**IRAP ASSESSMENT REPORT**

**<ORGANISATION NAME>**

**<SYSTEM NAME>**

<Assessor Details>

Instruction: This template provides the content requirements of IRAP Assessment Reports (or security assessment reports as referred to within the Information Security Manual). Assessors can use their own report templates for branding purposes however all sections within this template must be included.
For cloud systems, use the *Cloud Security Assessment Report Template*.

**Delete this and all other instructions from your final version of your report, as well as all ACSC branding.**

# Document Details

### Assessment

|  |  |
| --- | --- |
| **ISM Version** | <Month YYYY> |
| **Control Classification** | Choose an item. |
| **System Definition** |  |
| **ACSC Report template version** | V0.1 |

Prepared by

|  |
| --- |
| **<Assessor Organisation Name>** |
| Shape  Description automatically generated with low confidence | **Address** |  |
| **Assessor Name** |  |
| **Assessor Qualifications** |  |
| **Contact Email** |  |

Prepared for

|  |
| --- |
| **<Organisation Name>** |
| Shape  Description automatically generated with low confidence | **Address** |  |
| **Contact Name** |  |
| **Contact Email** |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** |
| vX.X | DD/MM/YYYY |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

1. Executive Summary 4

2. Introduction 5

 **2.1. Background** **5**

 2.1.1. Logical System Diagram **5**

3. Assessment Details 6

 3.1. Methodology 6

 3.2. Scope 6

 3.2.1. Exclusions **6**

4. System Overview 7

 4.1. Strengths and Weaknesses 7

 4.2. Governance 7

 4.3. Environments 10

 4.3.1. Administrative and Support Environments **10**

 4.3.2. Test, Development, Production Environments (where applicable) 12

5. Detailed Findings 17

 5.1. Assessment of ISM Guidelines 17

Annex: Supporting Information 17

Annex: Controls Matrix 17

Attachment A: Security Controls Matrix 17

# Executive Summary

Instruction:

* Brief summary of the system and the scope of the assessment.
* Summary of the security strengths and weaknesses of the system, with key considerations clearly
stated in a concise manner.
* Should include all ineffective Information Security Manual (ISM) controls, with recommendations
where appropriate.
* Any further additional concerns should be highlighted.
* State the:

– ISM version

– Assessment classification level

– Key dates of the assessment

– If applicable, reassessment timeframe for security assessment (as per the ISM)

– Security risks associated with the operation of the system

# Introduction

### Background

Instruction:

The background should describe all system environment details, including the design, operation, name
of key facilities and locations.

The customers and users of the system environment should also be identified in order to help define associated risks, however, only when appropriate for the given environment’ IRAP assessment details
also need to be included, such as:

* Key dates of the assessment;
* ISM version;
* Previous security assessment issues or ongoing recommendations;
* Maximum classification that the environment was assessed against.

**2.1.1. Logical System Diagram**

Instruction: The logical diagram should show the authorisation boundary, and logical relationship between all system components assessed, as well as the link to any outsourced system dependencies, the administrative and customer support environments, and system consumer access.



# Assessment Details

Instruction:
Detail the methodology used to assess the system in line with the **Australian Government Information Security Manual (ISM), Protective Security Policy Framework (PSPF) and IRAP Assessment Process Guide**.

### Methodology

### Scope

Instruction:
Identify the specific systems within the environment under assessment. If particular environments such
as the corporate environment or service provider environment are deemed out-of-scope, provide the justification for their exclusion from the assessment. Detail any assumptions or constraints.

**3.2.1. Exclusions**

Instruction:
List any systems or ISM chapters or sections that are not included in this assessment scope, and a justification for their exclusion. Where there is no visibility into an underlying subsystem or process,
this should be noted.

# System Overview

###  Strengths and Weaknesses

Instruction:

Capture any high-level strengths, weaknesses and risks associated with the system, as well as recommendations for remediation as appropriate. Controls should be grouped where there is a single underlying risk behind them.

Should include the security posture of any underlying systems or processes.

If appropriate, you may wish to comment on organisation’s security culture.

List any other applicable information security compliance certifications. A note should be made where these certifications cover a different scope to the IRAP assessment such as different set of system components, regions or customer base.

###  Governance

Instruction:
For each of the following topics, describe the organisation’s approach to implementing robust,
secure practices.

4.2.2.1. Enterprise & Risk Management

Instruction:
Describe the organisation's enterprise risk management framework/s to manage strategic and
operational risks.

4.2.1.2. Personnel Security

Instruction:
Describe the organisation’s practices for managing personnel security, including personnel vetting, training and awareness practices, and whether personnel are entirely the organisation’s staff, or whether sub-contractors are used. Detail whether these practices vary by teams such as administrative or support staff. Also include whether staff hold current Australian Government Security Clearances, and if so,
which groups of staff, and what level of clearance is held.

4.2.1.3. ICT Change Management

Instruction:
Detail how the organisation manages ICT change, how system consumers are notified of these changes, and the possible implications of change on the security of the system. For example, where a system’s security posture is affected by a critical operating system update, assess the processes used to make decisions about if or when to apply an update, and the communications processes and mediums used
to advise system consumers of associated changes.

4.2.1.4. Data Type Definitions

Instruction:
Detail and define the different data types used by the organisation including system consumer-owned data and organisation-owned data. Include definitions that provide details of data kept on system consumers such as tag names, resource group names, subscription names, payment data and associated information. Define the data types that are appropriate to store sensitive or classified data based on this security, and whether the system consumer retains full ownership and control of each type. Security guidance may be necessary for data owned and stored by the organisation that the system consumer
may consider sensitive or classified. Include details on the data types that may have Privacy Act (1988)
& Australian Privacy Principles protections implications.

4.2.1.5. Data Protections

Instruction:
With reference to the above data type definitions, detail the procedural and cryptographic protections afforded to each data type, including the conditions under which each data type may be accessed by an entity other than the system consumer. Identify if the organisation treats system consumer data differently when encrypted.

Identify how Public Key Infrastructure (PKI) material is used and accounted for, and who has the ability to decrypt data, and in what circumstances this will occur. This may include technical support, “break glass” scenarios, or lawful requests for data by governments.

4.2.1.6. Data Deprovisioning and Disposal

Instruction:With reference to the above data type definitions, describe how the organisation destroys system consumer data and metadata once the system or resource is no longer used. Describe the validation that occurs to ensure all copies of system consumer data are deleted when the system is no longer in use. Describe any data or metadata retention policies. Examples for consideration: Does the organisation retain copies of system consumer data for 30 days after the system consumer flags it for deletion?
Can the system consumer delete data in the event of a data spill? What data is retained, and for
what timeframe, after a system consumer deletes their account?

4.2.1.7. Supply Chain Risk Management

Instruction:Detail the organisation’s practices relating to their supply chain risk management processes, such as when procuring and outsourcing functions. The scope of the supply chain includes the design, manufacture, delivery, deployment, validation, support and decommissioning of hardware, software and related services that are used within a system.

4.2.1.8. Vulnerability Management

Instruction:
Describe the organisation’s policies and processes for vulnerability disclosure reporting, vulnerability management and transparency. Consider the perspectives of vendors, independent third parties,
internal staff, system consumers, and the general public.

4.2.1.9. Incident Response

Instruction:
Describe the organisation’s processes and procedures for Incident Response, where roles, responsibilities, actions and visibility are described in more granular detail than organisation-wide policies, and how the response plan is tested. Identify how the system consumer is notified of relevant security incidents,
and consumer specific functions or activities are required under the Shared Responsibility model.

4.2.1.10. Secure Development Lifecycle

Instruction:Describe the organisation’s processes that embed security throughout the system lifecycle (through manual or automated), that contributes to defence in depth, secure by design, and operational security outcomes. Include details on how the organisation defines security objectives and uses threat modelling to define security objectives during different phases of the lifecycle.

4.2.1.11. Support Model

Instruction:
Detail the model used for support of the system, including support availability times by region, and the location of support staff for Australian system consumers. For example, identify the location of staff that provide level 1, 2, and 3 support in a “follow the sun” support model.

###  Environments

4.3.1 Administrative and Support Environments

Instruction:
Using the ISM, provide an assessment of the environments used to administer and support the system. This includes the location of devices which can be used to directly or indirectly access the production environment for system administration purposes, and for customer support.

4.3.1.1. Administrative and Support System Overview

Instruction:
Describe the scope of this system. Particularly whether the general corporate network is used to administer or support the system, and is therefore in scope, or whether dedicated administrative and support environments are used, and the wider corporate network has been excluded from the assessment scope. This may be aided by an architecture diagram or reference to other diagrams in this document.

4.3.1.2. Physical Security

Instruction:
Provide details of the physical security of the administrative and support offices.

4.3.1.3. Segmentation and Segregation

Instruction:
Detail the security of the administrative and support segmentation and segregation, including
network zones.

4.3.1.4. System Hardening

Instruction:
Detail the system hardening (and, if applicable, enterprise mobility) for devices used to administer
or support the system.

4.3.1.5. Secure Administration

Instruction:
Describe the process used by privileged users of the organisation to access and administer the system. Identify the different levels of privileged access for different teams and tasks, the methods of privileged access management such as just-in-time access, the appropriate restriction of administrative privileges and separation of privileged users. Detail the elements and relevant contextual information of secure administration, including security controls used to detect unauthorised actions within the management systems used by the organisation. This section should include supporting systems used by the system consumer to manage their account and perform their role under the shared responsibility model.

4.3.1.6. System Security Shared Responsibility Model

Instruction:
Define which entity is responsible for each security layer of the system. The below table should be used
as a guide, though may be adapted to the layers described in the organisation’s own model if needed. Regardless, backups and incident response should be explicitly mentioned. A yes/no response can be provided, or additional text if appropriate.

|  |  |
| --- | --- |
| **Layer** | **Responsibility** |
| **<Outsourced Provider Name> (if applicable)** | **<Organisation Name>** | **System Consumer** |
| **Governance** |
| **Incident Response** | Choose an item. | Choose an item. | Choose an item. |
| **Backups** | Choose an item. | Choose an item. | Choose an item. |
| **Technical** |
| **Data** | Choose an item. | Choose an item. | Choose an item. |
| **Identity & Access Management** | Choose an item. | Choose an item. | Choose an item. |
| **Application**  | Choose an item. | Choose an item. | Choose an item. |
| **Platform**  | Choose an item. | Choose an item. | Choose an item. |
| **Virtualisation**  | Choose an item. | Choose an item. | Choose an item. |
| **Physical Hosts** | Choose an item. | Choose an item. | Choose an item. |
| **Physical Networking** | Choose an item. | Choose an item. | Choose an item. |
| **Physical Datacentre** | Choose an item. | Choose an item. | Choose an item. |

4.3.1.7. Key Findings

Instruction:
Capture any high-level strengths, weaknesses, and risks associated with the organisation’s administration of the system, as well as recommendations for remediation or system consumer implementation as appropriate. Controls should be grouped where there is a single underlying risk behind them. This should include the security posture of any underlying systems or processes. Where the organisation has no visibility into an underlying infrastructure or process, this should be noted.

*Alternate Security Controls*

Instruction:
Detail any controls assessed as “Alternate Control” in the control matrix. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a descript-tion of any identified vulnerabilities where a specific ISM control requirement has not been met, and details of the alternate control implemented by the organisation to otherwise meet the control objective. Alternate controls are those which meet an ISM control objective through an alternate implementation
or manage the risk that meets or exceeds the control objective, but not the specific wording.

| **Control Number(s)** | **Description** | **Description of Alternate Control** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

*Security Controls Not Implemented due to Business Decision*

Instruction:
Detail any controls assessed as “Not Implemented” in the control matrix for the administrative and support environments, where the organisation has decided to retain this implementation due to business decision. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the ISM control objective, and a rationale for remaining unaligned with the control objective. This can also detail any factors relating to
the environment which may partially mitigate this risk.

| **Control Number(s)** | **Description** | **Operational Requirements Rationaleand Mitigating Factors** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

*Security Controls Requiring Remediation*

Instruction:
Detail any controls assessed as “Not Implemented” or “Ineffective” in the control matrix for the administrative and support environments, where the organisation is seeking to remediate this risk following the security assessment. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the
ISM control objective, a recommended remediation by the security assessor or planned implementation by the organisation, as well as an expected date for remediation.

| **Control Number(s)** | **Description** | **Recommended Remediation** | **Expected Remediation Date** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

4.3.2. Test, Development, Production Environments (where applicable)

Instruction:
Using the ISM, provide an assessment of the common security controls used to support the system.
This includes common hardware infrastructure, elements of the control plane(s) and other common elements supporting the system including jump boxes or privileged access systems.

4.3.2.1. Network Security

Instruction:
Detail the network topology and security of the system’s production network, focusing on network
seg-mentation, separation, and access control features. The topology description should include
the links to telecommunications/internet providers, and any dedicated links that are available
to system consumers.

4.3.2.2. Decommissioning Hardware

Instruction:
Detail the organisation’s practices for decommissioning, sanitising, and disposing of production ICT equipment and media. Detail how the organisation mitigates the risk of system consumer information being leaked in the event of hardware failures, such as a drive failure.

4.3.2.3. Security Operations and Monitoring

Instruction:
Detail the organisation’s security operations and monitoring practices including event logging and analysis, vulnerability scanning, and penetration testing.

4.3.2.4. Cryptography and Key Management

Instruction:
Identify the use and management of cryptographic keys and associated hardware and software.
It includes their generation, registration, distribution, installation, usage, physical and logical protection, storage, access, recovery, and destruction. Document procedures used to identify appropriate standards when implementing cryptographic solutions. Identify the use cases for cryptography, such as identifying ISM requirements that need to be met for protecting data at rest, data in transit, or for hashing functions. Identify if the organisation has developed their own cryptographic implementations or is leveraging existing third party libraries. Identify if the cryptographic libraries have been assessed by a standards
body (e.g. Common Criteria / FIPS / ‘ISO/IEC 19790:2012’) and if they are configured to use ASD
Approved Cryptographic Protocols (AACPs) using ASD Approved Cryptographic Algorithms (AACAs). Identify when and how the organisation deprecates and decommissions standards no longer fit for purpose. Identify if the organisation uses Hardware Security Modules for key storage.

4.3.2.5. Data Transfers

Instruction:
Detail the procedures used to move data, including source code, binary files, and sensitive documentation into or out of the system infrastructure, including any content filtering, malware analysis or data integrity checks that are performed.

4.3.2.6. Identity and Access Management

Instruction:
Describe the Identity and Access Management models that are available to use by the organisation. Identify any special rules and vendor guidance related to root accounts (first account), Break Glass accounts, Multi-Factor Authentication, etc. Describe the shared responsibility model for any Role Based Access Control, Attribute Based Access Control, governance, and approval models (such as a multi-user approval process for high-risk activities). Describe service and API authentication and authorisation processes. Attaching vendor reference architecture and vendor produced security best practice documentation provided at the time of assessment may shorten the time it takes to capture this information.

4.3.2.7. Security Automation

Instruction:
Describe the processes used to automate security activities. For example, the organisation may automate functions relating to Security Information and Event Management (SIEM) integration, password rotation, vulnerability scanning, or code analysis.

4.3.2.8. Continuity and Availability

Instruction:
Detail the methods used to ensure system continuity and availability requirements, such as data replication and Distributed Denial of Service (DDoS) protections including responsive automated scaling
to mitigate the risk of a DDoS attack.

4.3.2.9. Key Findings

Instruction:
Capture any high-level strengths, weaknesses, and risks associated with the organisation’s administration, as well as recommendations for remediation or system consumer implementation as appropriate. Controls should be grouped where there is a single underlying risk behind them. This should include
the security posture of any underlying systems or processes. Where the organisation has no visibility
into an underlying infrastructure or process, this should be noted.

*Alternate Security Controls*

Instruction:
Detail any controls assessed as “Alternate Control” in the control matrix for the system. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of any identified vulnerabilities where a specific ISM control requirement has not been met, and details of the alternate control implemented by the organisation to otherwise meet the control objective.

| **Control Number(s)** | **Description** | **Description of Alternate Control** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

*Security Controls Not Implemented due to Business Decision*

Instruction:
Detail any controls assessed as “Not Implemented” in the control matrix for the system, where the organisation has decided to retain this implementation due to business decision. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the ISM control objective, and a rationale for remaining unaligned with the control objective. This can also detail any factors relating to the environment which may
partially mitigate this risk.

| **Control Number(s)** | **Description** | **Operational Requirements Rationaleand Mitigating Factors** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

*Security Controls Requiring Remediation*

Instruction:
Detail any controls assessed as “Not Implemented” or “Ineffective” in the control matrix for the system production environment, where the organisation is seeking to remediate this risk following the security assessment. Controls may be grouped as appropriate where there is a single underlying implementation factor. For each entry, provide a description of the misalignment with the ISM control objective, a recommended remediation by the security assessor or planned implementation by the organisation,
as well as an expected date for remediation.

| **ControlNumber(s)** | **Description** | **Recommended Remediation** | **Expected Remediation Date** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Detailed Findings

Instruction:
Detail the implementation of ISM controls against each applicable ISM chapter and section. Provide a
high level summary of the section’s controls implemented and their effectiveness. Don’t re-write the controls matrix (1–2 paragraphs max per section).
Detail:

* Ineffective control
* Alternate control
* Security controls not implemented due to business decision
* Security controls requiring remediation
* Outline any mitigation strategies for any residual risks. Don’t rate the risks.

### Assessment of ISM Guidelines

# Annex: Supporting Information

Instruction:
List all the necessary information associated with conducting the assessment.

# Annex: Controls Matrix

### Attachment A: Security Controls Matrix

Instruction:
Details on the Security Controls Matrix location. The Security Controls Matrix provides a listing of all
the ISM controls the organisation implements as well as the controls that are the system consumer’s responsibility, and any shared responsibilities.



**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.

**Copyright.**

© Commonwealth of Australia 2022.

With the exception of the Coat of Arms and where otherwise stated, all material
presented in this publication is provided under a Creative Commons Attribution
4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material
as set out in this document.



The details of the relevant licence conditions are available on the Creative
Commons website as is the full legal code for the CC BY 4.0 licence
 (www.creativecommons.org/licenses).

**Use of the Coat of Arms.**

The terms under which the Coat of Arms can be used are detailed
on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

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

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