Australian Government
Australian Taxation Office

UNCLASSIFIED External

Outcomes

Title:	Focus Group - Securing the broader ecosystem		
Issue date:	12 April 2019	**Venue:** WebEx	
Event date:	11 April 2019	**Start:** 11:00am	**Finish:** 12:00pm

Chair:	Terry Seiver	**Contact phone:**	02 4923 1060

Attendees:	Chris Howard – ABSIA / ADP Philip Vella - Amazon Simeon Duncan – for Intuit David Field - ozEDI Simon Foster – Squirrel Street Aaron O'Connor - Xero Matthew Prouse - Xero Jason Phua - ATO Terry Seiver - ATO Sonia Lark - ATO
Apologies:	Dino Alexandratos - Class Daniel Wyner - EmployGroup David Hawkins - ePayroll Geoff Clarke - Microsoft Mike Behling - MYOB Ann White - ozEDI Anthony Migliardi - Xero Cristina Blumberg - ACCC Jodi Ross - ACCC Paul Murray - AccountKit Michelle Lease - Intuit David Hawkins - Microsoft Lee Hickin - Microsoft Michael Wright - Sage Martin Mane - ATO

Next meeting	Week commencing **6 May 2019**

Key outcomes

The DSP Operational Framework was recognised as a potential starting point, however it was generally accepted that it would not be entirely suitable because of the different risk landscape.

The Intuit security requirements for listing on the app store, was recognised as a well advanced security standard for ecosystem developers. A gap analysis between the Intuit standard and the DSP Operational Framework may help shape further discussion on the minimum security standards.

There were a number of considerations raised on how a common security standard could be facilitated and maintained. DSPs proposed that the ATO could play a pivotal role to be the central point of contact for a common security standard.

DSPs collectively agreed that the minimum security standard should not include onshore data hosting requirements. DSPs also noted the importance of audit logging / security monitoring and appropriately responding to incidents and unusal patterns. Consistent breach notifications should also be in place.

Existing threat analysis by DSPs may help shape a risk assessment and the security standards.

Consumer privacy and the consent model were noted as future considerations, but will not be incorporated into the first iteration of the security standard.

It was propsed that the scope of the ecosystem security standards should include all software developers that consume 'internal and external api interfaces, which provide additional value add services to end customers and are sold commercially'. There was general agreement that a number of ecosystems may exist, however business and tax accounting will be the priority for this focus group.

While the implementation of the security standards may take some time (noting some ecosystems have set patterns for communicating with their ecosystem partners – eg every 6 months), there may be an opportunity to establish some requirements in the immediate future. It was suggested that a common approach to breach reporting could be discussed via email.

Actions

Action item:	**Due date:**	**Responsibility:**
20190411_1	**Friday 3 May 2019**	DPO
Perform gap analysis between Intuit standards and ATO operational framework		

Action item:	Due date:	Responsibility:
20190411_2	**Friday 3 May 2019**	DPO
Define an application ecosystem, to establish the scope of the security standards.		

Action item:	Due date:	Responsibility:
20190411_3	**Friday 3 May 2019**	DPO
Distribute a questionnaire for DSPs to describe their ecosystem, and what security requirements are already in place.		

Action item:	Due date:	Responsibility:
20190411_4	**Friday 26 April 2019**	DSP
Explore the breach reporting obligations for 3rd party software developers.		

Action item:	Due date:	Responsibility:
20190411_5	**Friday 3 May 2019**	DSPs
Provide the DPO with existing threat analysis of 3rd party software developers within an application ecosystem		