Australian Government
Department of Employment and Workplace Relations

Right Fit For Risk (RFFR) Questionnaire

Insert Program Name

Overview

The Department of Employment and Workplace Relations (the department; DEWR) are responsible for ensuring that any organisation it contracts to deliver services on its behalf have adequate security processes and controls in place to protect participant's personal information.

The intent of this questionnaire is to allow the department to understand the cyber security posture of each Tendering organisation. Responses to the questions should be collated from employees with the relevant knowledge in your organisation.

This questionnaire is the beginning of meeting RFFR requirements, so it is recommended that it is completed in conjunction with reading '*Section XX Information Technology' - Request for Proposal/Request for Tender*.

It is also recommended that tenderers understand the RFFR obligations they will be required to complete if successful. For more information, please refer to the DEWR website - **https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation.**

Instructions

This questionnaire covers a broad range of cyber security topics including governance, personnel processes, and specific systems you intend to use to deliver services. While multiple employees in your organisation may be involved to answer some sections, the department requests the Tenderer's signatory to sign the declaration.

If you are responding to this Tender as part of a group submission, each organisation must respond to this questionnaire separately.

Please note:

- All questions must be answered.
- Where appropriate provide as much information as possible to support your answer.
- Where you have answered 'yes' to a question, evidence must be available at the department's request.
- Where you have answered 'no' or 'unsure', please provide a brief explanation as to why this is the case.
- Assessment of a Tenderer's suitability will be made on the information provided in this questionnaire. Please ensure your responses are true and correct to the best of your knowledge.

RFFR Questionnaire

Question	Answer
Entity legal/trading name	
Registered ABN	
Registered address	
DEWR organisation code if you are an existing deed holder (4 letter alpha code issued by the department)	

1. Your Organisation	
1.1 Do you know how many participants you intend to service through this tender, combined with any other existing deeds with the department?	☐ Under 200 Participants ☐ 200 – 2,000 Participants ☐ Over 2,000 Participants
1.2 Please list all Federal government programs you are currently participating in (if applicable).	
1.3 How many employees do you currently have in your organisation as a whole?	
1.4a How many employees in your organisation will be involved in delivering services under the program described in the tender?	
1.4b How many sub-contractors to your organisation will be involved in delivering services under the program described in the tender?	
1.5 How many physical business sites will deliver services under the program described in the tender?	

2. Your Information Security Management System (ISMS)	
2.1 Has your organisation participated in RFFR in the past? *If so, detail each milestone and when they were completed, along with the date if accreditation was granted.*	

2.2 Does your organisation currently hold any ICT security certifications? *If so, please provide the type, date, and currency of the accreditation. E.g., ISO/IEC 27001, SOC 2, PCI DSS etc.*	
2.3 Please describe your experience in managing an environment for the collecting, storing and processing of information classified at the OFFICIAL: Sensitive level. *A description of Official: Sensitive information is available at: https://www.protectivesecurity.gov.au/publications-library/policy-8-classification-system.*	
2.4. Has your organisation completed a Privacy Impact Assessment covering your general operations and IT systems to address your management of personal information? *If so, please detail the recommendations and progress towards implementing those recommendations.* ***Note:** You will be required to undertake a Privacy Impact Assessment covering your general operations and IT systems as part of meeting RFFR requirements, including confirmation that all the recommendations in the Privacy Impact Assessment have been addressed.* *See guide: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/.*	
2.5. Do you have an Incident Response Plan or Data Breach Response plan? *If so, have these plans been tested?*	
2.6. Have you experienced any reportable cyber security incidents or notifiable data breaches within the past 3 years? *ASD's ACSC Reportable Cyber Security Incidents: https://www.cyber.gov.au/report-and-recover/report.* *Notifiable Data Breach: https://www.oaic.gov.au/privacy/notifiable-data-breaches.*	

2.7. What other policies and procedures does your organisation have regarding access to, and the handling of information in your IT systems.	

3. Data Sovereignty	
3.1 Please describe your understanding of your obligations regarding Data Sovereignty that are necessary under a deed with the department.	
3.2. Are any of your ICT systems hosted offshore? ***If yes, further information is required in question 3.4, 3.5 and Section 6 below.***	
3.3. Are any of your existing ICT systems accessed from offshore locations? *This may include employees working remotely, or system administration access.* ***If yes, further information within question 3.4, 3.5 and Section 6 below.***	
3.4 Do these systems collect, store, or process departmental data or participants personal or sensitive information?	
3.5 Do you have the ability to migrate these ICT systems to an equivalent Australian based solution?	

4. Your Personnel Onboarding	
4.1 Does your organisation have a documented personnel onboarding processes? *For example, conducting background checks such as Working with Children, Police check, Referee check, CV validation, etc.*	
4.2 Do you provide your employees with information security awareness training and privacy awareness training that they must complete prior to having access to your systems?	

The Essential Eight

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the ***Strategies to Mitigate Cyber Security Incidents***, to help organisations protect themselves against cyber threats. The most effective of these mitigation strategies are the 'Essential Eight'. When implementing the Essential Eight, organisations should first identify a target maturity level that is suitable for their environment and the value of the data held.

Organisations should then progressively implement each maturity level until that target is achieved. As the mitigation strategies that constitute the Essential Eight have been designed to complement each other, and to provide coverage of various cyber threats, organisations should plan their implementation to achieve the same maturity level across all eight mitigation strategies before moving onto higher maturity levels.

The department expects that organisations achieve Maturity Level 1 (ML1) as an initial baseline. Further information on Maturity Levels is available at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model.

5. Your ISMS Essential Eight Maturity	
Please ensure this section is completed by your technical specialist. For the full list of ML1 control requirements please refer to: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-ism-mapping. **Essential Eight Implementation Status Definitions (per the department)** **Not implemented:** The solution, if any, is not effective. **Partially implemented:** The solution is not fully effective or is only implemented on some relevant assets. **Fully implemented:** The solution effectively meets the control objective. **Note:** In some cases, you may have effective alternate or compensating controls. If so, please describe these in the relevant sections below.	
5.1 Essential Eight *Briefly describe your organisation's approach to implementation of the Essential Eight strategies.*	
5.2 Patch Applications *March 2024 ISM Control Ref:* *1807, 1808, 1698, 1699, 1876, 1690, 1691, 1905, 1704.*	☐ Not implemented ☐ Partially implemented ☐ Fully implemented, all controls achieve ML1 at a minimum Detail of current implementation:
5.3 Patch Operating Systems *March 2024 ISM Control Ref:* *1807, 1808, 1701, 1702, 1877, 1694, 1695, 1501.*	☐ Not implemented ☐ Partially implemented ☐ Fully implemented, all controls achieve ML1 at a minimum Detail of current implementation:

5.4 Multi-Factor Authentication *March 2024 ISM Control Ref:* *1504, 1679, 1680, 1892, 1893, 1681, 1401.*	☐ Not implemented ☐ Partially implemented ☐ Fully implemented, all controls achieve ML1 at a minimum Detail of current implementation:
5.5 Restrict Administrative Privileges *March 2024 ISM Control Ref:* *1507, 0445, 1175, 1883, 1380, 1688, 1689.*	☐ Not implemented ☐ Partially implemented ☐ Fully implemented, all controls achieve ML1 at a minimum Detail of current implementation:
5.6 Application Control *March 2024 ISM Control Ref:* *0843, 1870, 1657.*	☐ Not implemented ☐ Partially implemented ☐ Fully implemented, all controls achieve ML1 at a minimum Detail of current implementation:
5.7 Restrict Microsoft Office Macros *March 2024 ISM Control Ref:* *1671, 1488, 1672, 1489.*	☐ Not implemented ☐ Partially implemented ☐ Fully implemented, all controls achieve ML1 at a minimum Detail of current implementation:
5.8 User Application Hardening *March 2024 ISM Control Ref:* *1654, 1486, 1485, 1585.*	☐ Not implemented ☐ Partially implemented ☐ Fully implemented, all controls achieve ML1 at a minimum Detail of current implementation:
5.9 Regular Backups *March 2024 ISM Control Ref:* *1511, 1810, 1811, 1515, 1812, 1814.*	☐ Not implemented ☐ Partially implemented ☐ Fully implemented, all controls achieve ML1 at a minimum Detail of current implementation:

Your ICT Environment and Third-Party Services	
Please ensure this section is completed by your technical specialist.	
6.1 On-Premise ICT Infrastructure *Describe any on-premise ICT infrastructure used within your environment. This includes any physical/virtual servers (including email hosting and data storage capabilities), endpoints and networking devices.*	
6.2 Cloud Services *Describe all ICT cloud services used within your environment. This includes IaaS, SaaS and PaaS. This also includes the consumption intent to consume Artificial Intelligence (AI) services such as Microsoft Copilot and ChatGPT.* *For example: 'We consume Microsoft 365 for business hosted within the Australian East region, as well as an AWS S3 storage solution hosted in the Sydney region.'.* **Note: Australian onshore storage is required under the RFFR approach.**	
6.3 TPES – Third Party Employment and Skills Systems *Describe all currently used client management applications purchased from, and managed by, a vendor to support service delivery.* *Examples of current DEWR RFFR Accredited TPES Systems are available on the DEWR Website: https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation/accredited-third-party-employment-and-skills-tpes-systems.*	
6.4 MSP – Managed Services Provider *Describe all currently engaged managed service providers that manage or deliver any part of your ICT environment, infrastructure, system administration, document destruction, or other, on your behalf.*	

Please provide any additional comments that are not addressed in the questionnaire:

Declaration

I, <name, position>, on behalf of <organisation> declare that the information provided within this questionnaire is true and correct.

☐ I agree that the department will be notified of any changes in relation to the information supplied in this questionnaire, should they occur.

☐ I agree to implement or strengthen my organisation's information security posture as reasonably required by the department.

Tender Signatory / CEO	**Name**	
	Signature	
	Date	
	Email address	
	Phone number	
	Position	

Witness	**Name**	
	Signature	
	Date	
	Email address	
	Phone number	
	Position	

Please submit your completed questionnaire as part of your Tender response.