Instructions to assist SWD to complete the security operational questionnaire

The following information assists Software Developers (SWD) to complete the questions in the attached Security Practice Questionnaire (the Questionnaire) provided by the ATO to Practitioners using third-party software products and services.

Background

The Commonwealth's Digital Transformation Office (DTO) *Third Party Identity Services Assurance Framework*, defines level of Assurance as "A level of confidence in a claim, assertion, credential or service". The ATO is required to determine by the Government on which level of Assurance is needed for its risk management of digital services.

Accordingly, the ATO provides a security practice questionnaires to its Software Developers to complete and provide evidence when available as a part of whitelisting process. The questionnaires are based on relevant ISO/IEC standards. However, the Questionnaires are simplified with key operational areas that the ATO needs to know.

In the early version of the self-declaration security assessment questionnaires, many of these questions require "***assurance***" that a required level of security performance is reached by SWD's product. Assurance in this context is defined in ISO/IEC 15026: 2013 Part 1 Systems and software engineering – Systems and software assurance – Concepts and vocabulary as "**grounds for justified confidence that a claim has been or will be achieved**".

The references to Standards should not be taken to state that compliance with every control in the Standards is required. These references are only a guide to best practice in IT security. They are intended to show the extent or nature of the evidence to be used to support a rating of "Yes" in the Self-declaration.

For example, the mention of ISO/IEC 27034-2: 2015 is to draw out SWD's familiarity with security in product development rather than a specification of how SWD carry out the development.

If ISO standards are not used then SWD needs to show evidence that SWD's practices are of an equivalent quality.

Completion of Questionnaire

The questionnaire must be completed for each product provided by the SWD.

- Several questions have been asked by the ATO (SBR) before, such as when SWD have sought to obtain an AUSKey. It is still necessary to answer them here, to ensure that the information is up-to-date and linked to the rest of the requirements in order to provide a complete assessment of the extent to which the pertinent product can be trusted.
- Please rate **Yes** to each question with which SWD fully comply. That is, if SWD's practices have been designed with knowledge of the Standards, tailored as allowed, or have been certified against the given framework.
- Answer "***with in progress***" with a percentage that indicates the extent to which SWDs have taken account of the relevant Standards or frameworks in the current practices. For example, if SWDs are aware of the Standard but have not yet been able to follow its recommendations, then give a rating of 25%. If SWD are aware of the Standards and have been able to meet most of its recommendations so far the given a rating of 50%. If SWDs have been able to follow almost all of the recommendations but have not yet been fully certified against them, for example, then rate SWD themselves at 75%.
- Answer **No** if SWDs do not know of the Standards or have disregarded them (for given reasons).

Provision of Evidence

The answers must be accompanied by evidence to support the claims if possible. The evidence can be in the form of copies of the relevant certificates, if relevant; policy documents; procedural manuals; or similar documents that show the extent to which the self-declarations are valid. Full documents are not required, just tables of contents of manuals or similar summaries that show that the documents exist.

SWD is expected to be able to produce the full documents when asked by the assessors (when they are determined).

Further ATO Action

- After SWDs have lodged this Self-Declaration with the SIPO or the onboarding team, the ATO) will check the evidence that SWD have supplied and determine whether their rating should be adjusted.
- It will then use these ratings to assess the extent to which their product can be trusted because it has the abilities given below. This assessment will be based upon a model of the contributions that each category of answer makes the objectives reflected in the abilities in management of operational security risks.
- A rating of more than "**acceptable score / value**" will lead the ATO placing its product on the Software Register (whitelisted).
- If it is not placed in the Register, SWD product can still be used with ATO provided data but every message sent by it to the product will be subjected to additional verification and **monitoring**.
- If "the total score" is under "acceptable", there is a grace period for existing SWDs to change its performance and seek re-assessment
- For all new SWD, the security operational questionnaire must be completed before product can be 'registered / whitelisted".

Self-assessment by Suppliers of Software Products or Services (SWD) of Extent of meeting Security requirements

Objectives

The ATO needs your help in ensuring that it can build public trust and confidence in the tax and super systems as it makes more use of digital services. In order to build this trust, it must meet the following business objectives and constraints:

Keep tax and super information:

- Confidential to only authorised users – be they ATO staff, Practitioners, or taxpayers dealing with their own data
- With complete integrity – free from accidental or malicious alteration
- Yet available for use by authorised users when they need it

In a manner that is

- Efficient for all users
- Compliant with relevant taxation, privacy, or similar legislation

These objectives and constraints must be met for information that is sent to the ATO or is sent by the ATO, over all of the systems that link the taxpayers through the Practitioner and services that they use to the ATO.

Requirements

These objectives and constraints will be achieved only if the software products and services provided to Practitioners help them to

- Prevent malicious or accidental loss or alteration of data sent by the ATO to Practitioners, either in transit or whilst stored on systems used between the ATO and Practitioners or between Practitioners and their clients
- Prevent unauthorised access to such systems so that information cannot be used for fraudulent purposes

Assurance sought

The ATO needs to know the extent of trust that can be placed on suppliers of products or services, such as SWD, based upon assurance they provide about whether they can contribute to meeting the requirements listed above. At this stage, this assurance will be obtained through the self-assessment and supporting evidence sought in the following questionnaire.

The responses to these questionnaires will be assessed by ATO to see whether suppliers of products or services used by Practitioners can show that they have trustworthy arrangements for their software products, services and operational environments.

As outlined in the ATO's third-party products and services security policy, the ATO will monitor security practices and performance, as well as update relevant requirements and processes to reflect the evolving risk sources. The ATO requires evidence from you to support your claims made in the self-assessment and it will monitor the extent of trust that can be placed upon the use of your products for the provision of ATO-sourced information to Practitioner systems.

Category	Necessary Quality of Product or Service	Source of Evidence supporting declaration	Self-declaration (CD) / answer				
	The following minimum requirements are largely based on ISO 27001, 27002, 27005, and 27034 (various parts), as well as relevant industry best practices in Product, Environment, and Practice aspects. They provide measures of good security practice and the maturity of SWD regarding digital security risk management.	**Attach copies of certificates, authorisations, or approvals; citations of relevant documents**	**Yes**	**In Progress (%)**	**Need assistance**	**No**	**N/A**
General Info	ATO needs to know if you have already have established credentials for dealing with ATO						
	• Extent to which you have already sought accreditation or authentication to use ATO information						
	• Do you have SSID or AUSKey?						
	• Do you have ABN / TAN?						
API tests	The ATO provided APIs must be used for the intended and agreed business purpose and by authorised personnel. Describe the evidence that you have carried out security tests for the suitable use of ATO APIs.						
	• Have applications and APIs undergone security tests by certified independent parties that provide assurance about the trustworthiness of APIs?						
Standards	The ATO needs the SWD to meet basic security requirements, which are largely based on ISO/IEC 27001, 27002: 2013, 27005, and the parts of 27034and OWASP.						
	• Does the product development follow the ISO standards above, such as ISO/IEC 27034-2: 2015?						
	• Does the product follow other industry standards relevant to the security o data processed by it? Name them and explain their use.						
Risk Management	In addition to the product's conformance tests , products must undertake security tests to manage the risks arising from the following sources:						
	• Has your product been tested for protection from malicious code injection attacks (by SQL, html, php and script, for example)						
	• Has your product been developed to prevent unauthorised access, extraction, manipulation or deletion of data from a Practitioner's system?						
Authentication	The ATO requires assurance that the product(s) have required authentication						

	and authorisation features						
	• Are those features compatible with NeAF?						
	• Can the products be configured for user access controls when storing and transferring data from the ATO?						
Protection in Transit	The ATO requires assurance that client data or metadata obtained from the ATO is capable of being encrypted within the systems using the product.						
	• Are data encrypted whilst transmitted from the ATO?						
	• Are data encrypted whilst stored on Practitioner systems?						
	• Are ASD approved Cryptographic Protocols and ASD Approved Cryptographic Algorithms (AACAs) used for all encryption involving data obtained from the ATO						
	• Does PKI key management comply with ASD / industry guidelines?						
Environmental aspect	The ATO needs assurance that ICT systems used for data communication with the ATO and other external suppliers are secured adequately, as described in relative sections in ISO/IEC 27034						
	• Can you prevent clients accessing any data that is not their own?						
	• Can the product be configured for user access controls when transferring data from the ATO?						
	• Can all product logs be correctly configured and verified by independent security assessors?						
	• Is the allocation and use of privileged access rights controlled?						
	• Can the development systems monitor processes to ensure applications are adhering to security requirements?						
Business entity/ organisational aspect:	The ATO needs assurance that the policies and procedures used within the SWD follow ISO/IEC 27034, or equivalent industry standards in digital security and risk management regarding organizational operations						
	• Do all personnel who develop systems that enable access to client information undergo security checks, regular training to be compliant with industry code of conduct, and have adequate authentication requirements?						
	• Do you have published security policies regarding the hiring and supervising of personnel?						
	• Do all personnel who develop systems that enable access to client information receive regular training to be compliant with industry codes of conduct?						
	• Do you have staff with certification in application security?						

	• Do you have an incident management system that can be used for continuous improvement of the security of your applications ?						
Self-assessment	**Name:**	**Date:**					