**Digital Service Provider – Operational Framework Security Questionnaire**

|  |  |
| --- | --- |
| The intent of this questionnaire is to develop a base level understanding of the security posture of Digital Service Provider (DSP) products and their supply chain arrangements.  This document follows the DSP Operational Framework requirements. This questionnaire is best read in conjunction with the DSP Operational Framework [DSP Operational Framework implementation approach](https://softwaredevelopers.ato.gov.au/Operational_framework_wgFebruary2018). | |
|  | * Where you have answered yes to a question, evidence must be provided. Where you have answered no or in progress, further details as to why this control is not in place or what steps you are taking to implement this control must be provided. * General section questions are to be answered by all DSPs, sections 1, 2, 3, 4 and 5 have been tailored, please follow the questions before and after each section to determine what sections apply to you. You need to provide an answer to all questions in the sections that are relevant to you * Responses to this questionnaire need to be true and correct to the best of your knowledge. Providing false or misleading information in this questionnaire could lead to your software product or service being de-whitelisted.   If you need assistance in completing this questionnaire please contact the Digital Partnership Office ([DPO@ato.gov.au](mailto:DPO@ato.gov.au)) |

**General Information Section - Operational Framework Security Questionnaire**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Suitable Evidence** | **Response** | **Details and Attached Evidence** |
| **G1: Standard Business Reporting (SBR) Software**  - Are you currently using SBR software with the ATO or other government departments? | * Details of the SBR software product and applicable agency | * Yes * No * In progress |  |
| **G2: Personnel Security**  - Can you confirm that all personnel who will have any access to ATO Taxpayer information have satisfied personnel security integrity check process? (e.g. Police Checks) | * Internal policy document * Process description | * Yes * No * In progress |  |
| **G3: Data Protection**  - Can you supply details of your encryption in transit practices?    Examples  *ASD Approved Cryptographic Algorithms fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms.* | * Configuration files or screen shots (of the configuration page) * Message header which has the algorithm definition * Product data sheet/white papers (together with Product purchase/ownership documentation such as receipts, front page of a contract of product/support/service) * Federal Information Processing Standard Validation documents (US government computer security standard, e.g. FIPS 140-2) * Product Common Criteria Evaluation documents * Product Evaluation Assurance Level (EAL) documents | * Yes * No * In progress |  |
| **G4: Audit Logging**  –Can you provide assurance that your product or service captures and stores audit logs? | * Internal policy document * Process description Internal policy document * Process description | * Yes * No * In progress |  |

|  |
| --- |
| **Thank you for responding to the general questions section. Please read below to assess whether you need to provide additional responses to this questionnaire based on your individual circumstances.** |
| **Hosting of your software product or service**   * Is the software product or service stored and managed by the client?   + - Yes. **Please respond to section 1**     - No. **Please read on.** * Is the software product or service stored and managed by you as a DSP and consumes ONLY no/low risk APIs?   + - Yes. **Please respond to section 1.**     - No. **You do not need to respond to section 1. Please proceed directly and respond to section 2.** |

**Section 1 - Operational Framework Security Questionnaire**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Suitable Evidence** | **Response** | **Details and Attached Evidence** |
| **1.1: System Certification**  - Can you demonstrate the security posture of your product(s) / operating environment by suppling the ATO with a completed self-assessment or documented conformance with one of the following approved security standards:  • iRAP  • ISO/IEC 27001  • OWASP ASVS 3.0  • SOC2 | * Completed documentation demonstrating your conformance with the requirements (full control suite) of one of the approved security standards outlined above. | * Yes * No * In progress |  |

|  |
| --- |
| **Thank you for responding to section 1. Please read below to assess whether you need to provide additional responses to this questionnaire based on your circumstances.** |
| **Connecting to the ATO**   * Is the software product or service, which is stored and managed by the client, connecting directly to the ATO?   + - Yes. **You have now completed the required sections of the Operational Framework Security Questionnaire. Please submit the completed questionnaire and evidence to the Digital Partnership Office.**     - No. **Please respond to section 2.** * All other DSPs:   + - **Please respond to section 2.** |

**Section 2 - Operational Framework Security Questionnaire**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Suitable Evidence** | **Response** | **Details and Attached Evidence** |
| **2.1: Supply Chain Security**  – Can you supply the ATO with the details of the participants in your supply chain? | * Business details required: entity name, ABN, service provider role and or function (i.e. sending service provider, gateway)   *\* The ATO is developing a technical solution to provide visibility of the supply chain in the SBR message content. In the meantime the ATO still requires detail on what and who is in your supply chain.* | * Yes * No * In progress |  |
| **2.2: Payload Encryption** – TBA | * TBA   *\* Payload encryption solution is not currently available, but will be developed in the near future.* | * Yes * No * In progress |  |

|  |
| --- |
| **Thank you for responding to section 2. Please read below to assess whether you need to provide additional responses to this questionnaire based on your circumstances.** |
| **Supply Chain and Storage**   * Is the software product or service stored and managed by the client?   + - Yes. **You have now completed the required sections of the Operational Framework Security Questionnaire. Please submit the completed questionnaire and evidence to the Digital Partnership Office.**     - No. **Please respond to section 3.** |

**Section 3 - Operational Framework Security Questionnaire**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Suitable Evidence** | **Response** | **Details and Attached Evidence** |
| **3.1: Hosting Environment** **Security**  - Can you verify that your software product will use an ASD certified environment? | * Name of the provider * Provider location (onshore / offshore), * Redundancy location (Redundancy also onshore) required.   *\*Note: Your product or service is required to be hosted onshore by default with offshore hosting arrangements managed by exception only. If your product hosts data offshore please discuss this further with us.* | * Yes * No * In progress |  |
| **3.2: Multi-factor Authentication**  - Does your product support mandatory multi-factor authentication on user log in? | * Published product description, user manual, user description, user instructions paired with screen shots of the user interface.   *\*A transition strategy exists for existing DSPs, please refer to the Operational Framework implementation approach.* | * Yes * No * In progress |  |
| **3.3: Data Protection at Rest**  - Can you supply details of your encryption at rest practices?  Examples  *PGP – AES, BitLocker – AES, gemalto SafeNet – AES/3DS, Azure Storage Service Encryption (SSE) for Data at Rest – AES, THALES Vormetric – AES* | * Configuration files or screen shots (of the configuration page) * Product data sheet/white papers (together with Product purchase/ownership documentation such as receipts, front page of a contract of product/support/service) * Federal Information Processing Standard Validation documents (US government computer security standard, e.g. FIPS 140-2) * Product Common Criteria Evaluation documents * Product Evaluation Assurance Level (EAL) documents | * Yes * No * In progress |  |
| **3.4: Encryption Key Management**  - Can you verify your encryption key management (including PKI keys) complies with ASD/industry guidelines? | * Key Management Plan (internal documentation) | * Yes * No * In progress |  |

|  |
| --- |
| **Thank you for responding to section 3. Please read below to assess whether you need to provide additional responses to this questionnaire based on your circumstances.** |
| **Consumption of APIs and Volume of Taxpayer data**   * Is the software product or service holding or transacting high volumes of taxpayer or superannuation records (>10k accessible individual taxpayer or superannuation related information records)?   + - Yes. **You not need to respond to section 4. Please proceed directly and respond to section 5.**     - No. **Please read on.** * Is the software product or service consuming ONLY no/low risk APIs?   + - Yes. **You have now completed the required sections of the Operational Framework Security Questionnaire. Please submit the completed questionnaire and evidence to the Digital Partnership Office.**     - No. **Please respond to section 4.** |

**Section 4 - Operational Framework Security Questionnaire**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Suitable Evidence** | **Response** | **Details and Attached Evidence** |
| **4.1: System Certification**  - Can you demonstrate the security posture of your product by suppling the ATO with a completed self-assessment or documented conformance to one of the approved following standards:   * iRAP * ISO / IEC 27001 | * Completed documentation demonstrating your conformance with the requirements of one of the chosen approved security assessments. | * Yes * No * In progress |  |
| **4.2: Security Monitoring Practices**  - Can you verify that monitoring is conducted within your environment(s)?  Examples   * *Network / Infrastructure layer examples - NIPS/NIDS, Anomaly detection systems, , Log analysis systems/ Security Information and Event Management (SIEM) tools, Data Centre protection suites , Host based IDS/IPS, System integrity verification tools, Application whitelisting tools (with alert generation), Firewalls/proxies (with alert generation)* * *Application Layer example - Application built-in monitoring/alert capability (e.g. monitor unusual patterns of user behaviours in the application)* * *Transaction (data) layer example - Monitor unusual patterns of transactions/data (e.g. too large/small figures/transactions and etc.)* | Network / Infrastructure layer:   * Screen shots (product page, the management console page) * Product purchase/ownership doco (e.g. receipts, front page of a contract of product/support/service) * Configuration files * Photos of the product * Photos of SOC/SIEM centre (using the products)   Application layer:   * Screen shots of the function page in the application * Reports from the backend system     Transaction (data) layer:   * Reports from the backend system * Previous unusual casesPublished product description, user manual, user description, user instructions paired with screen shots of the user interface. | * Yes * No * In progress |  |

|  |
| --- |
| **Thank you for responding to section 4.** |
| **You have now completed the required sections of the Operational Framework Security Questionnaire. Please submit the completed questionnaire and evidence to the Digital Partnership Office.** |

**Section 5 - Operational Framework Security Questionnaire**

|  |  |  |  |
| --- | --- | --- | --- |
| **Question** | **Suitable Evidence** | **Response** | **Details and Attached Evidence** |
| **5.1: System Certification**  - Can you supply the ATO with current, evidentiary documentation demonstrating the security posture of your product in line with one of the following standards:   * iRAP * ISO / IEC 27001   *\*Please note that these certification types must be conducted by a qualified, independent assessor and must be renewed at regular intervals in line with the standard’s requirements.* | * Independently assessed report including Scoping documentation and Certificate of Compliance/Registration or Statement of Applicability with Certificate of Compliance/Registration) to:   + iRAP,   + ISO / IEC 27001 | * Yes * No * In progress |  |
| **5.2: Security Monitoring Practices**  - Can you verify that monitoring is conducted within your environment(s)?    Examples   * *Network / Infrastructure layer examples - NIPS/NIDS, Anomaly detection systems, ,Log analysis systems/ Security Information and Event Management (SIEM) tools, Data Centre protection suites , Host based IDS/IPS, System integrity verification tools, Application whitelisting tools (with alert generation), Firewalls/proxies (with alert generation)* * *Application Layer example - Application built-in monitoring/alert capability (e.g. monitor unusual patterns of user behaviours in the application)* * *Transaction (data) layer example - Monitor unusual patterns of transactions/data (e.g. too large/small figures/transactions and etc.)* | Network / Infrastructure layer:   * Screen shots (product page, the management console page) * Product purchase/ownership doco (e.g. receipts, front page of a contract of product/support/service) * Configuration files * Photos of the product * Photos of SOC/SIEM centre (using the products)   Application layer:   * Screen shots of the function page in the application * Reports from the backend system     Transaction (data) layer:   * Reports from the backend system * Previous unusual cases | * Yes * No * In progress |  |

|  |
| --- |
| **Thank you for responding to section 5.** |
| **You have now completed the required sections of the Operational Framework Security Questionnaire. Please submit the completed questionnaire and evidence to the Digital Partnership Office.** |