dspanz. digital service providers australia new zealand

SSAM Review Session 1 - Meeting Summary & Outcomes

Agenda Item	Description
1	**Welcome and Acknowledgment of Country** Matthew Prouse welcomed attendees to the session and acknowledged the Traditional Owners.
2	**Purpose of the Review** Simon Foster covered the purpose of the review: ● Two years since it was released ● Now actively used by DSPs who are reporting to the ATO as required by OSF ● Release of OSF version 6 ● To understand how SSAM is being used and identity any issues or gaps
3	**Overview of SSAM Review** Simon Foster covered the proposed overview for each of the sessions in the review and asked for feedback to be provided out of session. Any feedback can be emailed to maggie@dspanz.org. **Session 1: Operational Security Framework V6 changes and the potential impacts on SSAM** - *Uplifted requirements in OSFv6* - *New controls added to the OSF* - *Definition of a DSP* - *SSAM documentation* **Session 2: Review of received feedback on the implementation and operation of SSAM** - *Experiences of DSPs* - *Experiences of Add-on developers* - *Breach reporting* - *Key learnings and opportunities* **Session 3: Overlap of SSAM and other security standards** - *SSAM and CDR Rules* - *SSAM and FAPI 2.0* - *SSAM and Essential Eight* - *Accreditation and Certification*
4	**Summary of the DSP Operational Security Framework V6 for "Category A" DSPs** Diana Porter covered the review of the OSF including the changes to requirements. She noted that the OSF will continually evolve and adjust to mitigate identified risks. Updated requirements released through DSP newsletter on 18 August. Software developer website is also being updated and a new version of the questionnaire is expected to be released in the next DSP newsletter. Diana is happy to circulate more detailed information if required. **Action**

	Diana to come back with more information about how SOC2 and ISO27001 apply in the OSF.
5	**Walkthrough of the current SSAM documentation and identify possible areas for security uplift or enhanced documentation** Matthew Prouse covered that the SSAM is currently a set of technical security controls and not operational controls. It's estimated that around 1,000 apps have certified themselves against the SSAM. The ATO are building out better reporting on this through the OSF. *Encryption key management* ● Opportunity to go from OAuth 1.0 to OAuth 2.0 *Encryption in transit* ● Should we uplift from TLS 1.1 to 1.2 at a minimum? ● What would be the impacts on apps? ● A reasonable timeframe to do that uplift *Authentication* ● Should we change from two-step authentication to multi-factor authentication? ● Should information be added around what are appropriate MFA options (like what has been added in the OSF)? *Server configuration* ● Want to include patch management and periodicity of this ● Don't want it to be a set and forget *Encryption at rest* ● Are the definitions of personal and commercial information right? ● If it stores a TFN, it should be classified as a DSP? *Audit logging* ● Is it okay to not specify a log format? ● Monitoring and alerting should be called out specifically ● Should be looking at logs ● If they're not searchable, they don't serve a purpose ● Information on how you store logs and what you store in them? *Data hosting* ● Should more guidance be provided or is this enough? *Operational controls* Discussed the opportunity to add operational controls such as: ● Restricting administrator access ● Segregation of duties in change management process But noted that these may not be easier for smaller developers to comply with. Options to either tier the SSAM or provide a decision tree depending on what a developer is aiming to achieve. Noted that many developers will rely on their infrastructure to meet controls for them with Azure, AWS etc providing out of the box solutions. Opportunity for DSPANZ to

	list solutions that will assist in meeting the SSAM including: ● KnowBe4 ● SNYK ● Cloud Conformity
6	**Definition of a DSP and scope of the SSAM** Definition: Any software product or digital service that reads, stores, modified or routes any Taxation, Accounting, Payroll, Business Registry or Superannuation data. There are many definitions floating around and we're needing to unpack some specific examples of what a DSP is. ATO will do some work around this.
7	**Alternate security controls for future consideration** Simon Foster ran through the security standards / controls to be considered in the third review session. These included: ● OSF v6 ● Trans-Tasman Operational Framework for Peppol Access Points ● Schedule 2 of the Consumer Data Right rules ● Cyber.gov.au Essential Eight
8	**Next Steps and Action Items** ● Review SSAM requirements considering the following: ○ Which requirements could be uplifted / amended? ○ Do we need to be more descriptive? ○ Any further controls that could be added? ● Review the alternate security controls and how they may apply to your own organisations ● Talk to your teams and ecosystems about their experience with the SSAM ● Survey will be sent out to the group and broader DSPANZ community on the SSAM