IRAP ENTRY EXAMINATION GUIDE

Australian Government
Department of Defence

IRAP Entry Examination Guide

The IRAP entry examination aims to assess your judgment, reasoning and ability to make 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.

The examination will provide applicants with the opportunity to demonstrate technical and theoretical approaches, methods and techniques to applying information security within an Australian Government context. This examination should complement an applicant's significant practical experience from previous professional experience.

The entry examination does not always directly reflect the accompanying IRAP New Starter Training, but instead assesses complementary skills expected of ASD endorsed IRAP Assessors.

Mode of Delivery	In person
Examination Type	Hand-written
Pre-requisites	• Fulfilment of all IRAP qualification criteria as listed on the ASD IRAP website • Approval for progression to IRAP New Starting training by the IRAP Management Team • Completion of the IRAP New Starter training run by an ASD endorsed Training provider • Thorough understanding of the IRAP Policy and Procedures
Required Materials	• Photo Identification • Black or blue pen
Recommended Materials	• Internet-connected device • Digital copies of ASD publications

Contact us

Examination contact: IRAP Management Team
Phone: 1300 CYBER1 (1300 292 371) and select 1 and then 4 at any time
Email: asd.irap@defence.gov.au

Examination Overview

Expected skills
In order to pass the examination, applicants must be able to:

- Describe and explain information security principles
- Gather requirements for, design and evaluate the process of implementing information security advice
- Demonstrate the communication skills needed for requirements gathering, development and implementation of information security controls and their appropriate evaluation
- Describe how information security principles can be integrated into an overall ICT system
- Explain how applying specific information security techniques will benefit an organisation
- Understand sufficient theory of information security and ICT auditing to be able to recognise and suggest remediation to potentially vulnerable situations
- Identify key information security design errors in simple scenarios and suggest alternative approaches
- Discuss ethical issues involved in providing information security services to Australian Government
- Provide coherent and logical explanations as to why specific information security approaches are recommended
- Demonstrate an ability to find applicable and relevant information security advice from ASD publications when presented with a problem.

Examination Summary

The examination will consist of a combination of multiple choice and short answer questions, totalling 100%.

Assessment Task	Value
Multiple Choice	30%
Short Answer	70%

Required Reading

- IRAP Policy and Procedures
- *The Australian Government Information Security Manual*
- *The Protective Security Policy Framework*
- ACSC Publications.

Examination Process

Schedule
The entry examination is conducted on the final day of the IRAP New Starter Training. Time and location varies between ASD endorsed training providers, however the examination will be conducted as part of the training process.

An applicant should sit their examination at the prescribed time. No deferred examinations are available.

Examination Conditions
The entry examination is hand-written and paper based. Applicants must work individually in order to answer the questions within the allotted time period of two (2) hours. An additional 10 minutes will be granted at the start to allow applicants to read through the contents of the examination.

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 present member of the IRAP Management Team.

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

Marking
The IRAP entry examinations undergo a blind two-person review process by ASD cyber security personnel. Marks are awarded based on merit and according to sample answers generated from ASD's public information security advice.

Answers that digress from ASD's published information security guidance will be accepted if the alternate solution is logical, coherent and sufficiently explained and justified.

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 Management Team 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 released to the IRAP New Starter Training providers nor will they be published on the ASD IRAP Website.

Supplementary examinations
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.

Sample Questions

Previous Examinations
ASD does not release past examination papers for use by new applicants.

Applicants may find the limited sample examination questions and example answers contained in this document to be a useful study or self-assessment tool when preparing for the IRAP entry examination. Applicants should be aware that while the sample questions are inspired by previous years, the examination papers change frequently and may bear no resemblance to the sample questions.

Practice Question 1	**1 Mark**
How can web services mitigate against SQL Injection?	

Practice Question 2	**1 Mark**
Network segmentation and segregation can be achieved through: A. The use of IPsec to filter ports requesting access to sensitive servers B. Utilising jump servers for administration on the network C. Implementing desktop virtualisation for environments allowing web browsing D. Integrating publicly available Wi-Fi with the corporate domain	

Practice Question 3	**2 Marks**
Describe how Sender Policy Framework (SPF) assists in preventing compromise of a system.	

Practice Question 4	**3 Marks**
Outline the requirements of a cyber security incident register.	

Practice Question 5	
A government agency is investigating their options as to how to implement application whitelisting across their corporate network; currently they have no solution in place. You have been consulted to provide advice.	
Part A	**2 Marks**
Provide a recommendation as to how this agency should prioritise the rollout of application whitelisting.	
Part B	**2 Marks**
Compare the advantages and disadvantages of whitelisting applications based on file path or file hash.	

Sample Answers

Please note that these sample answers provide only a rough indication as to the types of responses that would be marked correct. It is acknowledged that multiple answers may exist, and they will be marked accordingly provided the answer is clear and appropriately justified.

These answers should not provide an indication as to the depth or length of responses. Applicants are encouraged to provide as much detail as they see necessary in order to adequately express their response.

Practice Question 1 – Sample Answer **1 Mark**

How can web services mitigate against SQL Injection?

By implementing prepared statements (or parameterised queries).

Practice Question 2 – Sample Answer **1 Mark**

Network segmentation and segregation can be achieved through:

A. The use of IPsec to filter ports requesting access to sensitive servers

B. Utilising jump servers for administration on the network

C. Implementing desktop virtualisation for environments allowing web browsing

D. Integrating publicly available Wi-Fi with the corporate domain

Solutions A, B and C are correct.

Practice Question 3 – Sample Answer **2 Marks**

Describe how Sender Policy Framework (SPF) assists in preventing compromise of a system.

SPF verifies that an email message originates from an email server that is authorised to send emails from that domain. SPF assists in blocking spam emails that use spoofed email addresses. Preventing these from reaching the end user reduces the potential for phishing attacks that could result in compromise of a system through the execution of malware.

Practice Question 4 – Sample Answer **3 Marks**

Outline the requirements of a cyber security incident register.

At a minimum, a cyber security incident register should include:

- *Date of incident discovery*
- *Date of incident occurrence*
- *Description of the incident*
- *Description of personnel and locations involved*
- *What actions were taken*
- *To whom the incident was reported*
- *A file reference*