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.

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

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 Questionnaire

### Information about your organisation

|  |  |
| --- | --- |
| **Entity legal/ trading name** |  |
| **Registered ABN** |  |
| **Registered address** |  |
| **Organisation code**  **[This is a unique number specific to your organisation if your organisation is an existing deed holder.]**  **[If your organisation is not an existing deed holder, then leave blank.]** |  |

### Size of your organisation

|  |  |
| --- | --- |
| **How many participants do you intend to service through this RFP/RFT, combined with any other existing deeds with DEWR?**  **[Sum of estimated number of participants currently serviced and those that your organisation is bidding for under the RFP/RFT]** | Under 2,000 participants  Over 2,000 participants |
| **How many individual employees do you currently have in your organisation as a whole?**  **[Full-time, part-time and casual employees are each counted as an individual]** |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Which DEWR programs do you currently or intend to participate in?** | |  | | --- | | **Employment Programs** | |  | |  | |  |  |  | | --- | | **Local Jobs Program** | |  | |  |  |  | | --- | | **Skills Programs** | |  | |  | |  | |
| **Are there any other Federal or state-based government programs that your organisation participates in?** | |  |  | | --- | --- | | **Other Federal/State government programs** | | | **Program** | **Responsible Department** | |  |  | |  |  | |
| **How many individual employees will be involved in delivering services under these programs?**  **[Estimated number of individual employees across current and intended programs being full-time, part-time or casual employees]** |  |
| **How many business sites will deliver services under these programs?**  **[Sum of estimated number of physical sites at which services are currently delivered or will be delivered]** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IT Security Accreditation History | | | | |
| 1. Does your organisation currently hold or is in the process of gaining any ICT security accreditation? | | | | |
| YES, RFFR  [Accreditation gained on achieving Milestone 3] | Date Achieved: \_\_\_\_/\_\_\_\_/\_\_\_\_\_\_  (Date of successful accreditation notification email from the department) | | Date next audit due: \_\_\_\_/\_\_\_\_/\_\_\_\_\_\_  Audit type:  Surveillance  Re-Accreditation  Self-Assessment Review | Proceed to  Q2  6 |
| YES, Other | Please list any other certifications held: | | | Proceed to  Q3  u |
| Date Achieved: \_\_\_\_/\_\_\_\_/\_\_\_\_\_\_ | | Date next audit due: \_\_\_\_/\_\_\_\_/\_\_\_\_\_\_  Audit type:  Surveillance  Re-Accreditation |
| Yes, Some RFFR Milestones | | Milestone 1 achieved on: \_\_\_\_/\_\_\_\_/\_\_\_\_  Milestone 2 achieved on: \_\_\_\_/\_\_\_\_/\_\_\_\_  (Date of successful milestone notification email from the department, If you are intending to submit, please add this date in the additional information field.) | | Proceed to  Q3  u |
| *NO,* we have not attained any accreditation through existing DEWR contracts. | | | |
| *NEVER,* been required to complete any accreditation. | | | |

|  |  |
| --- | --- |
| 1. Do you intend to implement significant changes to your ICT environment should you be successful and contracted to deliver the services from this RFP/RFT? | |
| YES | Please elaborate: |
| NO | You intend to maintain the same ICT environment as covered under your RFFR accreditation. |
| As you have already achieved accreditation under RFFR, please complete the declaration on the last page. uu | |

|  |
| --- |
| Respondent/Tenderers that are not currently accredited under RFFR will need to complete all following questions. |

|  |  |  |
| --- | --- | --- |
| 1. Do you intend to deliver your services for this contract in one of the following structures? | | |
|  | Responding as a sole organisation | |
|  | Responding as part of Consortium / Group with separate ICT Environments  If you are responding to this RFP/RFT as part of a consortium or a group submission, please have each organisation respond to this questionnaire independently. | Other Members: |
|  | Lead Organisation with subcontracting organisations to deliver services under this contract [Noting a Lead Organisation is responsible for ensuring the IT security of any subcontractor]. | Subcontractors: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. Managing Personal Information | | | | |
| Will you be managing personal information as a result of delivering the services?  For example, if the services will grant you access to departmental systems to manage a caseload of participants, you will most certainly be managing personal information in this contract.  Guiding questions:   * Will your organisation be collecting, storing, processing, using or disclosing any personally identifiable information (PII) of participants as a result of delivering the services you are bidding for? Examples include name, residential address, email address, training course attendance/results. * Will your organisation be collecting, storing, processing, using or disclosing any sensitive information as a result of delivering the services you are bidding for? Examples include details of an individual’s disability or their mental health.   See guide from [https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information](https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/) | | | YES | NO    If NO, please complete the declaration on the  last page.  uu |
| If YES   1. Have you performed a Privacy Impact Assessment to address your appropriate management of personal information?   See guide [https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/).  Please elaborate:   1. Have you prepared and tested a Data Breach Response Plan?   See guide <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response>  Please elaborate:   1. Are you committed to making the necessary improvements to information management and cyber security in your organisation in accordance with the department’s ESAF?   See Section 8 – Information technology of the RFP/RFT made available by the department from the RFP/RFT documentation.  Please elaborate: | | | | |
| 1. Please list all ICT services and products you are using or intending to use: | | | | | |
|  | Current | Planned | | | |
| Email Hosting:  (Is your email stored in Australia?) |  |  | | | |
| Storage:  (consider your storage needs in terms of both capacity and physical location e.g. Cloud Provider, local servers, offsite backup etc.) |  |  | | | |
| IaaS – Infrastructure as a Service:  (an instant computing infrastructure, provisioned and managed over the internet. e.g. Microsoft Azure, Amazon AWS, IBM cloud) |  |  | | | |
| SaaS - Software as a Service:  (a method of software delivery and licensing in which software is accessed online via a subscription, e.g. MYOB, Microsoft Office, etc.) |  |  | | | |
| PaaS – Platform as a Service:  (is a set of services to build and manage modern applications in the digital era. e.g. of PaaS companies including IBM, Microsoft etc.) |  |  | | | |
| TPES – Third Party Employment System:  (Client management application purchased from a vendor and managed by the vendor) |  |  | | | |
| ***Managed Services Provider:***  (is the use of external services to manage or deliver any part of your ICT environment, infrastructure, System Administration and document destruction) |  |  | | | |
| **Other third party services:** |  |  | | | |

|  |  |
| --- | --- |
| 1. Are Data Sovereignty requirements met by your current ICT environment?   *DATA SOVEREIGNTY - Data in your organisation cannot be stored, sent or accessed from offshore locations; and only persons who hold Australian Citizenship or Permanent Residency may be granted privileged / administrator access to your ICT systems.*   * *If you are using a cloud storage service, your data cannot be stored offshore.* * *Software applications cannot be stored, backed up or accessed offshore.* * *If you choose to use an outsourced help desk, they are not located offshore.* | |
| Yes | In our ICT environment, data cannot be stored, sent or accessed from offshore in our organisation and no systems are administered by persons who are not Australian Citizens/Permanent Residents of Australia. |
| No | *Our ICT environment has not been established to ensure that Data cannot be stored, sent or accessed from offshore in our organisation, and/or certain systems are administered by persons who are not Australian Citizens/Permanent Residents of Australia.*  *Please elaborate:* |
| Intended | *Our ICT environment will be reviewed and altered to ensure that Data cannot be stored, sent or accessed from offshore of our organisation and that no systems are administered by persons who are not Australian Citizens/Permanent Residents of Australia.* |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. **Please list the details of your personnel onboarding processes.** | | | |
| Basic Onboarding | Check the following as applicable to your organisation:   * Check references with previous employer * Conduct Interview | Implemented as indicated  Planned |
| Evolving Processes | All of the above plus (check as applicable):   * Staff sign confidentiality agreements on commencement * Police checks are completed * Qualifications are checked (e.g. sighting certificate) | Implemented as indicated  Planned |
| Mature Process | All of the above plus (check as applicable):   * Staff **and contractors** sign confidentiality agreements on commencement * Positive identity checks are completed * Working with vulnerable people checks are completed where required * Employment history check is completed * Entitlement to work in Australia check is completed | Implemented as indicated  Planned |

|  |  |  |
| --- | --- | --- |
| 1. Do you provide your staff with information security awareness training that they must complete prior to having access to your support systems or government data? (tick all applicable) | | |
| No training provided | Training is in planning | Training on Induction |
| Annual refresher course | Departmental systems access training | additional IT Security training based on role |
| Training specific to incident | Ad hoc awareness campaign | IT security spot checks of staff |
| Other: | | |

## 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)

1. **Please indicate how your ICT systems rate against the Essential Eight:**

|  |  |
| --- | --- |
| **Essential Eight # 1 - Application control** | |
| **Application control** is a security approach designed to protect against malicious code (also known as malware) executing on systems. It ensures that only approved applications (e.g. executables, software libraries, scripts and installers) can be executed.While traditional antivirus tools prevent “known bad” code from executing, application control only allows ‘known good’ code to execute – a higher standard of protection against new threats that have not yet been included in antivirus databases.  **Application control b**locks the user from running unapproved executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets on their computer or network. | **Application control is:**  Not Implemented  Planned  Implemented at Maturity Level 1 at the minimum |
| **Maturity Level 1** |
| The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients . |

|  |  |
| --- | --- |
| **Essential Eight # 2 - Patch Applications** | |
| All applications software must be maintained to be as free of known vulnerabilities as possible. When a vulnerability is found after the release of a piece of software, a patch can be used to fix it. Doing so helps ensure that assets in your environment are not susceptible to exploitation. Some applications automatically check for patches, while others require methods for identifying when a patch is available. | **Patching Applications is:**  Not Implemented  Planned  Implemented at Maturity Level 1 at the minimum |
| **Maturity Level 1 – all of the following** |
| Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within 2 weeks of release, or within 48 hours if an exploit exists.  Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products are applied within one month of release.  A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.  A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software and security products.  Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player and security products that are no longer supported by vendors are removed. |

|  |  |
| --- | --- |
| **Essential Eight # 3 - Configure Microsoft Office macro settings** | |
| Microsoft Office files can contain embedded code (known as a macro) written in the Visual Basic for Applications (VBA) programming language.  A macro can contain a series of commands that can be coded or recorded and replayed at a later time to automate repetitive tasks. Macros are powerful tools that can be easily created by novice users to greatly improve their productivity. However, an adversary can also create macros to perform a variety of malicious activities, such as assisting in the compromise of workstations in order to exfiltrate or deny access to sensitive information. | **Configuration of Microsoft Office macro settings is:**  Not Implemented  Planned  Implemented at Maturity Level 1 at the minimum |
| **Maturity Level 1 – all of the following** |
| Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.  Microsoft Office macros in files originating from the internet are blocked.  Microsoft Office macro antivirus scanning is enabled.  Microsoft Office macro security settings cannot be changed by users. |
| **Essential Eight # 4 - User application hardening** | |
| Application hardening is an overall term for “hardening” or protecting an application against intrusions by eliminating vulnerabilities and increasing layers of security.  By default, many applications enable functionality that is not required by users while security functionality may be disabled or set at a lower security level. This is especially risky for key business applications such as office productivity suites, PDF viewers, web browsers, common web browser plugins, email clients and software platforms that are likely to be targeted by an adversary. To assist in minimising this security risk, the ACSC produces guidance to assist in securely configuring key business applications. Further, to assist in securely configuring their applications, vendors may provide their own security guides. | **User application hardening is:**  Not Implemented  Planned  Implemented at Maturity Level 1 at the minimum |
| **Maturity Level 1 – all of the following** |
| Web browsers do not process Java from the internet.  Web browsers do not process web advertisements from the internet.  Internet Explorer 11 (if used) does not process content from the internet.  Web browser security settings cannot be changed by users. |

|  |  |
| --- | --- |
| **Essential Eight # 5 - Restrict administrative privileges** | |
| Restricting administrative privileges is one of the most effective mitigation strategies in ensuring the security of systems.  Users with administrative privileges for operating systems and applications are able to make significant changes to their configuration and operation, bypass critical security settings and access sensitive information. Domain administrators have similar abilities for an entire network domain, which usually includes all of the workstations and servers on the network.  Adversaries often use malicious code (also known as malware) to exploit security vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for an adversary’s malicious code to elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information or resist removal efforts.  An environment where administrative privileges are restricted is more stable, predictable and easier to administer and support, as fewer users can make significant changes to their operating environment, either intentionally or unintentionally. | **Restriction of administrative privileges is:**  Not Implemented  Planned  Implemented at Maturity Level 1 at the minimum |
| **Maturity Level 1 – all of the following** |
| Requests for privileged access to systems and applications are validated when first requested.  Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.  Privileged users use separate privileged and unprivileged operating environments.  Unprivileged accounts cannot logon to privileged operating environments.  Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. |

|  |  |
| --- | --- |
| **Essential Eight # 6 - Patch operating systems** | |
| Common areas that will need patches include operating systems and firmware for embedded systems (like network equipment). When a vulnerability is found after the release of a piece of software, a patchcan be used to fix it. Doing so helps ensure that assets in your environment are not susceptible to exploitation. When a system or service can be accessed from outside the organisation, such as a company website or a remote access solution for your staff, patching becomes much more important.  Patches for security vulnerabilities are provided by vendors in many forms, such as:   * fixes that can be applied to existing operating system and firmware versions * fixes incorporated into new drivers that require pre-existing versions to be replaced * fixes that require the overwriting of firmware on ICT equipment. | **Patch operating systems is:**  Not Implemented  Planned  Implemented at Maturity Level 1 at the minimum |
| **Maturity Level 1 – all of the following** |
| Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within 2 weeks of release, or within 48 hours if an exploit exists.  Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release.  A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services.  A vulnerability scanner is used at least fortnightly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices.  Operating systems that are no longer supported by vendors are replaced. |

|  |  |
| --- | --- |
| **Essential Eight # 7 - Multi-factor authentication** | |
| Multi-factor authentication is defined as ‘a method of authentication that uses 2 or more authentication factors to authenticate a single claimant to a single authentication verifier’.  The authentication factors that make up a multi-factor authentication request must come from 2 or more of the following:   * something the claimant knows (e.g. a personal identification number (PIN), password or response to a challenge) * something the claimant has (e.g. a physical token, smartcard or software certificate) * something the claimant is (e.g. a fingerprint or iris scan). | **Multi-factor authentication is:**  Not Implemented  Planned  Implemented at Maturity Level 1 at the minimum |
| **Maturity Level 1 – all of the following** |
| Multi-factor authentication is used by an organisation's users if they authenticate to their organisation’s internet-facing services.  Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.  Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.  Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation’s internet-facing services. |

|  |  |
| --- | --- |
| **Essential Eight # 8 - Regular backup** | |
| In information technology, a backup, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event. To mitigate the likelihood of data becoming unavailable due to accidental or malicious deletion of backups, organisations should ensure that backups are protected from unauthorised modification, corruption and deletion. | **Regular backup is:**  Not Implemented  Planned  Implemented at Maturity Level 1 at the minimum |
| **Maturity Level 1 – all of the following** |
| Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements.  Restoration of systems, software & important data from backups is tested in a coordinated manner as part of disaster recovery exercises.  Unprivileged accounts can only access their own backups.  Unprivileged accounts are prevented from modifying or deleting backups. |

|  |
| --- |
| 1. Have you planned to put any new or enhanced protective measures in place to protect data entrusted to you under this agreement? (This could include plans or schedules with timeframes where you are implementing processes to align with industry standard) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Area of Improvement:  *EXAMPLE*  Encryption | Actions Planned | e.g. Implement encryption on data at rest and in transit | | |
| Planned start date: | 01/09/2021 | Planned completion date: | 01/12/2021 |

**Add additional tables for each area of improvement:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Area of Improvement: | Actions Planned |  | | |
| Planned start date: |  | Planned completion date: |  |

## Additional information

Please use this section to provide additional information, including a brief explanation if questions were not considered applicable to your organisation.

|  |  |
| --- | --- |
| **Question #** | **Comment** |
| *EXAMPLE*  ***Question 1:***  ***Future submission of RFFR Milestones*** | ***Our organisation is currently working on RFFR accreditation and intended submission date of Milestone 3 is 15/12/21.*** |
|  |  |

# CEO declaration

I, <Respondent/Tenderer 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 revoked.

|  |  |  |
| --- | --- | --- |
| **Respondent/Tenderer Signatory / CEO** | **Name** |  |
| **Signature**  **[May be signed electronically]** |  |
| **Date** |  |
| **Email** |  |
| **Phone number** |  |
| **Position** |  |

|  |  |  |
| --- | --- | --- |
| **Witness** | **Name** |  |
| **Signature**  **[May be signed electronically]** |  |
| **Date** |  |
| **Email** |  |
| **Phone number** |  |
| **Position** |  |

Please submit your completed questionnaire as part of your RFP/RFT response to be uploaded in 360Pro.