dspanz. digital service providers australia new zealand

SSAM Review Session 3 - 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	**Summary of Session 2** Simon Foster provided a summary of the second review session. The group accepted that it was an accurate summary.
3	**Overlap of SSAM and DSP Operational Framework V6** Diana Porter ran through the OSF V6 requirements noting where there is overlap with the SSAM or changes were made to the framework. Simon Foster then covered the updated requirements that could be updated or added in the SSAM. *Encryption key management - should the SSAM deprecate OAuth 1?* The group agreed that the SSAM should also deprecate OAuth 1. *Encryption in transit - should the SSAM deprecate TLS 1.1?* The group agreed that the SSAM should deprecate TLS 1.1 and potentially have a transition period as it deprecates within the environment. *Entity validation - should the SSAM require entity validation?* The group agreed that full entity validation does not belong in the SSAM as it would be a lot of work for little uplift especially considering that DSPs are already required to undertake entity validation. Instead, it will be included in the SSAM as a recommendation or good practice for add-ons to collect email addresses and phone numbers of users.
4	**Overlap of SSAM and Trans Tasman E-invoicing** Simon provided an outline of the Operational Framework for Trans Tasman E-invoicing and pointed out how they are mapped back to ISO 27001 controls. When adding any further requirements, the group asked DSPANZ to think about what can be done by small DSPs/add-ons on a small budget. Particular focus was given to *information security awareness, education and training* as it can be low budget and deliver great results. There are low cost solutions and free resources readily available. The requirement for insurance was also discussed and it was agreed that there is minimal appetite from add-on participants to include insurance, however, if you would like to do business in Australia or with Australian citizens it is recommended. The group agreed to put these controls in as good practice but non-mandatory requirements and DSPANZ would provide sample policies that add-ons could use.
5	**Overlap of SSAM and CDR Schedule 2**

	From the survey feedback, there was interest in including some of the more technical controls but not so much the operational controls. It was noted that the CDR controls were quite similar to the e-invoicing controls covered above but there are a few with different names for essentially the same requirements. There was a discussion about customer data in non-production environments as this requirement does not exist in similar security standards. The group said that this was sensible but how would it be checked or verified by DSPs? Further how do you define customer data and is it still customer data if the data has been anonymised? This could be a requirement where an add-on provides an attestation and utilising a sample version created by DSPANZ. The ATO will look to have a conversation with Treasury about the CDR requirements, especially as the agreed upon stance for customer verification in the SSAM might not be enough for CDR.
6	**Further Discussion on Controls** Simon noted that there are still open conversations on breach reporting and notifications. Everyone agreed that DSPANZ needs to provide a definition for breach reporting. DSPANZ will also be looking into options for a centralised reporting mechanisms for add-ons.
7	**Accreditation and Certification** Ian Gibson had to leave the meeting early so we moved on to the next item.
8	**SSAM Auditors** Matthew asked the group whether there is any interest in DSPANZ determining what a SSAM audit may look like to make the process easier for add-ons and DSPs. There were a few questions as to whether DSPs would be able to accept third party audits. The group did think that if a third party prepared a spreadsheet or resource with answers to security questionnaires for add-ons that this would be useful and potentially cut down on the time it takes to complete multiple questionnaires.
9	**Summary of Review and Timeframes** In summary, the review has found that there is minimal desire for technical changes to the SSAM but there is interest in adding some optional operational requirements from the e-invoicing and CDR space and mapping these back to SOC 2 / ISO. DSPANZ will put together a draft version 1.1 of the SSAM and circulate to the group and the wider DSP and add-on community for feedback. The group may need to meet again before finalising the new version of the SSAM. In the meantime, DSPs should think about whether they are comfortable accepting attestations and add-ons on whether they are comfortable making attestations if they had the documentation to assist.