Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

IRAP Course and Examination Guidance

InfoSec Registered Assessors Program

June 2025

Table of contents

Introduction

Notes for participants

The InfoSec Registered Assessors Program (IRAP) examination has been designed to test the collective skills and experience expected of an IRAP assessor.

Participants undertaking this course are required to have extensive professional experience of Australian Government Frameworks, such as the Australian Government Information Security Manual (ISM) and Protective Security Policy Framework (PSPF), to secure or assess systems. As such, participants should expect to draw on this experience to pass the exam and not rely solely on the knowledge gained though this course.

Overview

The IRAP examination is not a learning exercise and is not meant to teach participants to be an IRAP assessor. It is a test designed to support an application for endorsement and verifies a participant's judgement, reasoning and ability to make assessments and recommendations for improving information security. This will be based upon existing knowledge of general information security principles, work experience, IRAP processes and procedures, and relevant Australian Government policy and information security guidelines, with a focus on the ISM, the PSPF, and other Australian Signals Directorate (ASD) technical publications.

The IRAP training reinforces core knowledge and expectations around applying the ISM, *IRAP Policy and Procedures*, and the *IRAP Common Assessment Framework*.

Required reading

For examination purposes, where there is an incongruity between ASD publications and the course material, the publications should be considered the authoritative source, unless specified by the ASD-endorsed training provider or ASD IRAP.

To ensure the most success in passing the IRAP examination, course participants must be familiar with the following publications and documents. All publications are available on the internet on the cyber.gov.au website - Resources for business and government | Cyber.gov.au.

- IRAP Policy and Procedures
- IRAP Common Assessment Framework
- IRAP Consumer Guide
- Information Security Manual
- Protective Security Policy Framework
- Strategies to mitigate cybersecurity incidents | Cyber.gov.au
- Essential Eight | Cyber.gov.au

Expected skills of an IRAP assessor

IRAP assessors are expected to have the following skills and knowledge:

to understand:

- understand and identify information security principles
- understand and adhere to conflict of interest policies
- understand and apply the intent of the ISM to systems and services
- understand quality of evidence definitions and aim for the best evidence available for a given control
- understand ICT risk management to be able to recognise and suggest remediation, to potentially vulnerable situations.

to explain:

- 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
- explain how applying specific information security controls will benefit an organisation
- explain, coherently and logically, why specific information security controls are recommended
- evaluate the implementation of security controls.

to demonstrate:

- 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 ASD and other applicable Australian Government publications, when presented with a problem.
- demonstrate the technical skills and ability to conduct assessments in accordance with the methodologies and requirements outlined in the IRAP Common Assessment Framework.

Examination process

The IRAP examination is delivered through multiple-choice questions. There are two (2) categories of questions: IRAP, and ISM.

IRAP examination questions relate to the participant's understanding of the program and designated assessment methodologies. ISM questions relate to the participant's knowledge of applying and understanding the intent of a control.

An overall mark of 80% is required to pass the IRAP examination.

Schedule

The IRAP examination is conducted on the final day of the IRAP training course. Applicants are required to sit their examination at the time prescribed by the invigilator. Deferred examinations are not available.

Examination conditions

The IRAP examination is 'open book' format. Participants are allowed to use the internet and available resources to assist in determining the answers to questions. However, **participants must not share, disseminate, copy, discuss, send or take pictures of the exam or its questions**. Participants caught performing such actions will have their examination or application terminated.

Participants must work individually and without assistance from other parties while answering the questions within the allotted time of 2 hours and 30 minutes.

If participants legitimately require reasonable adjustment to the standard examination protocols, the ASD endorsed training provider will contact ASD IRAP to request the appropriate provisions.

Examination submission

Examinations are submitted directly to the ASD-endorsed training provider at the end of the allotted examination time. Late submissions will not be accepted.

Marking

The IRAP examination undergoes a two-stage marking process. In the first stage, the ASD-endorsed training provider will mark the exam. Upon completion of this initial assessment, the results will be sent to ASD IRAP for a stage-two final review.

As per the IRAP Policy and Procedures, examinations will not be returned to applicants and no formal feedback will be provided.

The IRAP examination marking structure includes the application of 'negative-marking' for questions that require the selection of multiple answers (denoted by the 'Select all that apply'). For each incorrect answer selected, participants will lose one mark; with an overall total of zero marks being the minimum possible score for the question. However, participants will not receive a negative mark for not selecting an answer.

Example: In the marking structure example below, C and D are correct, while all other options are incorrect. Total possible marks for this question is 2:

Negative Marking Example			
A. B. C. D. E.	A. B. C. D. E.	A. B. C. D. E.	A. B. C. D. E.
Only 1 correct answer is selected; therefore, the participant receives 1 mark out of a possible 2.	Both correct answers are selected; therefore, the participant receives the full 2 marks.	2 correct and 1 incorrect answers are selected; therefore, the participant receives 1 mark.	1 correct and 2 incorrect answers selected; therefore, the participant receives 0 marks.

Notification of results

Examination results will be released by the ASD-endorsed training provider within 30 days. Results are provided via email or telephone using the contact details provided at the time of the examination.

Final results are released as either a Pass or Fail grade. Results will not be published on the Cyber.gov.au IRAP website. Results are valid for 12 months. ASD IRAP manages any results appeal, as per the IRAP Policy and Procedures.

Supplementary examinations

Participants who do not meet the pass mark requirement of 80% may reattempt the IRAP examination after a waiting period of at least 4 months.

An alternative examination is issued to participants resitting the IRAP examination after a failed attempt. It is the responsibility of the participant to schedule an examination resit attempt, in consultation with the ASD-endorsed training provider.

Participants who fail the second examination attempt are required to wait for a period of at least 12 months before reapplying for the course. It is strongly recommended that participants having failed 2 attempts at the examination consider whether they meet the requirements of an IRAP assessor.

Examination tips

The following tips may be helpful when answering exam questions:

- Read the question carefully, paying attention to key words within the question.
- Avoid making additional assumptions about the question or its context.
- Select the best answer based only on the information provided.
- For multiple selection answers, only select the ones participants are sure of to avoid losing marks.

Practice questions

The following questions are examples only and do not appear on the actual IRAP examination. The following questions are aligned to the December 2024 version of the ISM.

Question 1: Which of the following publications defines controls and principles that can be implemented for systems and organisations (Select one)?

a) Information Security Manual (ISM).

b) Protective Security Policy Framework (PSPF).

c) IRAP Policy and Procedures.

d) Strategies to Mitigate Cybersecurity Incidents.

Question 2: The Protective Security Policy Framework (PSPF) defines which systems an IRAP assessor can assess. From the following options, select the systems that an IRAP assessor can assess (Select one).

a) SECRET Private in-house cloud systems.

b) PROTECTED Gateway systems.

c) PROTECTED Out-sourced cloud systems.

d) All of the above.

Question 3: To log into a corporate device, an organisation has implemented 10-character passphrases, accompanied by an SMS onetime code to a corporately owned mobile device. Which of the following controls was not implemented effectively (Select one)?

a) ISM-1559 Memorised secrets used for multi-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are a minimum of 6 characters.

b) ISM-0421 Passphrases used for single-factor authentication on non-classified, OFFICIAL: Sensitive and PROTECTED systems are at least 4 random words with a total minimum length of 15 characters.

c) ISM-1401 Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

d) ISM-1682 Multi-factor authentication used for authenticating users of systems is phishing-resistant.

Question 4: An IRAP assessor has been contracted to perform an IRAP assessment of a government department's ICT on-premises system. The developed report will be consumed internally only. Which of the following options BEST describes the assessment methodology to use (Select one)?

a) Because the IRAP assessment report will only be consumed by the government department, the IRAP assessor can use the government department's assessment methodologies.

b) Because the IRAP assessment report will only be consumed by the government department, the IRAP assessor can use their own assessment methodologies.

c) Regardless of whether it will be consumed internally only, the IRAP assessor will need to use the methodologies prescribed in the IRAP Common Assessment Framework.

d) None of the above.

Question 5: In accordance with the IRAP Policy and Procedures, an IRAP assessor must FIRST complete which activity before commencing an IRAP assessment (Select one)?

a) Send to the assessed entity a list of the documents, tools and accesses required to streamline the assessment process.

b) Sign a Non-Disclosure Agreement to ensure that the confidentiality of the assessment is protected.

c) Develop the IRAP Security assessment plan and provide a copy to ASD IRAP.

d) Submit a Conflict of Interest declaration to ASD IRAP.

Question 6: Which of the following options describes the responsibilities of an IRAP assessor (Select all that apply)?

a) Assessing systems against the ISM and determining the authorisation based on risks.

b) Advising their clients on the marketing of IRAP.

c) Determining how a system should be implemented to reduce security risks.

d) Defining the assessment and authorisation boundary for an IRAP assessment.

e) Notifying ASD of any conflict-of-interest changes.

Question 7: Which of the following options is considered phishing-resistant authentication (Select one)?

a) Memorised secrets such as passphrases and passwords.

b) SMS one-time password authentication.

c) Mobile application receiving a challenge and response notification.

d) FIDO2 passkey.

Question 8: Which of the following options would be considered excellent evidence for an IRAP assessment (Select one)?

a) The IRAP assessor interviewed several organisational staff from different departments to understand how the system is designed and built.

b) With direct access to the system, the IRAP assessor ran a command to display the configuration settings.

c) During a workshop demonstration, the IRAP assessor requested that the administrator run through several tasks on the system in order to observe expected or unexpected results.

d) The IRAP assessor reviewed architecture documentation and then verified that the control was in place by requesting, from the administrator, screenshots of the system and its configuration.

Question 9: Which of the following options would be most effective in temporarily disabling Internet Explorer (Select one)?

a) Disabling Internet Explorer through group policy objects.

b) Blocking Internet Explorer through Application Control policies.

c) Uninstalling Internet Explorer completely.

d) Removing the Internet Explorer icon.

Question 10: An Australian Government entity is using cloud services from a Cloud Service Provider and has requested that you determine who is responsible for implementing some controls. Who, from the following options, is responsible for ensuring that a Chief Information Security Officer is appointed to oversee cybersecurity for the organisation (Select all that apply)?

a) The Cloud Service Provider (CSP).

b) The Australian Government entity.

c) The IRAP assessor's company.

d) The cloud regulation authority.

e) ASD IRAP.

Answers

Question	Answer
Q1	a) Information Security Manual (ISM).
Q2	d) All of the above.
Q3	d) ISM-1682 Multi-factor authentication used for authenticating users of systems is phishing-resistant.
Q4	c) Regardless of whether it will be consumed internally only, the IRAP assessor will need to use the methodologies prescribed in the IRAP Common Assessment Framework.
Q5	d) Submit a Conflict of Interest declaration to ASD IRAP.
Q6	b) Advising their clients on the marketing of IRAP. e) Notifying ASD of any conflict-of-interest changes.
Q7	d) FIDO2 Passkey
Q8	c) During a workshop demonstration, the IRAP assessor requested that the administrator run through several tasks on the system in order to observe expected or unexpected results.
Q9	b) Blocking Internet Explorer through Application Control policies.
Q10	a) The Cloud Service Provider (CSP). b) The Australian Government entity.

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.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre