Department of **the Premier and Cabinet**
Office of Digital Government

GOVERNMENT OF WESTERN AUSTRALIA

Office of Digital Government Information Security Risk Self-Assessment Table

Performing an initial Information Security Risk-Assessment in WA Government

Produced and published by

Department of the Premier and Cabinet

Office of Digital Government

Updated **August 2026**

Principal address:

Dumas House

2 Havelock Street

West Perth WA 6005

Postal address:

Locked Bag 3001

West Perth WA 6872

Telephone: (08) 6552 5000

Fax: (08) 6552 5001

Email: Cyber.Policy@dpc.wa.gov.au

Acknowledgement of Country

The Government of Western Australia acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders past, present and emerging.

Approval

Name / Title	Date
Peter Bouhlas, Chief Information Security Officer	August 2026

Contact Officers

Name	Email	Phone
Danijela Kambaskovic-Schwartz	Danijela.Kambaskovic-Schwartz@dpc.wa.gov.au	+61 8 6552 6020

Contents

Overview **5**

Understanding the Office of Digital Government Information Security Risk Self-Assessment Table **6**

Information Security Risk Self-Assessment Criteria 6

Western Australian Government Information Classification 6

Confidentiality or Sensitivity of Information 6

Integrity and availability of information 8

The Australian Government (Cwlth) classification 9

PROTECTED, SECRET and TOP-SECRET Classification (Cwlth) 9

Office of Digital Government Information Security Risk Self-Assessment Table (A3) **11**

Office of Digital Government Information Security Risk Self-Assessment Table **12**

Overview

The Office of Digital Government (DGov) Information Security Risk Self-Assessment Table outlines high-level information security requirements based on the confidentiality of government information being accessed, the entity's information availability and integrity needs, and the business impact of disruption.

The table is intended as a tool to support WA Government entities in undertaking an initial (high-level) information security risk assessment.

This initial high-level risk assessment underpins next steps in information security risk assessment in a variety of contexts, including, but not limited to, enterprise architecture, mobility, procurement and data offshoring.

The table is provided in A3 and A4 format for easier printing.

Understanding the Office of Digital Government Information Security Risk Self-Assessment Table

Information Security Risk Self-Assessment Criteria

The DGov Information Risk Self-Assessment Table has been developed to support entities in assessing the risk factors which will determine their approach to broader or more detailed consideration of information security in different contexts including, but not limited to, enterprise architecture, mobility, procurement and data offshoring. The assessment considers:

- What is the classification (confidentiality or sensitivity) of the information that can be accessed?
- What are the entity's needs when it comes to protection, availability and integrity of this information?
- What is the entity's tolerance for business interruption?

Western Australian Government Information Classification[1]

Confidentiality or Sensitivity of Information

Determining information confidentiality or sensitivity and appropriate information classification is a business process by which information is assessed and labelled according to the potential impact of its release. Information determined to be more sensitive typically requires different treatment and handling.

[1] While the scope of the WA Government Information Classification Policy does not extend to entities such as Government Trading Enterprises or Universities, they are encouraged to refer to and use this table as well as the principle of determining the security controls required to regulate access to most valuable information and system applies to all WA government entities included in the scope of WA Cyber Security Policy.

The Western Australian Government Information Classification Policy provides a common language for entities to identify risks and apply appropriate security controls to their information assets. Information classification assists entities to determine their security and offshoring requirements for government information.

The Western Australian Government Information Classification Policy requires that WA Government entities classify their information using the following categories:

- UNOFFICIAL (information that is not relevant to the work context).
- OFFICIAL
- OFFICIAL Sensitive

OFFICIAL Sensitive classification is used to regulate access to valuable or confidential government information attracting higher security controls ("Tier 1 Risk"), including:

- Cabinet submissions and supporting documentation
- Information subject to commercial or legal confidentiality
- Intellectual property and original research
- Information that could pose a risk to crime prevention or law enforcement efforts
- Information that could pose a risk to critical infrastructure, state or national interests, security, defence or the economy
- Data assets containing *Sensitive personal information* as defined in the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act);
- Data assets containing **two or more** of the following five categories of *Personal information* as defined in the PRIS Act, which can interact to form a "digital identity":
    - Name

- Date of Birth
- Government ID number
- Residential address
- Financial information

These five categories of personal information can be stolen, cross-referenced and used by malicious actors to steal an individual's identity or financial information, usually for financial gain. Residential addresses are included in this list as it has relevance for an individual's personal security. The WA Government Information Classification Policy Supplementary Guide has been updated to reflect this change in response to the evolving global and WA threat landscape.

Entities may also choose to apply the following sub-classifications to OFFICIAL Sensitive classification:

- OFFICIAL Sensitive Cabinet
- OFFICIAL Sensitive Legal
- OFFICIAL Sensitive Commercial
- OFFICIAL Sensitive Personal

Please refer to the Office of Digital Government Business Impact Levels Tool for further guidance.

Integrity and availability of information

In addition to confidentiality of their information holdings, WA Government entities will have different needs when it comes to how available they need their information to be, as well as their tolerance for data corruption or loss and business disruption. These factors will greatly influence their information security requirements.

Availability of information refers to how available your entity expects the digital information to be. Your availability requirements will affect the risk tiering of your information and systems.

Integrity of information refers to how reliably accurate, complete, consistent and safe your entity requires the information your entity owns to be. Integrity requirements consider what degree of assurance is required by your entity to ensure that the digital information accessible via a particular digital asset is uncorrupted and can only be modified by those authorised to do so. Your expectations in this regard will affect your risk tiering.

The Australian Government (Cwlth) classification

There are three additional information classification levels used by the Australian Commonwealth Government requiring more stringent protections. Western Australian Government entities may need to consider and meet Commonwealth information classification requirements for these classifications:

- PROTECTED
- SECRET
- TOP SECRET

PROTECTED, SECRET and TOP SECRET Classification (Cwlth)

Agencies handling COMMONWEALTH SECURITY CLASSIFIED information are required to comply with the provisions of the relevant inter-jurisdictional agreement(s) with the Australian Government. Additional information security requirements, not considered in the Information Security Risk Self-Assessment table, are required when managing information security with these classification levels.

Personnel security

All staff, consultants and contractors with access to government-owned information and systems must undergo an appropriate background check upon onboarding. The WA Government entity decides on the appropriate method of checking. Acceptable checks include:

- AusCheck or Australian Government Security Vetting Agency (AGSVA) are mandatory for critical workers in critical infrastructure entities captured under the SOCI Act 2018, designated government positions and financial institutions such as GESB)
- Police clearance
- NCCHC (Nationally Coordinated Criminal History Check)
- Any other clearance provider considered appropriate by the entity

Entities should conduct and document targeted reviews of privileged and generic account access and develop contractor, casual and third-party access management protocols aligned with Identity and Access Management principles.

Office of Digital Government Information Security Risk Self-Assessment Table (A3)

Risk Tier	Information Security Risk Self-Assessment Criteria					Information Security / Cyber Security - Next steps based on risk tiering			
	Confidentiality of Information		Availability of Information	Integrity of Information	Business Impact of Disruption	Cloud Services Offshoring (Data Sovereignty and Security)	Supply Chain and Third-party risk	Personnel Security	Identity and Access Management
	Information Classification	Information Type							
Tier 1	**OFFICIAL SENSITIVE** **Confidential information** (Additional criteria apply to Protected, Secret and Top-Secret Commonwealth information security classifications)	**OFFICIAL SENSITIVE** Highly valuable or confidential information. Cabinet submissions, information subject to commercial or legal confidentiality, intellectual property, research, law enforcement, state or national interests, security, defence, infrastructure or the economy. *Sensitive personal information* as defined in the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act), **or** any information asset that contains two or more of the following types of personal information ("digital identity"): • Name • Date of Birth • Government ID number • Residential address • Financial information	Available at all times. (99.9% uptime) High Capacity or peak usage expected.	Reliably accurate. High level of accountability required (e.g. financial information).	High business impact. Impact to critical services. Impact to public safety	Must be hosted in Australia (preferably in two different locations). Security controls are in place for offshore backups or user access from offshore locations. Data Encryption at rest and in transit.	Baseline information security considerations/ contract clause principles and Tier 1 information security considerations. Evidence of annual or biannual independent assessment of the information security risks associated with the service being procured (IRAP, ISO 27001, SOC2, FedRAMP). Supplier and their supply chain Offshoring and Foreign Ownership/ board membership risks have been considered and are not a risk. AI Security Risks have been considered and are not a risk.	Any individual in Australia accessing entity IT and OT systems should hold an AusCheck, AGSVA, NCCHC, Police or other clearance as appropriate. For individuals in the supply chain outside Australia, the requirement to guarantee the suitability of staff handling the information should be included in the contract with the main supplier.	Phishing-resistant Multi-Factor Authentication /the strongest form of MFA supported by the entity's system.
Tier 2	**OFFICIAL**	Includes most government information and communication. Routine business operations and services, emails, memos, non-sensitive draft policies and guidelines. *Personal information* as defined in the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act) not meeting criteria for Tier 1 risk.	Service available most of the time. Business continuity possible with short-term disruptions.	Reliably accurate.	Low/moderate business impact. Reduced efficiency and increased cost of operations.	Can be hosted outside Australia (requires a risk review if offshoring and assessment against Information Privacy Principle 9 when relevant provisions of the PRIS Act come into force). Limiting arrangements to countries of the Five Eyes alliance is strongly recommended (Australia, New Zealand, United States of America, United Kingdom and Canada).	Baseline information security considerations/ contract clause principles and Tier 2 information security considerations/contract clause principles. Supplier self-attestation against relevant information security requirements and regular reporting against compliance. Foreign ownership/ board membership has been considered and is not a risk.	Any individual in Australia accessing entity and OT systems should hold a Police clearance or other appropriate clearance. For individuals in the supply chain outside Australia, the requirement to guarantee the suitability of staff handling the information should be included in the contract with the main supplier.	Phishing-resistant Multi-Factor Authentication is recommended
Tier 3	**OFFICIAL**	Published information.	Can tolerate service unavailability.	Lower integrity threshold.	Low/moderate business impact.	Can be hosted outside Australia (requires a risk review if offshoring). Limiting arrangements to countries of the Five Eyes alliance is strongly recommended.	Baseline information security considerations.	No specific requirements.	Multi-Factor Authentication

Office of Digital Government Information Security Risk Self-Assessment Table

Risk Tier	Information Security Risk Self-Assessment Criteria					Information Security / Cyber Security - Next steps based on risk tiering			
	Confidentiality of Information		Availability of Information	Integrity of Information	Business Impact of Disruption	Cloud Services Offshoring (Data Sovereignty and Security)	Supply Chain and Third-party risk	Personnel Security	Identity and Access Management
	Information Classification	Information Type							
Tier 1	**OFFICIAL SENSITIVE** **Confidential information** (Additional criteria apply to Protected, Secret and Top-Secret Commonwealth information security classifications)	**OFFICIAL SENSITIVE** Highly valuable or confidential information. Cabinet submissions, information subject to commercial or legal confidentiality, intellectual property, research, law enforcement, state or national interests, security, defence, infrastructure or the economy. *Sensitive personal information* as defined in the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act), **or** any information asset that contains two or more of the following types of personal information ("digital identity"): • Name • Date of Birth • Government ID number • Residential address • Financial information	Available at all times. (99.9% uptime) High Capacity or peak usage expected.	Reliably accurate. High level of accountability required (e.g. financial information).	High business impact. Impact to critical services. Impact to public safety	Must be hosted in Australia (preferably in two different locations). Security controls are in place for offshore backups or user access from offshore locations. Data Encryption at rest and in transit.	Baseline information security considerations/ contract clause principles and Tier 1 information security considerations. Evidence of annual or biannual independent assessment of the information security risks associated with the service being procured (IRAP, ISO 27001, SOC2, FedRAMP). Supplier and their supply chain Offshoring and Foreign Ownership/ board membership risks have been considered and are not a risk. AI Security Risks have been considered and are not a risk.	Any individual in Australia accessing entity IT and OT systems should hold an AusCheck, AGSVA, NCCHC, Police or other clearance as appropriate. For individuals in the supply chain outside Australia, the requirement to guarantee the suitability of staff handling the information should be included in the contract with the main supplier.	Phishing-resistant Multi-Factor Authentication /the strongest form of MFA supported by the entity's system.
Tier 2	**OFFICIAL**	Includes most government information and communication. Routine business operations and services, emails, memos, non-sensitive draft policies and guidelines. *Personal information* as defined in the *Privacy and Responsible Information Sharing Act 2024* (PRIS Act) not meeting criteria for Tier 1 risk.	Service available most of the time. Business continuity possible with short-term disruptions.	Reliably accurate.	Low/moderate business impact. Reduced efficiency and increased cost of operations.	Can be hosted outside Australia (requires a risk review if offshoring and assessment against Information Privacy Principle 9 when relevant provisions of the PRIS Act come into force). Limiting arrangements to countries of the Five Eyes alliance is strongly recommended (Australia, New Zealand, United States of America, United Kingdom and Canada).	Baseline information security considerations/ contract clause principles and Tier 2 information security considerations/contract clause principles. Supplier self-attestation against relevant information security requirements and regular reporting against compliance. Foreign ownership/ board membership has been considered and is not a risk.	Any individual in Australia accessing entity and OT systems should hold a Police clearance or other appropriate clearance. For individuals in the supply chain outside Australia, the requirement to guarantee the suitability of staff handling the information should be included in the contract with the main supplier.	Phishing-resistant Multi-Factor Authentication is recommended
Tier 3	**OFFICIAL**	Published information.	Can tolerate service unavailability.	Lower integrity threshold.	Low/moderate business impact.	Can be hosted outside Australia (requires a risk review if offshoring). Limiting arrangements to countries of the Five Eyes alliance is strongly recommended.	Baseline information security considerations.	No specific requirements.	Multi-Factor Authentication