Australian Government

Department of Employment and Workplace Relations

Third-Party AI Assessment Framework

September 2025

Contents

Introduction

Artificial Intelligence (AI) presents an opportunity to transform the way Third-Party organisations (organisations) and the Department of Employment and Workplace Relations (the Department) deliver better services and improve outcomes. As AI becomes part of our everyday work, it is important to use it in a way that is ethical, secure and respectful.

The Third-Party AI Assessment Framework (the Framework) is designed to help organisations understand and meet the Department's expectations when applying to use AI in service delivery. It supports safe and responsible innovation while protecting individuals and communities.

The Department is committed to using AI in ways that:

- protect personal information and data
- are fair and respectful
- respect human rights and Indigenous data sovereignty
- keep humans at the centre of decision-making

Organisations must use the Framework to guide their applications and ensure their AI use aligns with the Department's values and legal obligations.

Purpose

The Framework sets out organisations' obligations when using AI to deliver services on behalf of the Department. It helps organisations understand their responsibilities and make sure their use of AI is safe, fair, and follows government standards.

The requirements in the Framework are intended to ensure that organisations' use of AI is consistent with:

- the Australian Government's Artificial Intelligence Ethics Principles
- the Digital Transformation Agency's Policy for the Responsible Use of AI in Government; and
- the Commonwealth AI Assurance Framework.

Organisations are expected to align with national standards and uphold ethical principles when applying to use AI, ensuring their systems are safe, responsible, and serve the public interest.

Scope

The Framework applies to all organisations that have signed a contract, agreement, or entered into a deed with the Department to deliver services.

This Framework should be read in conjunction with your organisation's relevant deed/contract and any other applicable Guidelines issued by the Department.

The Framework does not apply to how organisations use AI for internal business purposes, such as human resources systems, when those uses are unrelated to delivering services for the Department and are fully isolated from all service-related systems and data.

AI Systems Covered

All types of AI systems are covered by the Framework, including but not limited to:

- Machine learning
- Natural Language Processing (NLP)
- Generative AI

These obligations apply regardless of whether the AI system is:

- Built in-house
- Purchased from a vendor
- Adapted from existing tools

Monitoring and Accountability

The Department's AI initiatives, including the Framework, are overseen by the AI Accountable Officer. This role ensures that all AI systems used in service delivery are ethically managed, properly monitored, and compliant with legal and policy requirements.

Organisations applying to use AI in service delivery must identify their **AI Lead** or **AI Accountable Officer**. This role is responsible for making sure the organisation follows the Framework and meets all relevant legal and policy obligations – it reflects the Department's own approach to AI governance and accountability.

If the AI use case is approved, organisations must monitor and report any changes to:

- The AI system's function
- The data it uses
- The service context in which it operates

Organisations are also required to notify the Department when an approved AI use case progresses through the lifecycle stages.

For more information about how the Department manages AI, refer to the AI Transparency Statement.

Third-Party Requirements for AI Use

By default, organisations must not use AI to directly deliver services on behalf of the Department. AI use may only proceed if formally approved through the submission and assessment of a completed **Third-Party AI Assessment Application Form** (the form).

Organisations can refer to **Attachment A** for detailed guidance on completing the form, including expectations for each section and the principles that underpin responsible AI use.

AI may be used for internal tasks that are unrelated to service delivery if the AI system is **fully isolated** from all service-related systems and data. If isolation cannot be guaranteed, AI must not be used.

The Department prohibits the use of technologies that are considered high-risk or non-compliant with Commonwealth cybersecurity guidance. Refer to the Department of Home Affairs' (Home Affairs) Protect Security Directions under the Protective Security Policy Framework (PSPF).

When AI Use Is Allowed

AI use may be allowed only if all the following conditions are met:

- The technology is **not banned** for government use.
- The **contract** or **deed, including any guidelines, explicitly permits** AI use, subject to the Framework.
- A **formal application** is submitted in the approved format.
- The Department gives **written approval.**

Approved AI use will be monitored under the Right Fit for Risk (RFFR) accreditation process.

When AI Approval Can Be Withdrawn

The Department may withdraw approval if:

- The technology becomes prohibited under the Protect Security Directions.
- The third-party **fails to meet** the conditions outlined in their application or approval.
- The third-party **does not identify** an AI Lead or AI Accountable Officer to oversee AI use.

Ethics and Cybersecurity Commitments

As AI becomes more common in service delivery, it is essential that organisations understand and uphold the Department's expectations for responsible use. These expectations reflect the Department's commitment to ethics, privacy, and public trust, and are based on the Australian Government's AI Ethics Principles and the Department's RFFR accreditation process.

Organisations applying to use AI must demonstrate how these commitments are embedded throughout the AI system's lifecycle. This information must be clearly outlined in the form and will be assessed as part of the Department's approval process.

Refer to **Attachment A** for detailed guidance on how to address these areas in your application.

1. **Ethical and Privacy Considerations**
   - Organisations must ensure that ethical principles, privacy rights, and data protection laws are upheld throughout the AI system's lifecycle.
   - This includes safeguarding personal information and ensuring AI technologies do not compromise individual privacy.
   - Where AI is approved, organisations remain responsible for managing ethical and privacy risks and meeting all contractual obligations.

2. **Cybersecurity Requirements**
   - Organisations must adhere to the cybersecurity requirements outlined in the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM).
   - The application must demonstrate how cybersecurity risks are managed leveraging an effective Information Security Management System (ISMS).
   - Where approval is granted, organisations remain responsible for the continuous monitoring of AI systems using a threat driven risk management approach throughout the lifecycle.

More information

For more information, please contact the Department by email at securitycompliancesupport@dewr.gov.au.

Related documents

- *Privacy Act 1988 (Cth)*
- *Social Security Act 1991 (Cth)*
- *Social Security (Administration) Act 1999 (Cth)*
- APS Data Ethics Framework
- AI Transparency Statement
- Policy for the Responsible Use of AI in Government
- Voluntary AI Safety Standard
- Commonwealth AI Assurance Framework
- Australian Government Information Security Manual
- Protective Security Policy Framework

Attachment A: Third-Party AI Assessment Application Form Guidance

This guidance supports organisations in completing the **Third-Party AI Assessment Application Form** (the form). It provides detailed context for each section of the application and outlines the Department's expectations for ethical, secure, and responsible AI use in service delivery.

Organisations are expected to demonstrate how their AI systems uphold human-centred values, protect privacy, manage risks, and support fair and transparent outcomes.

Third-Party AI Use Application Overview

Organisations that wish to use AI to support service delivery for the Department must follow the formal approval process.

Each proposed use of AI requires a **separate application** and **written approval** from the Department before it can be implemented.

Step 1: Initial Check

Before applying, organisations should:

- conduct an **internal ethics and cybersecurity assessment**; and

Organisations must confirm:

- The AI use case is **directly related** to delivering services for the Department
- If the use is **not related to service delivery**, the AI system must be **fully isolated** from all service delivery systems and data. If isolation is not possible, the AI must not be used; and
- The AI technology is **not prohibited** under the Department of Home Affairs' the Protect Security Directions.

This step ensures only eligible and safe AI technologies proceed to application. Refer to the **Step 1 Initial Check Process Map** for guidance.

Step 2: Third-Party AI Assessment Application Form

The form helps the Department assess whether the proposed AI use:

- Aligns with the **Australian Government's AI Ethics Principles**; and
- Meets the Department's **RFFR** accreditation requirements.

Once eligibility is confirmed:

1. Complete the form and email it to securitycompliancesupport@dewr.gov.au.
2. The Department will review the application and may request further information where required.
3. The decision may involve consultation with other agencies, such as the Department of Social Services (DSS) or the National Indigenous Australians Agency (NIAA).
4. The Department will notify the organisation of the final decision.

Approved AI use cases will be reviewed annually as part of the RFFR process.

Ongoing Obligations

Organisations must monitor and report any changes to:

- The AI system's **function**
- The **data it uses**
- The **service context** in which it operates

Organisations must **notify** the Department when an AI system is progressed through its lifecycle stages, for example **moving** from **design** into **verification and validation** followed by **deployment** and **operation**.

- If an AI system does not progress beyond the **design** phase, it will not be included in the RFFR review process.

All changes must be reported to the Department for review. Refer to the **Step 2 Third-Party AI Assessment Application Form Process Map** for further detail.

Appealing a Decision

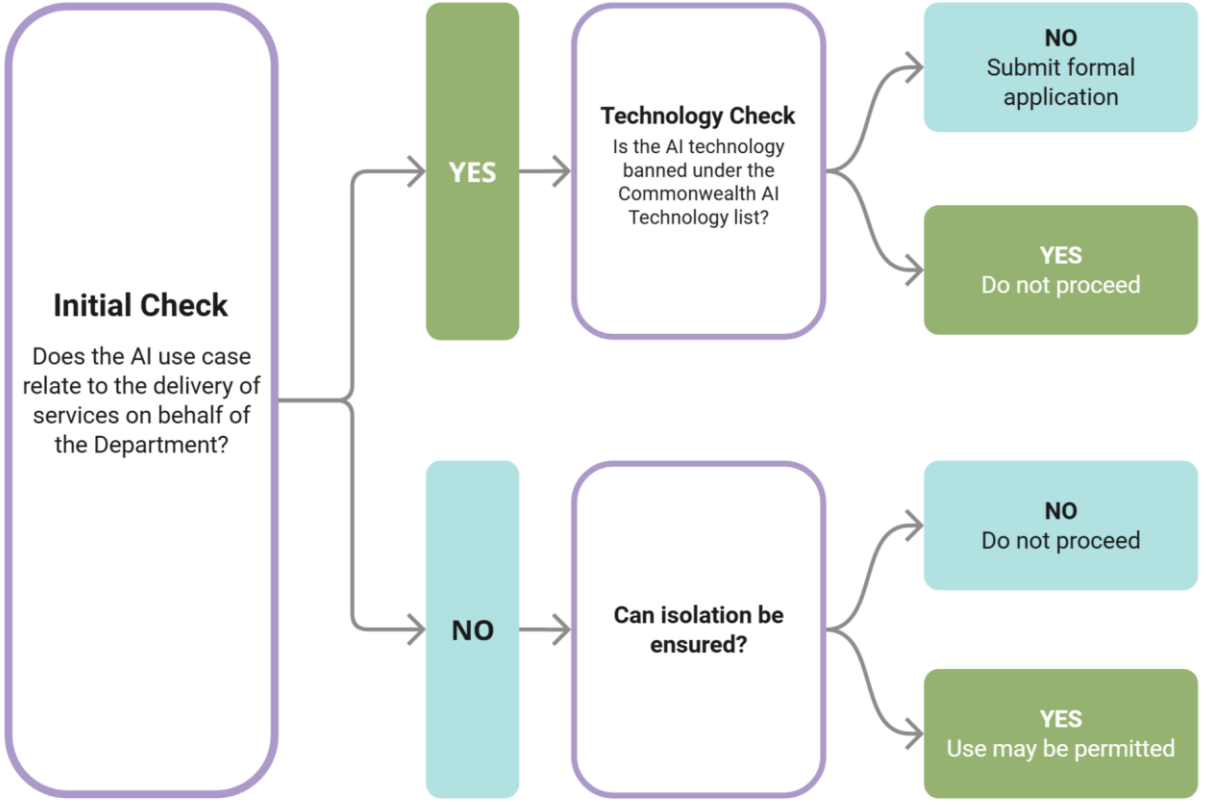
If an organisation's AI application is not approved, a review or appeal of the decision may be requested. The appeal process will follow the rules set out in the organisation's contract, agreement, or deed with the Department.

Organisations should refer to their specific contractual arrangement to understand:

- The steps for lodging an appeal
- The timeframes and documentation required; and
- Who to contact within the Department.

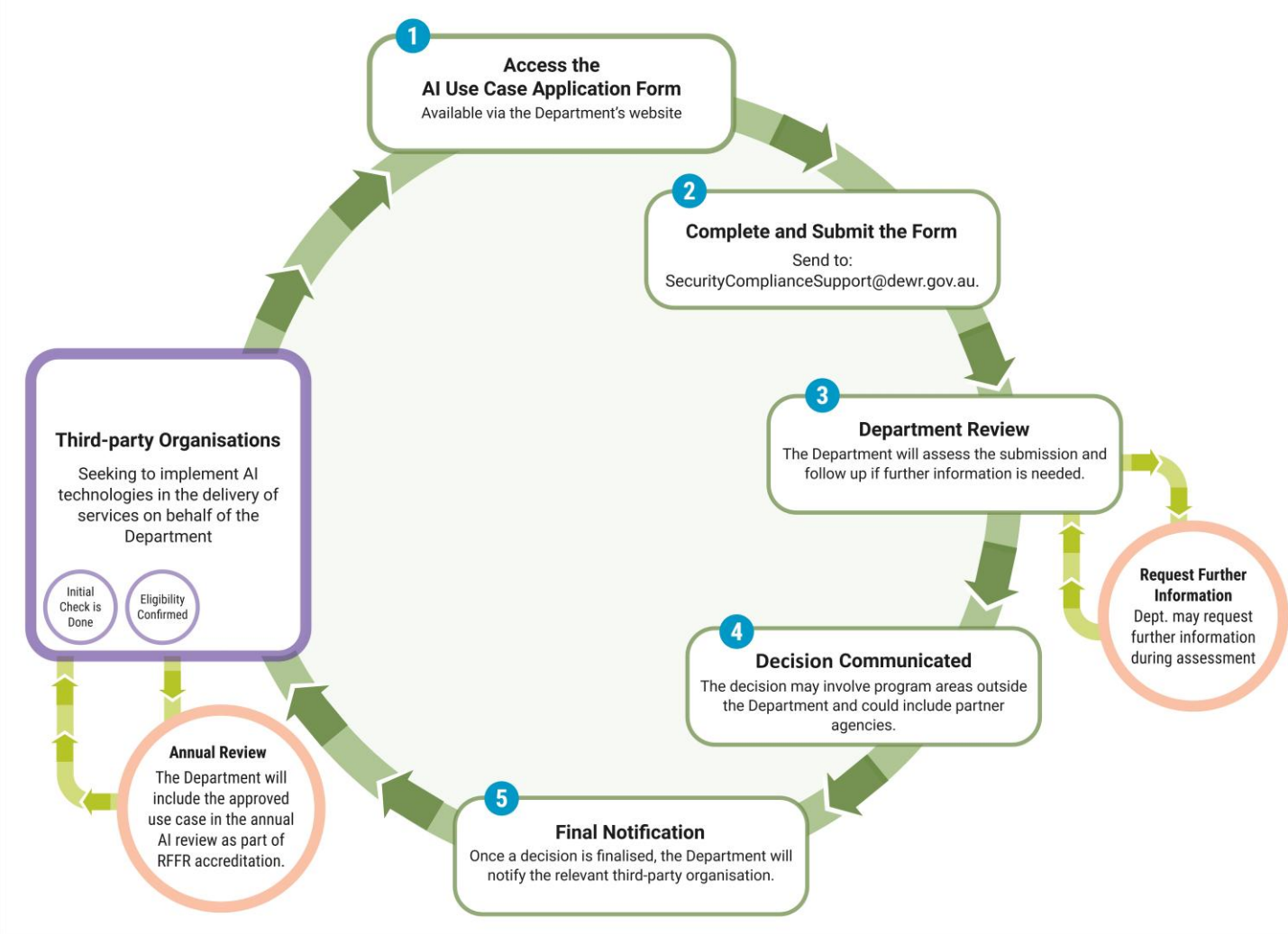
Step 1 Initial Check Process Map

The following process map outlines the steps involved in conducting the **initial check** prior to completing the Third-Party AI Assessment Application Form.



Step 2 Third-Party AI Assessment Application Form Process Map

The following process map outlines the steps involved in completing the Third-Party AI Assessment Application Form.



Application supporting information

Each section of the Form corresponds to key principles and standards. This attachment outlines what organisations should demonstrate in each area:

The Form Sections

1. Organisation Details
2. AI Use Case
3. Privacy Protection and Security
4. Reliability and Safety
5. Human-Centred Values and Fairness
6. Contestability and Accountability
7. Transparency and Explainability
8. Cybersecurity

Organisation Details

To ensure accurate assessment and alignment with contractual obligations, organisations applying to use AI must provide verified organisational details. This information enables the Department to confirm eligibility, link applications to existing service agreements, and establish appropriate points of contact.

Organisations must provide:

- **Legal and trading names** as registered with the Australian Business Register
- **Australian Business Number (ABN)** or **Australian Company Number (ACN)**
- **Four-letter organisation code**, if known, to support linkage with Workforce Australia Online systems
- **List of current Deeds or Contracts** held with the Department relevant to service delivery
- **Primary contact details** for the AI Lead or AI Accountable Officer responsible for the proposed AI use

This information supports the Department's governance, monitoring, and assurance processes, including the RFFR accreditation framework. It also ensures that AI use is traceable to the responsible entity and that communication channels are clearly established.

Organisations must ensure that all details are current and consistent with contractual records. Failure to provide accurate information may delay the assessment.

AI Use Case

Organisations applying to use AI must clearly define the purpose, scope, and expected impact of each proposed use case. This ensures alignment with the Department's ethical standards, service delivery goals, and assurance processes.

In line with the Australian Government's AI Ethics Principles of Human, Societal, and Environmental Wellbeing, AI systems should benefit individuals, society and the environment.

Organisations must demonstrate:

- **Purpose and benefit**: The AI system must have a clearly defined objective that supports improved outcomes for participants, communities, or service delivery. Efficiency alone is not sufficient justification.
- **Problem definition**: The use case must identify a specific challenge or opportunity that the AI system addresses, supported by evidence or operational need.
- **Impact assessment**: The organisation must assess who may be affected by the AI system, including individuals, communities, and service providers. This includes consideration of potential risks to marginalised or underrepresented groups.
- **Social and environmental considerations**: The use case must consider broader implications, including sustainability, accessibility, and unintended consequences.
- **Respect for Indigenous data sovereignty**: Where applicable, organisations must demonstrate how the AI system supports the rights of Aboriginal and Torres Strait Islander peoples to control their own data, in line with the Framework for Governance of Indigenous Data.
- **AI lifecycle stage**: Identify the current stage of the AI system using the following categories, adapted from the OECD's definition of the AI system lifecycle:
    - **Early experimentation** – Initial exploration without commitment to implementation, significant resourcing, or risk exposure.
    - **Design, data and models** – Planning, data collection and processing, and model development activities.
    - **Verification and validation** – Testing and tuning to assess performance, reliability and alignment with objectives.
    - **Deployment** – Integration into live environments, including piloting and change management.
    - **Operation and monitoring** – Ongoing use with continuous evaluation of impacts and system behaviour.
    - **Retirement** – Decommissioning or withdrawal from use, including data migration and evaluation.

Privacy Protection and Security

Under the Australian Government's AI Ethics Principles, the principle of Privacy Protection and Security is defined as the expectation that AI systems should respect and uphold privacy rights and data protection, and ensure the security of data.

Organisations must comply with privacy and legal obligations in their deed or contract with the Department. This includes strong data governance across the AI lifecycle—from collection to deletion.

Responsible data handling is essential for building public trust and ensuring fair, accurate outcomes.

For further guidance, refer to:

- Office of the Australian Information Commissioner's guidance on De-identification and the Privacy Act.
- *De-identification Decision-Making Framework, jointly developed by the OAIC and CSIRO Data61*.

Organisations must demonstrate:

- A guide on how your organisation ensures compliance with relevant contractual and legal obligations when collecting, storing, processing, and sharing such data.
- Secure handling and storage of sensitive information.
- Restricted and managed access to AI system data.
- Mandatory privacy training for staff.

Reliability and Safety

Under the Australian Government's AI Ethics Principles, the principle of Reliability and Safety is defined as the expectation that AI systems should reliably operate in accordance with their intended purpose.

Organisations applying to use AI must ensure their systems are tested, monitored, and maintained to perform as expected. This includes identifying and managing risks, and ensuring the system remains fit for purpose throughout its use.

Organisations must demonstrate:

- That the AI system works consistently and accurately
- Controls to ensure data quality and reliability
- Evidence of testing, validation, and monitoring
- A risk management plans for system failures or unexpected outcomes; and
- Procedures for human oversight and safe system shutdown.

Human-Centred Values and Fairness

Under Australian Government's AI Ethics Principles:

- **Human-Centred Values** is defined as: AI systems should respect human rights, diversity, and the autonomy of individuals.
- **Fairness** is defined as: AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups.

Organisations applying to use AI must ensure their systems:

- Support human decision-making, rather than replace it
- Are designed using human-centred approaches, involving diverse perspectives to reduce bias
- Are inclusive and accessible, avoiding unfair treatment or discrimination
- Are tested to ensure they do not reinforce existing biases or create new forms of disadvantage, particularly for vulnerable or underrepresented groups

Organisations must demonstrate:

- Involvement of diverse stakeholders in the design or oversight of the AI system
- That the AI system is used to enhance human judgment
- Identification and management of ethical risks, such as unintended consequences or privacy harm
- Assessment of the system for bias and discrimination risks
- Clear definitions and measurements of fair outcomes

- Actions taken to reduce fairness risks, including addressing bias and ensuring informed consent

For further guidance, refer to:

- The OECD Catalogue of Tools and Metrics for Trustworthy AI.
- The Fairness Assessor Metrics Pattern from the CSIRO Data61 Responsible AI Pattern Catalogue.

Contestability and Accountability

Under Australian Government's AI Ethics Principles:

- **Contestability**: when an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.
- **Accountability:** those responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.

AI systems used in service delivery must be designed and governed in ways that allow individuals to understand when AI is being used, challenge decisions that affect them, and ensure those responsible for the system are identifiable and accountable.

Organisations applying to use AI must demonstrate:

- That individuals are informed when AI is used
- Clear notification processes for decisions influenced by AI
- Accessible complaint and challenge mechanisms
- Timely appeal procedures that are easy to understand and use
- Identification of ethical risks linked to the AI system
- Documented plans to manage and reduce those risks
- Clearly defined roles and responsibilities across the AI system lifecycle
- Procedures for human oversight of AI decision-making

These requirements ensure that AI systems are responsibly managed, transparent, and responsive to the needs and rights of individuals affected by their use.

Transparency and Explainability

Under Australian Government's AI Ethics Principles, there should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI, and can find out when an AI system is engaging with them.

Transparency helps build public trust, supports informed consent, and ensures that AI systems remain understandable to both technical and non-technical audiences.

Organisations applying to use AI must demonstrate:

- Consultation with relevant communities or groups affected by the AI system
- That individuals are clearly informed when AI is used in service delivery
- Plain language documentation explaining how the AI system works and how it makes decisions

These requirements ensure that AI use is open, accountable, and respectful of the public's right to know.

Cybersecurity

AI systems must be secure, resilient, and responsibly managed throughout their lifecycle. Cybersecurity is a foundational enabler for safe and responsible use of AI. It protects sensitive data, upholds public trust, and ensures the integrity and availability of service delivery. As AI systems introduce new attack surfaces and complex supply chain dependencies, security must be embedded from the outset and maintained throughout the lifecycle, guided by a threat-driven risk management approach.

Organisations applying to use AI must demonstrate how cybersecurity risks are managed in alignment with the following government frameworks and industry standard. These should be evaluated and applied proportionally to the AI system's risk profile, lifecycle stage, and deployment context.

- Protective Security Policy Framework (PSPF) and associated PSPF Directions**:** set mandatory requirements for managing security risks across government services, covering governance, risk, information, technology, personnel, and physical security.
- Australian Government Information Security Manual (ISM): a cybersecurity framework that organisations can apply to protect their information technology systems, applications, and data from cyber threats. As AI systems are IT systems, ISM principles and security controls should be applied where relevant, with additional considerations for mitigating AI-specific security risks. Selected controls should be embedded early, following secure-by-design principles across the AI lifecycle.
- **ISO/IEC 27001:2022:** an international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). For AI systems, the standard supports a structured, risk-based approach to managing information security across the lifecycle. Where appropriate, it can be integrated with an AI Management System (AIMS) to ensure coordinated governance, risk management, and assurance across both information technology and AI-specific components.

Organisations must demonstrate:

- Evaluation and continuous monitoring of AI-specific threats and risks alongside traditional cyber threats, with a selection of mitigation strategies tailored to the AI system's architecture, data lifecycle and attack surface.
- Integration of AI systems into their ISMS, with controls tailored to business impact levels, data classification, and threat environment.
- Documented assessment of shared responsibilities for Commercial Off-The-Shelf (COTS) or third-party AI services, including contractual arrangements and assurance mechanisms.
- Adoption of secure-by-design practices and zero trust principles, particularly for in-house AI development, in line with Australian Signals Directorate (ASD) guidance for defensible architecture and secure AI system development.
- Ongoing monitoring and evaluation of AI systems under the Department's RFFR assurance lifecycle, ensuring alignment with government cybersecurity requirements.

Glossary

Term	Definition
AI Accountable Officer	An AI Accountable Officer is the senior individual within an organisation who holds strategic responsibility for the oversight and governance of AI initiatives. This role serves as the central point of coordination for AI-related activities, ensuring that the organisation's use of AI aligns with its values, objectives, and risk appetite.
Artificial Intelligence (AI)	As defined in the Policy for the Responsible Use of AI in Government, 'AI Technologies' means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments and may vary in their levels of autonomy and adaptiveness after deployment.
Data Sovereignty	Data sovereignty refers to the right of a nation to control and manage its own data, regardless of where that data originated and [is] stored. This means that a country has the authority to determine how its data is collected, processed, and shared, as well as enforce its own laws and regulations related to data protection and privacy. Data sovereignty is often linked to national security, as countries may be concerned about foreign access to sensitive data.
Information Security Manual (ISM)	The Australian Signals Directorate produces the Information security manual (ISM). The ISM is a cybersecurity framework that an organisation can apply, using their risk management framework, to protect their information technology and operational technology systems, applications and data from cyberthreats.
Personal Information	The Privacy Act defines 'personal information' as: 'Information or an opinion about an identified individual, or an individual who is reasonably identifiable: a. whether the information or opinion is true or not; and b. whether the information or opinion is recorded in a material form or not.'

Right Fit for Risk (RFFR) accreditation	The Department uses the External Systems Accreditation Framework (ESAF) and the Right Fit for Risk (RFFR) assurance approach to assess and accredit Providers' Information Security Management Systems (ISMS). The ESAF aligns with the Protective Security Policy Framework (PSPF) and supports the Department's accountability for safeguarding data across all contracted programs and systems.
Secure-by-Design	Secure by Design is a proactive, security-focused approach to the design, development and deployment of products and services that necessitates a holistic organisational approach to cybersecurity. For further information refer to the Australian Signals Directorate Secure by Design guidance.
Sensitive information	Sensitive information is personal information that includes information or an opinion about an individual's: • racial or ethnic origin • political opinions or associations • religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record • health or genetic information • biometric information (some aspects). Generally, sensitive information has a higher level of privacy protection than other personal information.
Third-Party Organisation	Any external entity contracted by the Department to deliver services under a deed or contract or agreement. These organisations may include employment services providers, skills and training program providers, or other service delivery partners.