




Department of the Premier and Cabinet  
Office of Digital Government

# 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**

Published **October 2025**

**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](mailto: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
<b>Sandra Franz A/Chief Information Security Officer</b>	September 2025

## Contact Officers

Name	Email	Phone
<b>Danijela Kambaskovic-Schwartz</b>	<a href="mailto:Danijela.Kambaskovic-Schwartz@dpc.wa.gov.au">Danijela.Kambaskovic-Schwartz@dpc.wa.gov.au</a>	+61 8 6552 6020



## Contents

<b>Overview</b> .....	<b>5</b>
<b>Understanding the Office of Digital Government Information Security Risk Self-Assessment Table</b> .....	<b>6</b>
Information Security Risk Self-Assessment Criteria.....	6
Western Australian Government information classification.....	6
Confidentiality of Information .....	6
Integrity and availability of information .....	8
The Australian Government (Cwlth) classification.....	8
PROTECTED, SECRET and TOP-SECRET Classification (Cwlth) .....	9
<b>Office of Digital Government Information Security Risk Self-Assessment Table (A3)</b> .....	<b>10</b>
<b>Office of Digital Government Information Security Risk Self-Assessment Table</b> .....	<b>11</b>





## 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.

The high-level initial 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 assess 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 availability and integrity of this information?
- What is the entity's tolerance for business interruption?

### Western Australian Government information classification

#### Confidentiality of Information

Determining information confidentiality needs and 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.

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



The Western Australian 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

Entities may also choose to apply the following sub classifications to OFFICIAL Sensitive information, where it requires special handling, or its use or disclosure is restricted under legislation:


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

Based on the evolving threat landscape, the WA Information Classification Policy has recently been updated to include a new category:

- OFFICIAL Sensitive: Digital Identity

The changing threat landscape requires some personal information which can interact to form a “digital identity” to be given more stringent protection. These types 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 updated [WA Information Classification Policy](#) requires that classification Official Sensitive: Digital Identity apply to all WA entity data holdings that contain **two or more** of the following types of personal information:

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

### 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.

## 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)	Supplier Security	Personnel Security	Identity and Access Management
	Information Classification	Information Type							
<b>Tier 1</b>	<b>OFFICIAL SENSITIVE</b> (Additional criteria apply to Protected, Secret and Top-Secret Commonwealth information security classifications)	<b>OFFICIAL Sensitive Personal</b> ('sensitive personal information' as defined under the Privacy and Responsible Information Sharing Act 2024) <b>OFFICIAL Sensitive Cabinet</b> <b>OFFICIAL Sensitive Commercial</b> <b>OFFICIAL Sensitive Legal</b> <b>Digital Identity</b> (Two or more types of 'Personal information' as defined under the Privacy and Responsible Information Sharing Act 2024, as listed below): <ul style="list-style-type: none"> <li>Name</li> <li>Date of Birth</li> <li>Government ID number</li> <li>Residential address</li> <li>Financial information</li> </ul>	Service 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. Consider supplier Foreign Ownership risks.	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). Foreign ownership/ board membership has been considered and is not a risk.	Individuals must have a police clearance. If in Australia, a regular police 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.	Multi-factor Authentication
<b>Tier 2</b>	<b>OFFICIAL</b> (other types not included in Risk Tier 1)	Other types of ' <b>Personal information</b> ' (as defined in the Privacy and Responsible Information Sharing Act 2024) not specified in Risk Tier 1. Most government information and communication. Examples include content related to routine business operations and services and may include emails, memos and draft policies and guidelines on issues deemed to be non-sensitive.	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.	Individuals must have a police clearance. If in Australia, a regular police 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.	Multi-factor Authentication
<b>Tier 3</b>	<b>OFFICIAL (NOT CONFIDENTIAL)</b> Unofficial information is not relevant to procurement.	Public information. No high value information.	Can tolerate unavailability of service.	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/ contract clause principles.	No specific requirements.	Multi-factor Authentication is recommended but not required.

# 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)	Supplier Security	Personnel Security	Identity and Access Management
	Information Classification	Information Type							
Tier 1	<b>OFFICIAL SENSITIVE</b> (Additional criteria apply to Protected, Secret and Top-Secret Commonwealth information security classifications)	<b>OFFICIAL Sensitive Personal</b> ('sensitive personal information' as defined under the Privacy and Responsible Information Sharing Act 2024)  <b>OFFICIAL Sensitive Cabinet</b> <b>OFFICIAL Sensitive Commercial</b> <b>OFFICIAL Sensitive Legal</b>  <b>Digital Identity</b> (Two or more types of 'Personal information' as defined under the Privacy and Responsible Information Sharing Act 2024, as listed below): <ul style="list-style-type: none"> <li>Name</li> <li>Date of Birth</li> <li>Government ID number</li> <li>Residential address</li> <li>Financial information</li> </ul>	Service 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.  Consider supplier Foreign Ownership risks.	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).  Foreign ownership/ board membership has been considered and is not a risk.	Individuals must have a police clearance.  If in Australia, a regular police 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.	Multi-factor Authentication
Tier 2	<b>OFFICIAL</b> (other types not included in Risk Tier 1)	Other types of 'Personal information' (as defined in the Privacy and Responsible Information Sharing Act 2024) not specified in Risk Tier 1.  Most government information and communication.  Examples include content related to routine business operations and services and may include emails, memos and draft policies and guidelines on issues deemed to be non-sensitive.	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.	Individuals must have a police clearance.  If in Australia, a regular police 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.	Multi-factor Authentication
Tier 3	<b>OFFICIAL (NOT CONFIDENTIAL)</b>  Unofficial information is not relevant to procurement.	Public information.  No high value information.	Can tolerate unavailability of service.	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/ contract clause principles.	No specific requirements.	Multi-factor Authentication is recommended but not required.