Australian Government
Australian Signals Directorate

IRAP SECURITY ASSESSMENT REPORT

<ORGANISATION NAME>

<SYSTEM NAME>

IRAP Assessment Report

Instruction:

This template provides the content requirements of IRAP Assessment Reports. Assessors can use their own branding, however all sections within this template must be considered in the conduct of an assessment.

Assessors should remove or add sections relevant to their specific assessment, whether it is cloud, gateway, or on premises.

Delete this and all other pre-populated instructions from the final version of your report, along with all Australian Signals Directorate (ASD) branding.

Document Details

Assessment

ISM Version	<Month YYYY>
Control Classification	Choose an item.
Assessment Report number	<Assessment-######>
System Definition	
System Type	Choose an item.
ASD Report template version	V1.0 - 2025

All assessments must have an Assessment Report number.

Failure to submit a Conflict of Interest declaration may result in revocation of IRAP endorsement

Prepared by

<Assessor Organisation Name>		
	Address	
	Primary IRAP Assessor name & number	
	Assessor qualifications	
	Secondary IRAP assessors & number	
	Contact email	

Prepared for

<Organisation Name>		
	Address	
	Contact name	
	Contact email	

Reviewed by

Name	Date	Organisation / position

Approved by

IRAP Assessor/s	Assessed Entity delegate
Name	**Name**
Signature	**Signature**

Revision history

Version	Date	Description	Author
vX.X	DD/MM/YYYY		

Template history

Version	Date	Description	Author
0.1	07/2022	First release of ASD IRAP assessment report template	ASD IRAP
1.0	02/2025	Updated template to include more fields such as COI, consumer guidance and penetration testing.	ASD IRAP

Delete template history table after final version

Contents

1. Administrative details

1.1. Conflict of Interest

Instructions:

- Outline any conflict of interest details regarding the assessment, including perceived or actual conflicts, or state if there is no conflict.
- Describe how any conflict was managed.
- Attach to this section, any enclosed letter from the provider or client, which confirms their acceptance of any conflict.

1.2. Security assessment team

Position	Name	Qualification	Specialisation
E.g. Lead IRAP Assessor	*Joe Blogs*	*- CISM, CISA, IRAP*	*General*
E.g. Network assessor	*John smith*	*- CCNA, CCNP, CCIE*	*Networking*

2. Consumer guidance and responsibilities

Instructions:

- Outline key considerations that consumers of the service must be aware of, including marketing terminology restrictions.
- Any recommendations that would be useful for the consumer to consider during implementation i.e. ensuring certain services are enabled for better security

If the report is for a government entity and no other entity will be consuming the service, this section can be removed or altered for the specific entity.

3. Executive summary

Instruction:
- Brief summary of the system and the scope of the assessment.
- 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.

3.1. Strengths and weaknesses

Instruction:
- Summary of the security strengths and weaknesses of the system, with key considerations clearly stated in a concise manner.

4. Introduction

4.1. 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. Whenever 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.

4.2. Cloud Service Provider

Instruction:
Provide a one to two page high-level introduction to the Cloud Service Provider, including:

- The ownership of the CSP;
- The locality of the CSP;
- Where its cloud services are provided from;
- Whether there is any potential extrajudicial control and interference over a CSP by a foreign entity;
- Where the CSP's personnel, such as support and administration, is located; and
- The ownership of the CSP.

4.3. Cloud Service Platform

4.3.1 Overview

Instruction:
Provide a high-level overview of the Cloud Service platform, outlining:

- The services provided i.e. IaaS, PaaS, SaaS
- Access to the Cloud Service Platform
- What the Cloud Service Platform is built on i.e hypervisor or on other cloud services.
- Any other supporting infrastructure

5. System details

5.1. System boundary

Instruction:
Identify the specific systems within the environment. Include: supporting systems, ingress / egress points, devices and security appliances, and Services functions.

5.1.1 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.

5.2. Dependencies and Inheritance

Instruction:
List any external systems', services, or applications (including client software) on which this service platform is dependent ('dependencies') - either owned by the assessed entity, or other providers. Dependencies may implement controls that the cloud service platform relies on. Specify if these dependencies have previously been assessed against the ISM, and if access to the assessment was provided.
Note any inheritance of ISM controls, the implementation of any configuration guidance the dependency source has provided, and any variation made by the service that may impact inherited controls.
Lastly, include whether the security of the external dependencies are in scope of this assessment.

Provider	<e.g. IaaSProvider / Managed service Provider>
Services Used	<e.g. IaaSService, AuthService>
Data Locality Used	<e.g. AUS-Southeast-A>
IRAP Assessed	<e.g. IaaSProvider has an existing IRAP assessment issued 2019-01-01 with the lasted CSP addendum issued 2019-12-12.>
Visibility and incorporation of IRAP assessment	<e.g. Visibility of this assessment was available, and the control implementation is detailed in the Common Infrastructure CSCM, with key details outlined in in Section 4.4 of this report. Note that this is the extent of evidence viewed, and the assessor provides no further assurance for the validity of IaaSProvider's assessment.>
Description of Use	<e.g. CSP relies on IaaSProvider to provide data locality for AUS-SouthEast-1 region>

Provider	<e.g. IaaSProvider>
Services Used	<e.g. IaaSService, AuthService>
Data Locality Used	<e.g. AUS-Southeast-A>
IRAP Assessed	<e.g. IaaSProvider has an existing IRAP assessment issued 2019-01-01 with the lasted CSP addendum issued 2019-12-12.>
Visibility and incorporation of IRAP assessment	<e.g. Visibility of this assessment was available, and the control implementation is detailed in the Common Infrastructure CSCM, with key details outlined in in Section 4.4 of this report. Note that this is the extent of evidence viewed, and the assessor provides no further assurance for the validity of IaaSProvider's assessment.>
Description of Use	<e.g. CSP relies on IaaSProvider to provide data locality for AUS-SouthEast-1 region>

5.2.1 Data centre and service locations

Instruction:
This section should list the different locations the CSP is based in to provide its cloud services, including data centres and management, support and administrator locations.

Function	Location (Country/City)		Physical Security Certification(s)
	Country	City	
<e.g. Office HQ>	<e.g. USA>	<e.g. New York>	<e.g. None>
<e.g. Support Office>	<e.g. India>	<e.g. Bangalore>	<e.g. None>
<e.g. Local Office>	<e.g. Australia>	<e.g. Sydney>	<e.g. None>
<e.g. Support DC>	<e.g. USA>	<e.g. Chicago>	<e.g. TSI>
<e.g. DC Syd 1>	<e.g. Australia>	<e.g. Sydney>	<e.g. Zone 3 SCEC, TSI>
<e.g. DC Syd 2>	<e.g. Australia>	<e.g. Melbourne>	<e.g. Zone 3 SCEC, TSI>
<e.g. DC San Francisco 1>	<e.g. USA>	<e.g. San Francisco>	<e.g. TSI>

5.2.2 Service Regions

Instruction:
List the data locality service regions assessed for this assessment, and identify which of the above locations are relevant to storing or processing data for the selected region.

Service Regions	Data Localities Used
<e.g. AUS-East-1>	<e.g. DC Syd 1, DC Syd 2>
<e.g. AUS-SouthEast-1>	< e.g. DC Syd 4, DC Melb 1>
<e.g. USA-West-1>	<e.g. DC San Francisco 1>

5.2.3 Cloud Services

The cloud services assessed are dependent on the following locations:

Instruction:
This section should list all cloud services in scope of this assessment as well as the location they are provided from for Australian based Cloud Consumers. This should include essential services of the platform required for use, such as the web console, account management and resource management, as appropriate.

Cloud Service	Available Service Regions	Other Dependencies	Assessed Classification
<e.g. Great PaaS Service>	<e.g. AUS-East-1, AUS-SouthEast-1>	<e.g. Support DC, SaaSProvider>	<e.g. PROTECTED>

<e.g. Great SaaS Service>	<e.g. AUS-East-1, AUS-SouthEast-1>	<e.g. Another SaaS Service>	<e.g. OFFICIAL:Sensitive>
<e.g. Another SaaS Service>	<e.g. USA-West-1>	<e.g. Support DC>	<e.g. OFFICIAL:Sensitive>

5.2.4 Applications and services

Service name	Description	Connection	Hosting
Vulnerability scanner	Scans vulnerabilities in the network	Scans all endpoint devices	Windows Server 2024
Central event logging system	Provides logging capabilities	Connected to all end points to collect logs	RHEL 7.4

6. Assessment details

6.1. Assessment Methodology

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

6.2. Sampling methodology

Instruction:
Detail the sampling methods used during the collection of evidence

6.2.1 Control testing methodology

Instruction:
Detail the control testing methods used, if any automated tools such as ACVT or E8MVT were used.

6.2.2 Evidence collection

Instruction:
Outline the type of evidence collected, storage of evidence and retention of evidence.

Evidence name	Evidence type	Evidence description
E.g. System security Plan	Specification	The System Security Plan outlines controls that are implemented within the system…
Disaster Recovery process review	Activity	Disaster Recovery process review was a tabletop exercises during the first day and later was a parallel test on the weekend.

6.3. Assessment boundary

Instruction:
Identify the specific systems within the environment under assessment. If particular environments, such as the corporate environment or service provider environment, are deemed not applicable, provide the justification for their exclusion from the assessment. Detail any assumptions or constraints.

6.3.1 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.

6.3.2 Assessment boundary diagram

7. System overview

7.1. 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.
Include the security posture of any underlying systems or processes.
If appropriate, you may wish to comment on the 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 a different set of system components, regions or customer base.

Outline the key security risks, vulnerabilities, issues or concerns that a consumer or entity should be aware.

7.2. Penetration testing and Vulnerability assessments

Instruction:
Include any findings identified during a penetration test or vulnerability assessment, that may be useful for the consumer to know and understand. Outline any remediation activities identified during the assessments that were completed because of the penetration test. In addition, outline if any control testing contradicted any findings presented. The penetration test or the vulnerability assessment should have been conducted within a reasonable timeframe.

7.3. Security culture

7.3.1 Response to Cyber Security Incidents

Instruction:
List any notable cyber security incidents in the provider's history, and an analysis of the provider's response to handling these incidents. The focus should be on the provider's response to the incident, rather than the incident itself.

7.3.2 Contributions to Cyber Security

Instruction:
Describe any research or initiatives the provider takes to actively contribute to a global cyber security posture, including research papers, blogs or software.

7.3.3 Cyber Security Guidance

Instruction:
Describe the clients record of providing consumer guidance on how to use its services securely, including guidance in line with ASD's ACSC publications.

7.3.4 Information Security Compliance Certifications

Instruction:
List any other information security certifications completed for the assessed cloud platform, such as FedRAMP, SOC, ISO27001/2, HIPAA, PCI or (CSA) STAR. A note should be made where these certifications cover a different scope to this security assessment, such as a different set of services, available regions, or customer base.

7.4. Governance

7.4.1 Security documentation and procedures

Instruction:
Detail the organisational and system policies, system administration procedures and relevant security documentation available. Explain how they are maintained, reviewed and communicated.

7.4.2 Enterprise and risk management

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

7.4.3 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.

7.4.4 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 whether or when to apply an update, and the communication process and mediums used to advise system consumers of associated changes.

7.4.5 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.

7.4.6 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, 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 government.

7.4.7 Data sanitisation 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?

7.4.8 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.

7.4.9 Vulnerability and patch 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.

7.4.10 Incident response

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

7.4.11 Secure development lifecycle

Instruction:
Describe the organisation's processes that embed security throughout the system lifecycle (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.

7.4.12 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.

7.4.13 Security Intelligence

Instruction:
Describe the automated activities and actions taken by the provider to identify, prevent, and report on cloud consumer or provider vulnerabilities and misconfigurations. Identify what automated security alert functions are available to identify configurations that do not align with provider security best practices.

7.5. Environments

7.5.1 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.

7.5.1.1 *Administrative and support system overview*

Instruction:
Describe the scope of this system. In particular describe 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 referenced to other diagrams in this document.

7.5.1.2 *Physical security*

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

7.5.1.3 *Segmentation and segregation*

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

7.5.1.4 *Interconnected systems*

Instruction:
Detail all the systems any other system that connects to the environment, explaining:

- The services provided by the connected system
- Security controls protecting the system
- If any services replicate between systems i.e. user accounts
- Data sent between systems

7.6. Secure administration

7.6.1 System hardening

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

7.6.2 Privileged access control

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.

7.6.3 Service and shared account management

Instruction:
Describe the process used by the organisation; how they manage, provision and protect service accounts, shared accounts.

7.6.4 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.

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.

7.7. 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.

7.7.1 Network security

Instruction:
Detail the network topology and security of the system's production network, focusing on network segmentation, 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.

7.7.2 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.

7.7.3 Security operations and monitoring

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

7.7.4 Cryptography and key management

Instruction:
Identify the use and management of cryptographic keys and associated hardware and software. Include 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.

7.7.5 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.

7.7.6 Identity and access management

Instruction:
Describe the Identity and Access Management models that are available for 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.

7.7.7 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.

7.7.8 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.

7.7.9 Protection of Data at Rest

Instruction:
For each data type, detail the cryptographic data at rest protections, including whether these are ASD Approved Cryptographic Algorithms (AACAs). Where possible, refer to the Data Types as defined in section 4.2.1.4.

7.7.10 Data Backup and Restore

Instruction:
Detail any dedicated backups that are performed of cloud consumer data, including whether this is inherent in the use of the service, or whether this relies on configuration by the cloud consumer.

7.8. Control overview

Instruction:
Capture a high level overview of the control landscape 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.

7.8.1 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

7.8.2 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 a 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 Rationale and Mitigating Factors

7.8.3 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.

Control Number(s)	Description	Recommended Remediation	Expected Remediation Date (if available)

7.8.4 Security controls with no visibility

Instruction:
Detail the controls that have “no visibility” and outline some mitigating factors or issues that need to be considered by the consumer.

Control Number(s)	Description	Recommended Remediation

8. Detailed findings

8.1. Assessment of ISM guidelines

Instruction:
Detail the implementation of ISM controls against each applicable ISM chapter and section. Provide a detailed summary of the section's controls implemented and their effectiveness. Don't re-write the controls matrix.
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*.

Annex: supporting information

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

Annex: controls matrix

Attachment A: 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.