Certification and Assessment Focus Group outcomes

| Issue date: | 29 August 2017 |
| Venue: | Webex |
| Event date: | 28 August 2017 |
| Start: | 11:00am |
| Finish: | 4:45pm |
| Chair: | Stuart Coulson |
| Contact phone: | 02 4923 1060 |
| Attendees: | Sandeep Gopalan (Impact Software), Chris Denney (SuperChoice), Simon Foster (Shoeboxed), David Field (OzEDI), Michael Ross (MessageXchange), Koustubh Bandyopadhyay (CBA), Art Czernecki (Sage MicroPay), Mike Behling (MYOB), Andrew Smith (MYOB), Sergio Dutra (Xero), Matthew Addison (ICB) |
| ATO: | Stuart Coulson, Toby McMahon, Miranda Shaw, Terry Seiver, Kylie Johnston, Warwick Ragg |

Key Notes

- The ATO has an unprecedented number of APIs available but we are observing an increased volume of tax agent and business software data breaches. The ATO is strengthening the level of security applied across our digital channel ecosystem in order to reduce data breach occurrences and ensure we’re taking reasonable steps to safeguard taxpayer data from compromise and misuse.
- Certification (along with monitoring), are the central elements to reduce the risk associated with exposing ATO APIs / services. Confidence in who we share information with and how they handle it is at the core of enabling future digital services.
- iRAP certification is considered to provide the highest level of assurance, with ISO27001 being the minimum standard for ATO APIs rated category 3 and 4. The ATO recognises that 100% compliance with either certification is difficult however they can be implemented using a risk based approach. The certification will identify compliance
gaps, these risks are to be known and understood. Where required, these risks can be addressed with a clear path towards remediation.

- It was noted that mandating certification may have the potential to limit innovation and restrict start-up businesses from the market. It was suggested that we explore whether the certification approach, as per the ASIC SandBox model, is appropriate. This may potentially support levelling the playing field for smaller commercial groups.
- Clarification was sought regarding whether the ATO has mapped the risk categories of the API's / Services to the Certification threshold. This was clarified by Toby, who confirmed this has been considered and is represented within the supporting documentation.
- The high cost associated with certification was highlighted, scaling upwards due the scope involved and the scale of business operations. A question was asked if SOC 2 certification is relevant, and whether it would meet the minimum threshold.
- It was noted that work may be required to align to the overarching service (eg PLS) with the collection number of APIs that might be typically used for that service.
- The ATO confirmed that the API risk categorisation is based on both the nature of the information, the subsequent action performed by the ATO and risk surrounding downstream fraud.
- The ATO confirmed that it has incorporated learnings from the SuperStream Gateway certification process into the Operational Framework.
- Discussion then continued to flow around whether it may be suitable for the ATO to conduct a gap analysis (on a case by case basis) regarding the controls which may be met within the Standard. Clarification was provided that this level of review would not be sustainable.
- It was identified that a micro group may be used to unpack the roles and responsibilities of the DSPs, as dependant on where they operate within the supply chain. Given the overlap with the supply chain starting point suggest this be incorporated into that group.
- The minimum certification threshold should be consistently applied by the ATO and transparently available to all government and industry groups.
- A number of DSPs are required to be compliant with PCI-DSS and the requirement to maintain ISO or iRAP certification represents an additional impost /cost.
- Grandfathering arrangements for existing, in-channel, DSPs are yet to be formalised. Additional consultation would be required to progress this component.
- Stuart provided clarity that documents related to the Certification and Assessment focus group are generally Unclassified and unless there is sensitive information – the artefacts can be shared beyond the group.
Key Notes

<table>
<thead>
<tr>
<th>Action item</th>
<th>Due date</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8 Sep</td>
<td>Toby McMahon</td>
</tr>
<tr>
<td>2</td>
<td>5 Sep</td>
<td>Xero</td>
</tr>
<tr>
<td>3</td>
<td>8 Sep</td>
<td>Secretariat</td>
</tr>
<tr>
<td>4</td>
<td>8 Sep</td>
<td>Kylie</td>
</tr>
<tr>
<td>5</td>
<td>6 Sep</td>
<td>Focus Group</td>
</tr>
<tr>
<td>6</td>
<td>4 Sep</td>
<td>Focus Group</td>
</tr>
</tbody>
</table>

- **Action item: 1**
  - **Due date: 8 Sep**
  - **Responsibility: Toby McMahon**
  - Toby to explore the ASIC Sandbox model and provide a written response back to the focus group.

- **Action item: 2**
  - **Due date: 5 Sep**
  - **Responsibility: Xero**
  - Xero to provide details regarding SOC2 certification.
  - This can be emailed to DigitalBusinessCouncil@abr.gov.au

- **Action item: 3**
  - **Due date: 8 Sep**
  - **Responsibility: Secretariat**
  - The Secretariat will provide the focus group with the engagement plan.

- **Action item: 4**
  - **Due date: 8 Sep**
  - **Responsibility: Kylie**
  - Provide the focus group with further details on the API risk categorisation.

- **Action item: 5**
  - **Due date: 6 Sep**
  - **Responsibility: Focus Group**
  - Interested Focus Group members should nominate to participate in a micro group to explore which digital service providers in a supply chain require certification.

- **Action item: 6**
  - **Due date: 4 Sep**
  - **Responsibility: Focus Group**
  - The focus group will provide examples of supply chains (without names) – including the key functions (eg Data provider, Transformation provider, Messaging provider) of the entities in the chain. This should include some of the more nuanced supply chains.

  Note that this will be used by the Supply Chain micro group being formed under the Supply Chain and Encryption focus group.

If you have any feedback for the consultation process please email DigitalBusinessCouncil@abr.gov.au