Rectangle

Description automatically generated with low confidence

Right Fit For Risk (RFFR) Questionnaire

Insert Program Name

## Purpose

The Department of Employment and Workplace Relations (the department; DEWR) is responsible for ensuring that any organisation it contracts to deliver services on our behalf has adequate security processes and controls in place. This includes any processes to protect sensitive and government or participant data accessed, generated, held or managed in their supply chain. The External Systems Assurance Framework (ESAF) aims to strengthen the security of the associated ecosystem.

**It is recommended that tenderers understand the RFFR obligations they will be required to achieve if successful. Details are available at this link -** [**Right Fit For Risk Cyber Security Accreditation - Department of Employment and Workplace Relations, Australian Government (dewr.gov.au)**](https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation)**.**

The intent of this cyber security questionnaire is to develop a base level of understanding of the security posture of each Responding/Tendering organisation. This questionnaire attempts to determine how your organisation will store and manage data. As such, responses should be collated from staff with the relevant knowledge in your organisation.

Completing this questionnaire is the beginning of meeting the Right Fit For Risk (RFFR) requirements, so it is best read in conjunction with Section 8 Information Technology of a Request for Proposal/Request for Tender.

If a tender response is successful, discussing the completed questionnaire with the with the Digital Partnership Office’s Cybersecurity team allows Providers to achieve the first milestone in the Right Fit For Risk (RFFR) approach to Provider accreditation.

## How to complete this questionnaire

This questionnaire covers a broad range of cyber security topic areas from governance to personnel processes, use of information and communications technology (ICT) services and processes to identify and report a security breach. While multiple staff in your organisation may be involved to answer different sections, the department requests the Respondent/Tenderer’s signatory / CEO sign the declaration.

If you are responding to this RFP/RFT as part of a consortium or a group submission, each organisation must respond to this questionnaire independently.

## Minimum evidence requirements

* All questions must be answered.
* Where required, please provide further information 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 Respondent/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.

## What’s next?

* Your submission will be reviewed and evidence to support your answers may be requested to help the department understand the security posture of your organisation.
* The department will work with successful Respondent/Tenderer’s towards achieving accreditation under RFFR.

# RFFR Tender Questionnaire

|  |  |
| --- | --- |
| **Question** | **Answer** |
| Entity legal/ trading name |  |
| Registered ABN |  |
| Registered address |  |
| Organisation code if you are an existing deed holder (4 digit 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 - 2000 Participants  Over 2,000 Participants |
| 1.2 Please list all Federal government programs you are currently participating in, if any? |  |
| 1.3 How many employees do you currently have in your organisation as a whole? |  |
| 1.4 How many employees will be involved in delivering services under the program described in the tender? |  |
| 1.5 How many physical business sites will deliver services under program described in the tender? |  |
| 1. **Information Security Management System** | |
| 2.1 Does your organisation currently hold any ICT Security Accreditation? If so, please provide the type, date and currency of the accreditation. |  |
| 2.2 Has your organisation participated in RFFR in the past? If yes, please provide details on the milestones achieved including the dates they were achieved. |  |

|  |  |
| --- | --- |
| 2.3 Please describe your knowledge and/or experience of managing an environment for the collecting, storing, processing of information classified at the OFFICIAL:Sensitive level.  A description of Offical:Sensitive information is available at: <https://www.protectivesecurity.gov.au/publications-library/policy-8-sensitive-and-classified-information> |  |
| 2.4 If you are not already RFFR accredited, describe the activities and/or processes you will undertake to develop your Information Security Management System and complete RFFR? |  |
| 2.5 Has your organisation ever performed a Privacy Impact Assessment to address your management of personal information? If you have, what were the results?  Note: You will be required to undertake a Privacy Impact Assessment as part of RFFR accreditation.  See guide <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/> |  |
| 1. **Data Sovereignty** | |
| 3.1 Please explain your understanding of the Data Sovereignty requirements that will be required under a deed with the department? |  |
| 3.2 Are any of your ICT systems based offshore? If so, please provide details in question 6. |  |
| 3.3 Are any of your existing ICT systems accessed from offshore locations? For example, staff working remotely or for administration access. |  |
| 1. **Personnel onboarding** | |
| 4.1 Does your organisation have detailed and documented maturepersonnel onboarding processes? For example, conducting background checks such as Working With Children, Police Check, Referee check, CV validation among others. |  |
| 4.2 Do you provide your staff with information security awareness training that they must complete prior to having access to your systems? |  |

## Essential Eight strategies to mitigate cybersecurity incidents

The Australian Cyber Security Centre (ACSC) 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 as an initial baseline. Additional information on Maturity Levels can be reviewed here: [Essential Eight Maturity Model | Cyber.gov.au](https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model) (cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

The RFFR Statement of Applicability (SoA) provides a detailed list of Essential 8 controls and is available at this link - <https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation/resources/soa-template>.

|  |  |
| --- | --- |
| 1. **Your ISMS Maturity** | |
| **Essential eight implementation**  **Further information on the Essential 8 can be found at this link -** <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model>  **Please ensure this section is completed by your technical specialist.** | |
| **5.1 Essential eight**  **Briefly describe your organisation's approach to implementation of the Essential 8 controls.**  **The following questions refer to the implementation status of each set of controls.** |  |
| **5.2 Application whitelisting/control**  <https://www.cyber.gov.au/acsc/view-all-content/publications/technical-example-application-control> | **Application whitelisting/control is:**  Not Implemented  Planned  Implemented all controls to achieve Maturity Level 1 at the minimum.  Details: |

|  |  |
| --- | --- |
| **5.3 Multi-factor authentication**  <https://www.cyber.gov.au/acsc/view-all-content/publications/technical-example-application-control> | **Multi-factor authentication**  **is:**  Not Implemented  Planned  Implemented all controls to achieve Maturity Level 1 at the minimum.  Details: |
| **5.4 Patch applications**  <https://www.cyber.gov.au/acsc/view-all-content/publications/technical-example-patch-applications> | **Patching Applications is:**  Not Implemented  Planned  Implemented all controls to achieve Maturity Level 1 at the minimum.  Details: |
| **5.5 Office macro settings**  <https://www.cyber.gov.au/acsc/view-all-content/publications/technical-example-configure-macro-settings> | **Office macro settings is:**  Not Implemented  Planned  Implemented all controls to achieve Maturity Level 1 at the minimum.  Details: |
| **5.6 User** **application hardening**  <https://www.cyber.gov.au/acsc/view-all-content/publications/technical-example-user-application-hardening> | **User application hardening is:**  Not Implemented  Planned  Implemented all controls to achieve Maturity Level 1 at the minimum.  Details: |
| **5.7 Restrict administrative privileges**  <https://www.cyber.gov.au/acsc/view-all-content/publications/technical-example-restrict-administrative-privileges> | **Restrict administrative privileges is:**  Not Implemented  Planned  Implemented all controls to achieve Maturity Level 1 at the minimum.  Details: |

|  |  |
| --- | --- |
| **5.8 Patch operating systems**  <https://www.cyber.gov.au/acsc/view-all-content/publications/technical-example-patch-operating-systems> | **Patch operating systems is:**  Not Implemented  Planned  Implemented all controls to achieve Maturity Level 1 at the minimum.  Details: |
| **5.9 Regular backups and testing**  <https://www.cyber.gov.au/acsc/view-all-content/publications/technical-example-regular-backups> | **Regular backups and testing**  **is:**  Not Implemented  Planned  Implemented all controls to achieve Maturity Level 1 at the minimum.  Details: |

|  |  |
| --- | --- |
| 1. Please list all ICT services and products you are using in your IT environment and identify those that will be used to deliver services. | |
| 6.1 Email Hosting:  Describe your email services for example, do you have your own website/domain or do you subscribe to an email service provider |  |
| 6.2 Storage:  Consider your storage needs in terms of both capacity and physical location for example, Cloud Providers, on premise servers, offsite backup etc.  Note: Australia onshore storage is required under a department deed |  |
| 6.3 Cloud Services  Please describe all cloud services that you use including IaaS, SaaS and PaaS  Note: Australia onshore storage is required under a department deed |  |
| 6.4 TPES – Third Party Employment amd Skills Systems:  Client management application purchased from a vendor and managed by the vendor |  |
| **6.5 Managed Services Provider:**  For example, the use of external service providers to manage or deliver any part of your ICT environment, infrastructure, System Administration, and document destruction |  |
| * 1. **Other third-party services:**   Any other ICT service or product that will be used to deliver the service |  |

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

# CEO declaration

I, <Tender signatory / CEO>, on behalf of < organisation > declare that the information provided within this questionnaire is true and correct.

I agree that the department must be notified of any changes in relation to the information supplied in this questionnaire.

I agree to implement or strengthen my organisation’s information security posture as reasonably required by the department, in accordance with the deed and the External Security Assurance Framework (ESAF).

I acknowledge that failure to do so may result in any deed granted on the basis of the questionnaire being revoked.

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

|  |  |  |
| --- | --- | --- |
| **Witness** | **Name** |  |
| **Signature** |  |
| **Date** |  |
| **Email** |  |
| **Phone number** |  |
| **Position** |  |

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