External Systems Assurance Framework (ESAF)

This framework sets out the External Systems Assurance Framework (ESAF) under which the Department gains assurance over External IT Systems, and provides information for Providers in relation to:

- the security and assurance requirements that Providers must meet under the ESAF, and
- how Providers must meet these security and assurance requirements, including through achieving and maintaining Right Fit For Risk (RFFR) Accreditation for any Provider IT System, and in relation to Third Party IT accreditation.

A Provider's failure to comply with any applicable ESAF requirement (including any requirement in relation to timeframes) may constitute a breach of the Agreement, and the Administering Department may take action against the Provider in relation to the breach in accordance with the Agreement.

ESAF Overview

The objective of the ESAF is to ensure that any External IT Systems and supporting processes used in the delivery of Services are compliant with Australian Government security and privacy requirements.

The ESAF provides a structured assurance framework for all External IT Systems used by Providers or any Subcontractors that:

- support the delivery of Services, or
- are used to Access the Administering Department's IT Systems.

This includes Provider IT Systems and any Third Party IT.

The use of External IT Systems in association with the delivery of Services or to Access the Administering Department's IT Systems introduces security risks that must be actively managed. Responsibility for managing these risks is shared between the Administering Department, Providers and Third Party IT Vendors. This shared approach ensures that appropriate safeguards are in place to protect relevant information throughout the term of the Agreement.

Developed in alignment with the Protective Security Policy Framework (PSPF), the ESAF ensures the RFFR accreditation approach reflects whole-of-government security requirements, as well as relevant legislative and regulatory obligations.

The ESAF is reviewed annually by the Department to ensure continued alignment with whole-of-government obligations, evolving regulatory requirements, and the Department's strategic objectives. These reviews inform updates to ESAF requirements.

Templates and other resources

Providers must ensure that all information provided to the Department for the purposes of meeting ESAF requirements is true, accurate and complete, and reflects the Provider's current security posture.

To assist Providers in achieving and maintaining RFFR Accreditation, the Department publishes templates and other resources on its website. Providers must use the latest version of templates relevant to their assigned Assurance Category when submitting Deliverables required for the purposes of meeting ESAF requirements.

The Department may publish updates to these templates and other resources to reflect changes to the Department's and whole-of-government security requirements. If the Department issues a new version of a template less than three (3) months before a Provider's Deliverables are due, the Provider may choose to use either the previous version or the updated version.

RFFR Core Expectations

Under the ESAF, each Provider is assigned to one of four Assurance Categories based on the risk profile of their organisation. Providers must comply with all RFFR Core Expectations set out in the ESAF, in addition to any category-specific requirements that apply to them.

Personnel Security

Providers must ensure that prior to employing or engaging any individual to support the delivery of Services, they:

- verify the individual's identity through positive identification procedures,
- obtain a satisfactory police check for the individual,
- ensure that the individual:
    - is an Australian citizen, or
    - where the individual is not an Australian citizen or Australian permanent resident, that they hold a valid visa with the appropriate right to work, and
- ensure, as a condition of their employment or engagement, that:
    - the individual is subject to information security and non-disclosure obligations that meet the requirements under the relevant Agreement, and
    - such obligations continue to apply to the individual after their employment ends.

Subcontractors

To the extent that subcontracting is permitted under the relevant Agreement, Providers must ensure that any Subcontractors comply with all security, privacy and data sovereignty obligations set out in the relevant Agreement.

Physical Security

Providers must implement physical security measures at Facilities that minimise the risk of information and physical assets being:

- made inoperable or inaccessible, and
- accessed, used or removed without appropriate authorisation.

Cyber Security

Providers must establish, implement, and maintain cyber security measures proportionate to their risk profile, to minimise the risk of the Administering Department's information and supporting systems (including External IT Systems) being:

- compromised, altered, or disclosed without authorisation, or
- made unavailable or otherwise unable to support the delivery of the Services.

The cyber security measures must include measures to:

- identify and manage cyber security risks, including risks arising from the provision of Services under the Agreement,
- define security governance, roles, and responsibilities for managing cyber security within the Provider's organisation,
- implement and maintain security controls that are appropriate to the Provider's assigned Assurance Category and applicable to the Provider's IT and operating environment,
- detect, respond to, and recover from cyber security incidents in a timely manner, to ensure early identification and response and support business continuity and the continued provision of Services;
- monitor system security and identify and implement any changes necessary to ensure the ongoing effectiveness of the Provider's security program, and
- continually review and improve cyber security measures to remain effective against evolving threats.

External IT Systems

An 'External IT System' means any information technology system or service (including any cloud platform), other than the Administering Department's IT Systems, used by the Provider or any Subcontractor in association with the delivery of the Services or to Access the Administering Department's IT Systems. 'External IT System' includes a Provider IT System and any Third Party IT.

Providers must ensure that any External IT System used in association with the delivery of the Services or to Access the Administering Department's IT Systems:

- complies with all Agreement requirements, including requirements relating to privacy and data sovereignty, and
- meets the relevant requirements of the ESAF.

Where under the Agreement the Administering Department requires that the Administering Department's IT Systems are used to collect or store Participant information, or to perform

certain tasks in the delivery of Services, Providers must not use any External IT System for that purpose, even if that External IT System meets the requirements of the ESAF.

Third Party IT

'Third Party IT' means any:

- information technology system (including any cloud platform) developed and managed, or
- information technology service provided,

by a Third Party IT Vendor and used by the Provider or any Subcontractor in association with the delivery of the Services or to Access the Administering Department's IT Systems. 'Third Party IT' includes a Third Party Employment and Skills (TPES) System and a Third Party Supplementary IT System (TPSITS).

Providers must ensure that their Accreditation Deliverables describe all Third Party IT used by the Provider or any Subcontractor in association with the delivery of the Services or to Access the Administering Department's IT Systems.

TPES System

A TPES System is any Third Party IT used in association with the delivery of the Services, whether or not that Third Party IT Accesses the Department's IT Systems, and where that Third Party IT contains program specific functionality or modules.

An accredited TPES System may be used for the analysis of Records relating to the Services or any derivative thereof.

The Provider must not use a TPES System to Access the Administering Department's IT Systems or electronic Records relating to the Services unless it has been accredited by the Department in accordance with a Third Party IT Vendor Deed. Before using a TPES System, the Provider must:

- ensure that the relevant Third Party IT Vendor has entered into a current Third Party IT Vendor Deed with the Department in relation to the TPES System,
- confirm that the TPES System is currently included in the list of accredited TPES Systems published on the Department's website,
- review the relevant TPES System's RFFR accreditation report, including the scope of the TPES System's RFFR accreditation and description of shared responsibilities, and
- implement any controls and/or system configuration requirements specified in the relevant TPES System's RFFR accreditation report as 'customer responsibilities'.

The Department's accreditation of a TPES System provides assurance that the TPES System meets the Department's security requirements. However, Providers remain responsible for ensuring that any TPES System is configured and used in a way that effectively mitigates their own information security risks. The Department does not warrant that any TPES System that is accredited in accordance with a Third Party IT Vendor Deed is fit for its intended use or for a Provider's specific business processes, or is free from error or security weaknesses.

Before using an accredited TPES System, the Provider must ensure that the TPES System is identified, and its use clearly described, within the Provider's Accreditation Deliverables and where relevant, its Updated Deliverables.

TPSITS

A TPSITS is any Third Party IT used in association with the delivery of the Services, where that Third Party IT:

- does not Access the Administering Department's IT Systems, and
- does not contain program specific functionality or modules.

A TPSITS may be used for the analysis of Records relating to the Services or any derivative thereof.

A TPSITS is not accredited by the Department for the purposes of the ESAF. However, before using a TPSITS, the Provider must ensure that the TPSITS:

- is included within the scope of the Provider's RFFR Accreditation and clearly described within their Accreditation Deliverables, and
- complies with all ESAF requirements applicable to the Provider's assigned Assurance Category.

Right Fit For Risk (RFFR)

The Department's RFFR assurance approach operationalises the ESAF by defining the processes through which the Department obtains assurance over External IT Systems. It applies a risk-based methodology to ensure requirements are proportionate to the Administering Department's risk exposure and establishes the Assurance Lifecycle through which Providers achieve and maintain RFFR Accreditation.

Assurance Lifecycle

The Department is responsible for granting RFFR Accreditation to Providers. To obtain RFFR Accreditation, Providers must demonstrate to the Department's satisfaction that they have implemented reasonable and appropriate security controls to support the secure delivery of the Services and protect Administering Department information.

The Assurance Lifecycle sets out the stages through which assurance is established and maintained under the RFFR accreditation approach. It provides a structured approach to managing assurance activities throughout the Term of the Agreement.

Providers must achieve the requirements of each stage of the Assurance Lifecycle within the timeline specified below and to the Department's satisfaction.

Table A – Assurance Lifecycle

Assurance Lifecycle stage	Timeline
Categorisation	The Provider must complete the Categorisation stage within **one month** of the Agreement Commencement Date.
Initial Assessment	The Provider must submit the Initial Assessment Deliverables within **two months** of the Agreement Commencement Date. The Provider must complete the Initial Assessment stage within **three months** of the Agreement Commencement Date.
Accreditation	The Provider must submit the Accreditation Deliverables at least **six weeks** before the Provider is required to obtain RFFR Accreditation. The Provider must obtain RFFR Accreditation within **nine months** of the relevant Agreement Commencement Date.
Accreditation Maintenance	The Provider must submit Updated Deliverables at least **six weeks** before the Provider is required to complete the Accreditation Maintenance stage. The Provider must complete the Accreditation Maintenance stage every **12 months** from the date that RFFR Accreditation was obtained, other than every third year when the Provider must instead complete the Reaccreditation stage.
Reaccreditation	The Provider must submit Updated Deliverables at least **six weeks** before the Provider is required to complete the Reaccreditation stage. The Provider must complete the Reaccreditation stage every **3 years** from the date that RFFR Accreditation was obtained.

Categorisation

Categorisation is the first stage of the Assurance Lifecycle and is used by the Department to determine the Provider's Assurance Category. The Assurance Category that is assigned by the Department to the Provider in the Categorisation stage will determine the level of assurance that is required for the Provider to achieve RFFR Accreditation.

The Provider must submit the Categorisation Deliverables and undertake the assurance activities required for the Categorisation stage, as set out in Table B, within **one month** of the Agreement Commencement Date.

Table B – Categorisation Deliverables and assurance activities

Deliverable/Activity	Description
Categorisation Questionnaire	The Provider must submit a Categorisation Questionnaire as part of their response to the relevant procurement or grant documentation.

Categorisation Meeting	The Provider must attend a Categorisation Meeting with the Department for the purposes of: • validating the information provided by the Provider in the Categorisation Questionnaire, • enabling the Department to understand the Provider's operating model and External IT System/s, and • discussing the RFFR accreditation approach, including key stages and timeframes, to assist in identifying the systems and processes that are within the scope of accreditation.
Outcome and next steps	The Department will assess the information and Categorisation Deliverables provided by the Provider in the Categorisation Questionnaire and Categorisation Meeting and notify the Provider of their assigned Assurance Category and the associated assurance requirements.

In the Categorisation stage, the Provider is assigned one of four Assurance Categories (i.e. Category 1, Category 2, Category 3 or Category 4) by the Department following an assessment of:

- the service delivery context, and
- the Provider's operating model.

Service delivery context refers to the nature of the Services delivered by the Provider, and the type and volume of information that the Provider is required to handle in delivering the Services.

Operating model refers to the Provider's organisational and technical characteristics that influence the complexity of the environment in which Services are delivered. Indicative relevant factors that the Department will take into account include:

- system integrations and data flows,
- data storage arrangements,
- the complexity of the Provider's IT environment,
- organisational scale,
- supply chain involvement, and
- relevant historical security or privacy incidents.

These examples are provided for context and do not limit the Department's ability to consider any additional factors that are relevant to the Provider's threat and risk profile as part of its assessment for the Categorisation stage.

Upon the completion of the Categorisation stage, the Department will assign to the Provider the Assurance Category that best reflects the Provider's overall threat and risk profile. The four Assurance Categories represent graduated levels of assurance that scale according to different risk profiles. Higher categories correspond to environments that involve greater exposure to

sensitive information or increased operating complexity, and lower categories apply to environments with limited data exposure or simpler operations.

Initial Assessment

The Initial Assessment stage involves an assessment by the Department of the Provider's security posture against the requirements of their assigned Assurance Category.

The Initial Assessment stage considers:

- the context in which the Services are delivered,
- the implementation of applicable security controls, and
- any associated risk treatment plans.

The Initial Assessment stage enables the Department to assess how the Provider will safeguard the Administering Department's information and to determine the Provider's readiness to progress toward obtaining RFFR Accreditation.

The Provider must submit the Initial Assessment Deliverables required for the Initial Assessment stage in accordance with their assigned Assurance Category, as specified in Table C below, within **two months** of the Agreement Commencement Date. This timeframe is to allow the Department to complete the Initial Assessment stage within **three months** of the Agreement Commencement Date.

Where the Department determines that the submitted Initial Assessment Deliverables do not clearly demonstrate the Provider's security posture, the Department may:

- request clarification from the Provider where information is missing, incorrect, or unclear, and
- in exceptional circumstances, consider limited adjustments to the Initial Assessment stage timeframe where the Department determines that additional time is required for the Provider to address identified deficiencies.

The Department will notify the Provider when it has successfully completed the Initial Assessment stage.

Table C – Initial Assessment Deliverables

Category	Deliverable	Description
Category 4	• Security Assessment Questionnaire (SAQ)	A Category 4 Provider must complete a SAQ outlining the Provider's current implementation of applicable security controls, including treatment plans for applicable controls not yet fully implemented.

Category 3	• Provider Security Plan (PSP) • PSP Annex	A Category 3 Provider must submit a completed: • PSP clearly defining the scope of the Services and security controls in place to safeguard the Administering Department's information, and • PSP Annex with all applicable Category 3 controls addressed to reflect their current implementation, along with a treatment plan for applicable controls not yet fully implemented.
Category 2	• Provider Security Plan (PSP) • PSP Annex	A Category 2 Provider must submit a completed: • PSP clearly defining the scope of Services and security controls in place to safeguard the Administering Department's information, and • PSP Annex with all applicable Category 2 controls addressed to reflect their current implementation, along with a treatment plan for applicable controls not yet fully implemented.
Category 1	• Provider Security Plan (PSP) • PSP Annex • ISO/IEC 27001 or DEWR ISMS Scheme Stage 1 Audit Report	A Category 1 Provider must submit: • a completed PSP clearly defining the scope of Services and security controls in place to safeguard the Administering Department's information, • a PSP Annex with all applicable Category 1 controls addressed to reflect their current implementation, along with a treatment plan for applicable controls not yet fully implemented, and • an ISO/IEC 27001 or DEWR ISMS Scheme Stage 1 Audit Report conducted by a JASANZ accredited certification body, validating the Provider's approach to implementing applicable controls within the PSP Annex.

Note: As part of the Department's initial assessment of a TPES System for the purposes of its accreditation in accordance with a Third Party IT Vendor Deed, Third Party IT Vendors are required to submit to the Department:

- a completed System Security Plan (SSP) clearly defining the scope of the TPES System and security controls in place to safeguard the Administering Department's information,
- a SSP Annex with all applicable controls addressed to reflect their current implementation, along with a treatment plan for applicable controls not yet fully implemented, and
- an ISO/IEC 27001 or DEWR ISMS Scheme Stage 1 Audit Report conducted by a JASANZ accredited certification body, validating the implementation of applicable controls within the SSP and SSP Annex.

Accreditation stage

The Provider must achieve RFFR Accreditation within **nine months** of the Agreement Commencement Date. The Provider must submit all required Accreditation Deliverables, as specified in Table D below, no later than **six weeks** prior to the deadline for achieving RFFR Accreditation.

If a Provider does not obtain RFFR Accreditation within nine months of the Agreement Commencement Date, the Provider must immediately cease using, and ensure that any relevant Subcontractor ceases using, the relevant Provider IT System.

The Department will assess the Provider's security posture for RFFR Accreditation based on the Accreditation Deliverables submitted by the Provider, as specified in Table D. As part of this assessment, the Department will evaluate the Provider's service delivery context, data lifecycle, operating model, and implementation of applicable security controls, including any associated risk treatment plans.

Where the Department determines that the submitted Accreditation Deliverables do not clearly demonstrate the Provider's security posture, the Department may at its absolute discretion:

- request clarification from the Provider where information is missing, incorrect, or unclear,
- request evidence from the Provider to confirm the implementation or effectiveness of security controls, and/or
- in exceptional circumstances, consider a limited adjustment to the Accreditation stage timeframe where the Department determines additional time is required for the Provider to address identified deficiencies.

The Provider's RFFR Accreditation is achieved upon the Provider's successful completion of the Accreditation stage, as notified to the Provider by the Department, following the Department's assessment of, and formal acceptance of the residual risk associated with, the Provider's security posture.

A Provider's RFFR Accreditation remains valid for **three years** (unless it is revoked in accordance with the ESAF), at which time the Provider must have successfully completed the Reaccreditation stage in order to maintain its RFFR Accreditation status.

Table D – Accreditation Deliverables

Category	Deliverable	Description
Category 4	• Security Assessment Questionnaire (SAQ)	A Category 4 Provider must submit an updated and completed SAQ describing the current implementation of applicable security controls and any risk treatment plans or changes to the Provider's security posture since the Initial Assessment stage.
Category 3	• Provider Security Plan (PSP) • PSP Annex	A Category 3 Provider must submit an updated and completed PSP and PSP Annex clearly defining the scope of Services and security controls in place to safeguard the Administering Department's information.
Category 2	• Provider Security Plan (PSP) • PSP Annex	A Category 2 Provider must submit an updated and completed PSP and PSP Annex clearly defining the scope of Services and security controls in place to safeguard the Administering Department's information.
Category 1	• Provider Security Plan (PSP) • PSP Annex • ISO/IEC 27001 or DEWR ISMS Scheme Stage 2 Audit Report • ISO/IEC 27001 or DEWR ISMS Scheme Corrective Actions Plan • ISO/IEC 27001 or DEWR ISMS Scheme Certificate	A Category 1 Provider must submit: • an updated and completed PSP and PSP Annex clearly defining the scope of Services and security controls in place to safeguard the Administering Department's information, • an ISO/IEC 27001 or DEWR ISMS Scheme Stage 2 Audit Report conducted by a JASANZ accredited certification body, validating the Provider's approach to implementing applicable controls within the PSP Annex, • an ISO/IEC 27001 or DEWR ISMS Scheme Corrective Actions Plan (if applicable), and • an ISO/IEC 27001 or DEWR ISMS Scheme Certificate.

Note: As part of the Department's assessment of the security posture of a TPES System for the purposes of its accreditation in accordance with a Third Party IT Vendor Deed, Third Party IT Vendors are required to submit to the Department:

- an updated and completed System Security Plan (SSP) and SSP Annex clearly defining the scope of the TPES System and security controls in place to safeguard the Administering Department's information,
- an ISO/IEC 27001 or DEWR ISMS Scheme Stage 2 Audit Report conducted by a JASANZ accredited certification body, validating the implementing of applicable controls within the SSP and SSP Annex,
- an ISO/IEC 27001 or DEWR ISMS Scheme Corrective Actions Plan (if applicable), and
- an ISO/IEC 27001 or DEWR ISMS Scheme Certificate.

Accreditation Maintenance stage

The Accreditation Maintenance stage is an annual assurance activity that ensures the Provider's security posture remains appropriate for the secure delivery of Services and the protection of the Administering Department's information. This stage requires that any significant changes to the Provider's service delivery, operating model, supporting systems or data handling practices are accurately reflected in the Provider's Updated Deliverables.

The Accreditation Maintenance stage must be completed by the Provider every 12 months from the date of the RFFR Accreditation (the Accreditation Maintenance Date), other than every third year, when the Provider must instead complete the Reaccreditation stage.

At least **six weeks before** each Accreditation Maintenance Date, the Provider must submit to the Department the Updated Deliverables. The Updated Deliverables must reflect the Provider's current operating environment and External IT Systems.

Where the Department determines that the Updated Deliverables do not clearly demonstrate the Provider's security posture, the Department may at its absolute discretion:

- request clarification from the Provider where information is missing, incorrect, or unclear,
- request evidence from the Provider to confirm the implementation or effectiveness of security controls, and/or
- in exceptional circumstances, consider a limited adjustment to the Accreditation Maintenance stage timeframe where the Department determines additional time is required for the Provider to address identified deficiencies.

The Department will notify the Provider once it has successfully completed the Accreditation Maintenance stage.

Reaccreditation stage

The Reaccreditation stage involves a full reassessment by the Department of the Provider's security posture to confirm continued compliance with the ESAF requirements for the Provider's assigned Assurance Category, taking into account the Provider's RFFR accreditation history.

The Provider must successfully complete the Reaccreditation stage every third year from the date that the Provider obtained RFFR Accreditation (the Reaccreditation Date). Completion of

the Reaccreditation stage ensures that the Provider's security posture remains aligned to whole-of-government requirements and Departmental priorities.

At least **six weeks before** the Reaccreditation Date, the Provider must submit to the Department the Updated Deliverables. The Updated Deliverables must reflect the Provider's current operating environment and External IT Systems.

Where the Department determines that the submitted Updated Deliverables do not clearly demonstrate the Provider's security posture, the Department may at its absolute discretion:

- request clarification from the Provider where information is missing, incorrect, or unclear,
- request evidence from the Provider to confirm the implementation or effectiveness of security controls, and/or
- in exceptional circumstances, consider a limited adjustment to the Reaccreditation stage timeframe where the Department determines additional time is required for the Provider to address identified deficiencies.

The Provider must successfully complete the Reaccreditation stage in order to maintain its RFFR Accreditation. The Department will notify the Provider once it has successfully completed the Reaccreditation stage.

Reporting Requirements

Change of Circumstances

The Provider must notify the Department of any change of circumstances that may alter the risk profile of their organisation by submitting a Change of Circumstance form within **5 Business Days** of a change of circumstance. Where applicable, this includes, but is not limited to, when the Provider:

- enters into a new Agreement or terminates an Agreement,
- changes its legal or organisational arrangements, including to its:
    - legal entity details (such as changes to its legal entity or business name(s)),
    - organisational or corporate structure (including subsidiaries or group member organisations), or
    - key Personnel or governance roles (such as Chief Executive Officer, Chief Information Security Officer or equivalent positions).
- changes its market share or the location(s) from which it delivers Services (including employment regions or sites),
- changes how it handles information, or the volume or sensitivity of information it handles,
- changes its subcontracting arrangements (from one Subcontractor to another, or introduces a new Subcontractor),
- changes its IT systems, infrastructure or online services,
- changes its Third-Party IT Vendors who are supporting its IT environments, and/or

- implements the use of AI technology in the delivery of Services.

The Department will assess any change of circumstances notified by the Provider and determine whether the Provider is required to complete the Reaccreditation stage (out of cycle) or a reassessment of the Provider's Assurance Category is required.

In the event of a change of circumstances, the Provider must provide to the Department any additional information within the timeframes requested by the Department.

Security Incidents

Providers must promptly report all actual or suspected breaches of IT security (including a breach of an External IT System) to the Department through their nominated Security Contact, including where any of its Personnel or any Subcontractor suspect that a breach may have occurred or that any entity may be planning to breach IT security. This requirement applies in relation to any actual or suspected IT security breach, regardless of whether the breach is connected to the delivery of the Services or involves access to, or storage of, the Administering Department's information.

Following notification of a breach or suspected breach of IT security, the Department may review the Provider's incident report and assess the Provider's Accreditation Deliverables to confirm the implementation and effectiveness of relevant security measures. This review is undertaken so that the Department can determine whether the Provider continues to meet the level of assurance required for its assigned Assurance Category.

Based on this assessment, and in addition to any other action the Administering Department may take under the Agreement, the Department may identify corrective actions, require the Provider to undertake an independent audit, or revoke the Provider's RFFR Accreditation where the Provider is assessed as no longer meeting the required level of assurance (see further below). The Department will notify the Provider of the outcome of its assessment, including whether the Provider's RFFR Accreditation has been revoked and/or any required actions, and the Provider must undertake/implement those actions within the timeframes specified by the Department.

Other Accreditation events

Accreditation Revocation

The Department may revoke a Provider's RFFR Accreditation status at any time during the Assurance Lifecycle where the Provider is unable to demonstrate that it continues to meet the security and assurance requirements of its assigned Assurance Category. Without limiting the Department's discretion, this may include circumstances where the Provider:

- provides false, inaccurate, or materially misleading assurance information,
- fails to provide any additional information to the Department within required timeframes,

- does not meet assurance submission or reporting requirements, including where the Provider does not meet those requirements within the required timeframes (without obtaining an extension from the Department),
- does not notify the Department of a security incident or breach within required timeframes,
- is subject to a cyber security incident that, as determined by the Department, demonstrates fundamental gaps in the Provider's security program, or
- does not notify the Department of a change of circumstance impacting its security posture.

Revocation is intended to be an interim assurance measure designed to allow the Provider to restore its security posture. When RFFR Accreditation is revoked:

- the Provider's RFFR Accreditation status will be removed until the required assurance obligations are met,
- the Department will establish a timeframe within which the Provider must regain its RFFR Accreditation status by completing the Reaccreditation stage, and
- the Provider must complete all required assurance activities to successfully complete the Reaccreditation stage within that specified timeframe.

If the Provider does not complete the Reaccreditation stage within the timeframe set by the Department following the revocation of its RFFR Accreditation status, the Provider may be in breach of its obligations under the Agreement.

Recategorisation

The Department may recategorise a Provider's Assurance Category at any time during the Assurance Lifecycle if the Provider's level of risk exposure to the Administering Department changes. Recategorisation typically occurs when there are significant changes to factors such as:

- the sensitivity or volume of the Administering Department's information handled, and/or
- the nature or scope of Services delivered.

Such changes may increase or decrease the Provider's risk profile and may result in a reassessment of the Provider's Assurance Category.

Following recategorisation of a Provider's Assurance Category by the Department, the Department will update the Provider's applicable Assurance Category and will notify the Provider of any revised submission requirements and timeframes for required Deliverables, and/or advise the Provider if it is required to complete the Reaccreditation stage (out of cycle). The Provider must comply with any such requirements within the timeframes advised by the Department.

Reaccreditation (out of cycle)

If a Provider's RFFR Accreditation is revoked, or the Provider is recategorised to a different Assurance Category, the Department may require the Provider to undergo the Reaccreditation stage outside of the standard three-year cycle.

In such circumstances, the Provider must demonstrate compliance with the assurance requirements of the Provider's Assurance Category. The Department will notify the Provider of the applicable requirements and the associated timeframes for the out of cycle reaccreditation process. The Provider must comply with any such requirements within the timeframes advised by the Department.

Extensions

A Provider may request an extension of time where they are unable to meet the timeframes specified in the ESAF or as otherwise required by the Department, including where additional time is required for:

- the implementation of required security controls,
- the completion of independent audit activities, or
- submitting or updating Deliverables to meet the requirements of the applicable Assurance Lifecycle stage.

A Provider may make a request for an extension of time in writing to SecurityComplianceSupport@dewr.gov.au. The Provider must ensure that any request for an extension of time clearly demonstrates why additional time is required, outlines the Provider's progress in meeting the ESAF requirements to date, and specifies the proposed extension date.

The Department will only grant an extension of time in exceptional circumstances and only for the minimum time period necessary.

The Department will consider any request for an extension of time and advise the Provider of the outcome in writing.

ESAF Annual Review

The Department conducts an annual review of the ESAF and RFFR accreditation requirements to ensure they continue to align with whole-of-government security obligations and the Department's strategic objectives. This review may result in updates to accreditation requirements, including changes to security control expectations.

Following any review, the Department will notify Providers of any changes to the requirements. Updated templates and supporting documents will be made available on the Department's website.

Use of Artificial Intelligence in Service Delivery

Note: This section only applies to Programs administered by the Department of Employment and Workplace Relations.

This section of the ESAF applies where a Provider is delivering Services to the Department and sets out Providers' obligations relating to the use of Artificial Intelligence (AI) in the delivery of Services.

The requirements in this section are intended to maintain the integrity, security, and ethical standards in the delivery of Services, and to ensure that Providers' use of AI is consistent with the Digital Transformation Agency's Policy for the responsible use of AI in government and the Department's privacy and information security requirements.

Providers' compliance with this section will help maintain public trust and ensure the effective and responsible delivery of Services.

In this section, **'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. AI Technologies may vary in their levels of autonomy and adaptiveness after deployment. This may include AI technologies such as machine learning, natural language processing, and generative AI tools.

Providers' requirements relating to the use of Artificial Intelligence

The Department is committed to realising the benefits of AI by engaging with AI confidently, safely, and responsibly. As such, the Department will permit the use of AI by Providers in the delivery of Services but **only where** the Department gives its explicit approval to the specific AI Use Case for the delivery of Services **and** provided that the following conditions are met:

1. The AI Use Case does not involve AI Technologies banned by the Australian Government.
    - The Australian Government or the Department may from time-to-time advise or notify Providers of AI Technologies that are banned. Australian Government advice is provided in the Protective Security Policy Framework Publication Library.
    - The Department advises the following as banned AI Technologies:
        - products and web services from DeepSeek and Kaspersky Lab, Inc. This is consistent with the Department of Home Affairs' guidance to Commonwealth Agencies (see Direction 001-2025 and Direction 002-2025).
2. Providers must ensure the AI Use Case upholds ethical principles, privacy and data protection laws, and contractual requirements with respect to information management (including in relation to intellectual property, confidentiality and Records management).
    - This includes ensuring that the AI Use Case:
        - safeguards personal, sensitive and protected information,
        - does not compromise the privacy of individuals,
        - does not involve automated decision-making, and
        - ensures the keeping of detailed records.

- The AI Use Case must not include the use of AI bots for the purposes of recording meetings with the Department.
- Providers wishing to use AI bots to record meetings with Participants must seek prior written approval from the Department in accordance with the Third-Party AI Assessment Framework.
- Providers are responsible for managing compliance with these principles, relevant laws and contractual requirements in implementing and maintaining the AI Use Case, and for otherwise meeting their contractual obligations.

3. Providers must ensure that any AI Use Case implemented within their External IT Systems adheres to the cyber security requirements outlined in the Australian Government Information Security Manual (ISM) and the Protective Security Policy Framework (PSPF) to ensure the secure operation of all systems.

A Provider who would like to request to use AI in delivering Services should refer to the Third-Party AI Assessment Framework and Application Form.

The Provider must make any request for approval of an AI Use Case by sending the completed application form to SecurityComplianceSupport@dewr.gov.au, copying in the contract manager listed in the Agreement.

Any request must address in detail that the conditions above have been satisfied by the Provider.

Providers may utilise AI Technologies for functions not directly related to the delivery of Services without approval from the Department. Providers are responsible for ensuring any AI Use Case being used for such purposes is isolated from all aspects of the delivery of Services. If isolation cannot be ensured, the AI must not be used unless approved by the Department.

GLOSSARY

Term	Definition
Access	Means access or facilitation of access (whether directly or indirectly), traverse, view, use, or interface with, Records or the Administering Department's IT Systems.
Accreditation	The stage of the Assurance Lifecycle where the Department undertakes a full assessment by the Provider's security posture for RFFR Accreditation, based on the Accreditation Deliverables submitted by the Provider. As part of this assessment, the Department will evaluate the Provider's service delivery context, data lifecycle, operating model, and implementation of applicable security controls, including any associated risk treatment plans.
Accreditation Deliverables	The documents that a Provider must submit for the Accreditation stage to show that it meets the

	requirements for RFFR Accreditation for its assigned Assurance Category.
Accreditation Maintenance	The stage of the Assurance Lifecycle during which the Department conducts annual surveillance reviews focusing on the Provider's progress in implementing outstanding treatment or improvement actions, alignment with any updated RFFR requirements, and any material changes to the Provider's operating model or External IT Systems.
Administering Department	The Department or the Commonwealth department or agency with responsibility for administering the relevant Agreement which requires compliance with the ESAF and under which the RFFR Accreditation is conducted.
Administering Department's IT Systems	The Administering Department's IT computer system accessible by the Provider and Subcontractors, and through which information is exchanged between the Provider, Subcontractors, and the Administering Department in relation to the Services.
Agreement	A contract, agreement, or deed entered into between the Provider and the Administering Department to deliver services. Includes a grant agreement between the Administering Department and a Provider for the provision of funding for specific projects.
Agreement Commencement Date	The date on which the Agreement comes into effect, being the date it is executed by the last party, unless otherwise specified.
AI Use Case	A specific application of an AI system or systems by a Provider to achieve certain objectives or perform certain tasks.
Assurance Category	The category to which a Provider is assigned, based on its overall threat and risk profile, the Services it delivers, and the complexity of its operating environment, in order to determine how much assurance is required for the Provider for the purposes of the ESAF.
Assurance Lifecycle	The structured set of stages used by the Department to obtain, maintain, and renew assurance over External IT System/s under the RFFR accreditation approach. It covers all activities, requirements, Deliverables, assessments, timeframes, and obligations for all

	stages of the RFFR accreditation approach, including the Categorisation, Initial Assessment, Accreditation, Accreditation Maintenance, and Reaccreditation stages.
Categorisation	The stage of the Assurance Lifecycle where the Department assesses the Provider's service delivery context and operating model to determine the Provider's assigned Assurance Category. The assigned category sets the level of assurance the Provider must provide to achieve and maintain RFFR Accreditation and/or RFFR Reaccreditation.
Categorisation Deliverables	The documents that a Provider must submit for the Categorisation stage to enable the Department to determine the Provider's Assurance Category.
Deliverables	The documents that a Provider must submit for a particular stage of the Assurance Lifecycle.
Department	The Department of Employment and Workplace Relations, or the Commonwealth department or agency responsible for conducting the ESAF assurance process as described from time to time.
Facility	Any physical space in which business is performed to support the provision of the Services, including a building, a floor of a building, or a designated space within a building.
Initial Assessment	The stage of the Assurance Lifecycle where the Department reviews the Provider's security posture against the requirements of its assigned Assurance Category. Initial Assessment considers how the Services are delivered, the implementation of applicable security controls, and any associated risk treatment plans, and is used to determine whether the Provider is ready to progress to the Accreditation stage.
Initial Assessment Deliverables	The documents that a Provider must submit for the Initial Assessment stage to demonstrate its security posture against the requirements of its Assigned Assurance Category.
Participant	Any individual who is determined or recorded by the Administering Department, an authorised agency, or the Provider as eligible for, or receiving, services, supports, or activities delivered under an Agreement.

Personnel	Means, in relation to the Provider, any individual who is an officer, employee, volunteer, or professional advisor of that entity.
Provider	Any external entity (and its Personnel) that has entered into an Agreement with the Administering Department for the delivery of Services.
Provider IT System	An information technology system or service (including any cloud platform) used by the Provider or any Subcontractor in association with the delivery of the Services or to Access the Administering Department's IT Systems.
Reaccreditation	The stage of the Assurance Lifecycle that occurs: • every three years from the date of the Provider's RFFR Accreditation; and • at other times on an out of cycle basis, where required by the Department in accordance with the ESAF. This stage of the Assurance Lifecycle involves a full assessment of the Provider's Updated Deliverables by the Department to confirm that the Provider continues to meet the ESAF requirements for its assigned Assurance Category.
Records	Documents, information and data developed, created, copied or derived by the Provider, the Administering Department or the Department in relation to the delivery of the Services and stored by any means.
RFFR Accreditation	Accreditation by the Department of the Provider as meeting the requirements of RFFR.
Services	The activities, functions, deliverables, or other obligations that the Provider is required to perform, provide, or carry out, under an Agreement entered into with the Administering Department.
Security Contact	One or more of the Provider's Personnel with responsibility: (a) for ensuring the Provider's compliance with the Department's security policies; and (b) to communicate with the Department in relation to IT security related matters.

Subcontractor	Any party which has entered into a subcontract with the Provider and includes the Subcontractor's Personnel, successors and assignees as relevant.
Third Party IT Vendor	An entity contracted by the Provider to provide information technology systems or services to the Provider in association with the delivery of the Services, whether or not the entity is a Subcontractor, and includes as relevant, its personnel, successor and assignees, and any constituent entities of the Third Party IT Vendors organisation. A Third Party IT Vendor includes a cloud services vendor, an infrastructure as a service vendor, a software as a service vendor, a platform as a service vendor, an applications management vendor, and also any vendor of infrastructure (including servers and network hardware) used for the purpose of Accessing or storing Records.
Third Party IT Vendor Deed	An agreement between a Third Party IT Vendor that provides or uses a TPES System and the Department in the terms and form as specified by the Department from time to time.
Updated Deliverables	The revised Accreditation Deliverables submitted by a Provider for a particular stage of the Assurance Lifecycle that: • reflect the Provider's current security posture and operating environment; and • are based on the latest applicable Department-issued templates, unless transitional arrangements specified in the ESAF apply.