional referees who can attest to the applicant's ICT and/or auditing experience, character and competence. Please let your referees know to expect a call from ASD. If we cannot make contact with your referees, be prepared to provide us with alternative options
- Proof of Australian citizenship as evidenced through a baseline security clearance.

In order for applications to be processed by ASD, IRAP applicants must:

- Submit an IRAP application form which can be found on the ASD IRAP website
- Ensure all supporting documentation is complete and accurate
- Have been granted their baseline security clearance
- Allow 10 business days for ASD to begin processing the application.

Once ASD has reviewed the application for the above criteria, suitably qualified applicants will be provided with a registration number. This registration number will be required to enrol in an IRAP New Starter Training course with an ASD endorsed IRAP Training Provider. As part of the training process, an IRAP examination will be administered.

Applicants must not identify themselves as IRAP Assessors until the training and examination have been successfully completed. Once ASD officially endorses an applicant, they will be notified in writing and their name will appear on the IRAP Website's list of IRAP Assessors.

Examination

ASD performs all administration and maintains full control over the IRAP examination. The examination consists of scenario based multiple-choice and 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 annually to reflect changes in government policy, the cyber threat landscape and ASD expectations.

ASD 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.

If an applicant does not obtain a pass mark of 80%, the applicant may re-attempt the IRAP examination at no additional cost 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, but will be at full cost to the applicant, and subject to Training Provider approval. 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.

If an applicant fails the IRAP examination twice, they must re-apply for entry into the program. Applicants must wait at least 12 months 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.

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

IRAP Membership

IRAP Assessors must demonstrate a strong understanding of ICT, information security and auditing practices, with a special focus toward their application in an Australian Government context. This is achieved through a combination of professionally recognised ICT and auditing qualifications, relevant professional experience, tailored IRAP training by ASD endorsed IRAP Training Providers and the successful completion of the IRAP examination.

IRAP applicants will be recognised as IRAP Assessors on successful completion of the IRAP application process, training and examination. ASD will confirm successful IRAP membership with the IRAP applicant.

Successful applicants become registered IRAP Assessors with their details published at *http://www.asd.gov.au/irap/assessors.htm*.

IRAP Assessors are required to undertake Mandatory Annual Training (MAT) in line with the annual publication of the ISM. Failure to complete MAT will result in the suspension of an Assessor's membership for a period determined by ASD. IRAP Assessors must also maintain all pre-requisite professional qualifications.

An IRAP Assessor will forfeit IRAP membership should they fail to pay for training received by endorsed IRAP Training Providers. No financial compensation will be provided for costs incurred by an IRAP applicant or Assessor related to IRAP Membership.

As a member of the program, all IRAP Assessors will:

- Maintain pre-requisite professional qualifications as identified in Category A and B of the application process
- Maintain all held security clearance requirements
- Adhere to the IRAP Policy and Procedures and behave professionally and ethically when representing ASD
- Undertake all IRAP-related training as directed by ASD, including MAT
- Complete all IRAP Assessments within three months of engagement unless an extension is granted by ASD
- Produce factually accurate IRAP Assessment reports in line with ASD IRAP Assessment Reporting Guide. ASD reserves the right to request and receive any reporting generated under the program. If received IRAP Assessment reports are of consistently low quality or accuracy, or if ASD receives complaints relating to either behaviour or ability, ASD will inform the Assessor in the first instance, but reserves the right to remove the Assessor from the program.
- Provide email notification of all IRAP engagement via the ASD IRAP website community feedback form (or directly via *asd.irap@defence.gov.au*)
- Maintain an understanding of government advice and policy through IRAP communications and the ASD OnSecure portal
- Contribute to the IRAP community via events, forums, workshops and general correspondence
- Inform ASD IRAP Management if any conflicts arise relating to the program as soon as possible
- Appropriately secure all information and electronic devices used in IRAP services to a standard associated with the risk of aggregated government data, in accordance with ASD information security policy and guidance.

Failure to comply with membership conditions could result in the revocation of IRAP membership as deemed appropriate.

ASD reserves the right to conduct ad-hoc audits of all IRAP related work and to overturn an IRAP Assessor's recommendations. In this event, ASD will consult the IRAP Assessor involved and provide detailed reasoning for the decision.

Membership requirements will be reviewed annually, or as required, 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.

IRAP Assessors

IRAP Assessors are endorsed by ASD to conduct independent assessments of any system, network and gateway, for compliance with the ISM, *Australian Government Protective Security Policy Framework* (PSPF) and other Australian Government guidance. The IRAP Assessor will conduct an independent assessment as described in the *Conducting Audits* chapter of the ISM.

Stage One and Stage Two audits will include, but will not be limited to, the following activities:

- Informing IRAP Management of any and all IRAP work being undertaken
- Full system documentation review
- Onsite inspection
- Interview(s) with key staff, including system owners, operations staff and stakeholders
- Evidence gathering to confirm effectiveness of security controls.

For further information please see the *Conducting Accreditations* chapter of the ISM.

IRAP Assessors will not award certification or accreditation of any ICT system. For information on system certification authorities please consult the *Conducting Certifications* chapter of the ISM.

IRAP Assessors are also endorsed to provide ICT assessment services and advice relating to Fedlink connections and Gatekeeper networks.

Security Clearance

IRAP Assessors must hold a baseline security clearance prior to applying for entry into the program. The minimum clearance to be held by the Assessor must be equivalent to the classification of the system which is being assessed. IRAP Assessors engaged by agencies to conduct an assessment of a system at a higher classified level than the clearance held must gain sponsorship from the engaging agency to undergo the relevant security process. This higher clearance must be granted and held prior to gaining access to the system.

The provision of initial baseline security clearances prior to entry into the IRAP program is not managed by ASD and must be arranged between the government agency requiring the engagement and the respective IRAP Assessor. ASD may only take over clearance sponsorship for an existing IRAP Assessor. The IRAP program assumes that an IRAP applicant already has existing familiarity and experience with government agencies, policies, systems and the ISM. IRAP applicants and Assessors will be required to apply for their own work and clearance sponsor within government.

For further details see the Australian Government Security Vetting Agency guidelines at: *www.defence.gov.au/agsva/*.

Conflicts of Interest

IRAP Assessors are often entrusted to sensitive information and public resources. Additionally, they may be responsible for contributing toward the information security of an Australian Government entity. It is therefore critical that ASD is aware of any perceived or actual conflicts of interest to enable ASD to maintain a high level of confidence and trust in IRAP Assessors, and to assist in ensuring that Australian Government systems are appropriately secured.

A conflict of interest involves circumstances which may affect an IRAP Assessor's ability to perform their work or fulfill their responsibilities with impartiality. These circumstances might include personal relationships, interests or corporate affiliations that might influence the IRAP Assessor's provision of services. An actual or real conflict of interest exists between current official IRAP Assessor duties and existing private interests or corporate affiliations. Perceived or apparent conflicts of interest exist when external parties might suspect that private interests or corporate affiliations are influencing an IRAP Assessor, regardless of whether or not this is actually the case.

It is considered a conflict of interest if an IRAP Assessment is being performed on a system under influence by the IRAP Assessor directly, or by another party with a strong relationship to the IRAP Assessor. This influence includes but is not limited to the development, ownership or update of system components, documentation, mitigation advice or implementation guidance. This conflict of interest exists regardless of separate reporting structures, differences in physical location and the point in time in which the work is undertaken. This includes in 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. Australian Government agencies 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.

ASD takes any perceived or actual conflicts of interest seriously and will handle all declarations with sensitivity. It is a requirement that all IRAP Assessors declare to ASD any potential conflicts of interest as soon as they become apparent. No further action may be undertaken by the IRAP Assessor until the issue has been discussed and resolved with ASD. The non-declaration of a conflict of interest 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. ASD encourages Australian Government agency staff, industry partners or service providers to declare and discuss conflicts of interest with ASD as soon as they become apparent. Conflicts of interest can be declared by sending an email to *asd.irap@defence.gov.au.*

Marketing

IRAP membership is restricted to individuals. Employers of IRAP Assessors must not advertise their organisation as 'IRAP accredited, certified, endorsed, or registered'. Employers of IRAP Assessors may promote employee involvement in the program. The approved ASD IRAP logos are avaialble on request from ASD IRAP Management for use on promotional material.

Specific marketing or advertising material relating to IRAP and IRAP Assessors should be approved by ASD IRAP Management before publication or presentation. ASD will request the removal or recall of marketing materials referencing IRAP without approval from ASD.

For further guidance please refer to the *IRAP Branding Guidelines* found on the ASD IRAP website under 'Toolkit'.

Training Providers

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

- ASD learning objectives
- Consult with ASD on all IRAP training course changes or updates (including pricing changes)
- Provide a facilitator who has IRAP experience and been approved by ASD
- Provide adequate facilities for training
- Incorporate any changes to course material as requested by ASD.

Staff of IRAP Training Providers may complete the IRAP New Starter Training with the employer without a conflict of interest. This is achieved by ASD developing and facilitating the IRAP examination in isolation from the Training Provider(s). This removes any perceived or actual conflict of interest involving Training Provider staff having or gaining an unfair advantage over other applicants. IRAP Training Providers must advise ASD IRAP Management of all training candidates prior to commencement of training.

Cloud and Gateway Security – Commercial or Government

Cloud and gateway providers holding government information must document their compliance with scoped ISM controls, the Attorney-General's Department's PSPF and the Australian Security Intelligence Organisation's (ASIO) T4 Physical Accreditation requirements.

A cloud or 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 *http://www.asd.gov.au/irap/assessors.htm.* ASD must be informed when certification is being sought. ASD recommends cloud and gateway providers allow at least three (3) months for IRAP Assessment and certification activities to occur before certification.

Cloud and gateway providers must prepare all system documentation prior to a Stage 1 Audit commencement as required by the ISM (refer to the *Conducting Audits* chapter in the ISM). The cloud or 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 IRAP Management as soon as possible for clarification and approval.

A gateway providing services to multiple Australian Government agencies must be IRAP assessed and ASD certified annually. Cloud service providers must be assessed and certified every two (2) years. ASD will act as the Certification Authority (CA) (refer to the Conducting Certifications chapter in the ISM). All ASD Certified cloud services and gateways will be listed on the IRAP website unless deemed inappropriate by ASD.

ASD, as the CA, will review the scope of assessment, IRAP Assessment, compliance of controls, residual risks and mitigations, and award certification (if appropriate), in consultation with the provider and the IRAP Assessor. The outcome is a Certification Letter and accompanying Certification Report.

The cloud or gateway provider will be expected to supply the ASD Certification Report on request to the respective government agencies (or other customers) who are looking to procure their services. For details on Accreditation see the ISM Chapter Conducting Accreditation.

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

- The lapse of certification expiration dates without consultation with ASD IRAP Management
- The discovery that controls are not operating effectively
- Inappropriate management of a cyber incident
- A change to gateway location, architecture or design
- A change to the residual risk occurs or a new risk is introduced
- A new or emerging threat to the gateway is identified.

For the list of ASD certified cloud and gateway services see *http://www.asd.gov.au/irap/certified_services.htm.*

The Australian Signals Directorate's Responsibilities

ASD oversees the daily running 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.

Where possible, ASD 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.

ASD will respect the intellectual property created by IRAP Assessors and will not share IRAP Assessment reports outside ASD without the expressed consent of the report owner. ASD reserves the right to evaluate IRAP Assessment reports 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.

ASD IRAP Management 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 ASD endorsed IRAP Assessors.

ASD reserves the right to make changes to IRAP at any time, including 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.

Conflict and Resolution Process

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

ASD IRAP Management will contact the complainant on receipt of the formal notification, and the time frame for resolution will be agreed. Where the complaint concerns the activities of another IRAP Assessor or their general competency, the Assessor against whom the complaint has been made will be advised in writing from ASD IRAP Management of the allegations and will be requested to submit a response.

ASD 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 Assistant Secretary Cyber Security (ASCS), who will arbitrate the complaint. Following an appeal, the decision of the Assistant Secretary Cyber Security is final.

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 contract or payment disputes between Australian Government agencies and IRAP Assessors.

IRAP Assessment Reporting Guidelines

ASD expects all IRAP Assessors to provide quality services to clients. All IRAP Assessment reports are expected to uphold the quality outlined in the *IRAP Assessment Reporting Guidelines.*

ASD will accept respective company marketing and templates provided they contain the information above.

If reports do not meet these guidelines, reports will be returned to the IRAP Assessor for resubmission. ASD has the right to request additional information regarding the Assessment and retains the right to audit the Assessment and evidence collected. ASD will provide feedback to the author on request.

Related Documents

- *Australian Government Protective Security Policy Framework* (PSPF)
- *Australian Government Information Security Manual* (ISM)

asd.gov.au/irap