IRAP Exam Guidance

08/2021

Australian Signals Directorate
Infosec Registered Assessors Program

Information Security Registered Assessors Program Exam Guidance

The Information Security Registered Assessors Program (IRAP) examination is not a learning exercise. It is a test designed to support an application for endorsement and verifies your judgment, reasoning and ability to make assessments and recommendations for improving information security. This will be based upon your existing knowledge of general information security principles, IRAP processes and procedures, and relevant Australian Government policy and information security guidelines with a focus on the *Australian Government Information Security Manual* (ISM), the *Protective Security Policy Framework* (PSPF) and other Australian Cyber Security Centre (ACSC) technical publications.

The IRAP New Starter Training reinforces core knowledge and expectations of applying the ISM and *IRAP Policy and Procedures*. The entry examination tests skill and experience expected of an IRAP assessor, and therefore requires extensive professional experience using the ISM to secure systems to pass.

Expected skills of an IRAP assessor

IRAP assessors are expected to have the following skills:

- understand and identify information security principles
- describe how information security principles can be integrated into ICT systems
- discuss ethical issues involved in providing information security services to Australian Government and Industry
- demonstrate the communication skills needed for requirements gathering, development and implementation of information security controls and their appropriate evaluation
- gather requirements for the process of implementing information security advice
- design information security advice
- demonstrate an ability to find applicable and relevant information security advice from ACSC and other applicable Australian Government publications when presented with a problem
- evaluate the implemention of security controls
- understand ICT risk management to be able to recognise and suggest remediation to potentially vulnerable situations
- explain how applying specific information security controls will benefit an organisation
- provide coherent and logical explanations as to why specific information security controls are recommended.

Examination overview

The examination is delivered through multiple choice questions. A mark of 80% is required to pass the IRAP examination.

Required Reading

- *IRAP Policy and Procedures*
- *Australian Government Information Security Manual*
- *Protective Security Policy Framework*
- ACSC technical publications

Examination process

Schedule

The entry examination is conducted on the final day of the IRAP New Starter Training.

An applicant should sit their examination at the prescribed time. Deferred examinations are not available.

Examination conditions

The entry examination is open book, hand-written and paper-based. Applicants must work individually without assistance from other parties, in order to answer the questions within the allotted time period of two (2) hours.

Applicants are permitted to use the internet and available resources in order to assist in developing their answers.

Examination submission

Examinations are to be submitted at the end of the allotted examination time directly to the ASD-endorsed training provider. ASD recognises that some applicants may require special examination adjustments to accommodate their circumstances, so they can complete their examination on the same basis as other applicants. ASD-endorsed training providers will contact the IRAP Administrator to request appropriate provisions.

No late or amended submissions will be accepted, nor will any extension be granted.

Marking

The IRAP entry examinations undergo a two-person review process by ASD personnel.

Returning examinations

As per *IRAP Policy and Procedures*, no examinations will be returned to applicants, and no formal feedback will be provided.

Notification of results

Examination results will be released by the ASD-endorsed training provider within thirty (30) days. Results are released directly to applicants via email or over the telephone with the contact details provided at the time of the examination.

Results are released as either a Pass or Fail grade only and are regarded as final. Results will not be published on the ACSC IRAP website. Results are valid for 12 months.

Supplementary examinations

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.

Alternate examinations will be issued to applicants who are re-sitting the IRAP entry examination after a failed attempt. Supplementary examinations will be different in content from the previous examination.

Examination tips

The following tips may be helpful when answering exam questions:

1. Read the questions carefully, paying attention to key words within the question.
2. Avoid making additional assumptions about the question or its context.
3. Select the best answer based only on the information provided.

Sample Questions

1. Which cyber security principle does attack surface reduction relate to? (Select one answer)

   a. Govern

   b. Protect

   c. Detect

   d. Respond

2. Where would you find tailored configuration guidance for vendor-specific mobile platforms? (Select one answer)

   a. The ISM

   b. The Essential Eight

   c. The ACSC's Security Configuration Guides

   d. The Strategies to Mitigate Security Incidents

3. IRAP assessors are endorsed to perform IRAP assessments of TOP SECRET systems (Select one answer)

   a. True

   b. False

4. IRAP assessors can authorise systems to operate (Select one answer)

   a. True

   b. False

5. IRAP assessors assisting in the development of system security documentation can also assess that documentation as part of an IRAP assessment (Select one answer)

   a. True

   b. False

6. An organisation using TLSv1.2 would be marked as 'effective' in an IRAP assessment (Select one answer)

   a. True

   b. False

7. When assessing control 0298, you find that an organisation uses a centralised and managed approach to patch applications but not drivers. In an IRAP report, which implementation status best reflects the finding? (Select one answer)

   a. Partially compliant

   b. Effective

   c. Ineffective

   d. Partially effective

   e. Not implemented

8. Which security control would best address a requirement for system integrity? (Select one answer)

   a. Privacy filters are applied to the screens of highly classified mobile devices.

   b. If data is signed, the signature is validated before the data is exported.

   c. Dynamically scaling resources due to a genuine spike in demand or a denial-of-service attack is tested as part of capacity planning processes.

9. Which category is security control 1438 attempting to address? (Select one answer)

   a. Confidentiality

   b. Integrity

   c. Availability

10. Which category is security control 0235 attempting to address? (Select one answer)

   a. Confidentiality

   b. Integrity

   c. Availability

Answers:

1:b	2:c	3:b	4:b	5:b
6:b	7:c	8:b	9:c	10:a

Getting Help

11. For further assistance regarding IRAP, please contact asd.irap@defence.gov.au.