Australian Government
Australian Taxation Office

OFFICIAL External

Key Outcomes

Title:	Digital Service Provider, Operational Framework Review Fraud Detection & Monitoring Focus Group
Issue date:	6 May 2021
Venue:	WEBEX

Event date:	7 April 2021	**Start:** 10:00	**Finish:** 12:00

Chair:	Diana Porter	**Facilitator:**	Diana Porter
Contact:	Julie Huynh	**Contact phone:**	(02) 8894 9304

Intent:	Improve information security documentation relating to fraud detection and monitoring controls

Attendees:

ATO
Kylie Johnston – Digital Partnership Office (DPO)
Diana Porter – Operational Framework Lead (DPO)
Fiona Homan – Information & Cyber Security
Mark MacDowell – Digital Communication & Identity Services
Anu Duggirala – Digital Wholesale Integration
Andrew Davis – DCIS Product Management
James Bills – DCIS Product Management
Ian Lloyd – Relationship Manager Digital Partnership Office
Stephen Knight – DCIS Product Management
Operational Framework Team

Industry

ABSIA	Simon Foster
Ascender Pay	Craig Booth
Intuit	Matt Lewis
MYOB Australia	Andrew Smith
Ozedi Holdings	Josef Bobinac
Sage Software Australia	Estevan Chaves
Superchoice	James Cameron
SuperConcepts	Grant Christensen
Thomson Reuters	Clyde Netto

	Xero	Erin Adams
	Xero	Helen MacGillivray
	Xero	Matthew Prouse

Apologies: ATO

Melissa Goodwin - DCIS
Claire Miller – Director, Digital Communication & Identity Services
Nick Kelly – IT Security Analyst DCIS Architecture

Industry

AMP	Andrew Strong
BT Financial	Kim Sung Do
ELMO Software	Artur Czernecki
e-Payday	Brett Reed
IRESS	John Paul Lonie
Reckon	Simon Hutchinson

Next meeting: TBA

The key outcomes for this meeting are best read with the Fraud Detection & Monitoring Focus Group presentation.

Agenda item: 1 – Introduction & Overview

Three key themes were discussed including an overview of feedback from the first session on:

1. Expanding Security Monitoring
2. Preservation and Retention of Log Data
3. Breach Notification Guidance

It was noted some items raised during the review that will be taken out of session and finalised post review.

Agenda item: 2 – Expanding Security Monitoring

The group discussed previous feedback on expanding security monitoring:

- Commercial impacts for small DSPs
- ATO to establish baseline controls.

Discussion on expanding scope of security monitoring to all DSP controlled cloud environments, including exploring benefits, risks and considerations.

Outcomes from industry discussion:

- The control will be uplifted for security monitoring to be included to all DSP controlled cloud environment's (there will be no differentiation to the API risk rating or volumes).
- Streamline guidance on evidence required, to better represent the types of evidence provided by DSPs
- Evidence required will include a screenshot of the security monitoring system detecting the intrusion i.e. dashboard of detection system that generates alerts. This is because it shows

evidence of the intrusion. This screenshot should also include the name/s of the relevant assets.

Further consideration is needed for:

- Define the specific requirements to show all i.e. does the requirement relate to the whole application or just to the part of the software that interacts with the ATO.
- The group noted ATO could investigate the use AWS Guard Duty, this will be taken out of the DSP OPF Review.

Agenda item: 3 – Protection and preservation of audit logs

The group discussed previous feedback on Improved Guidance of Retention and Preservation of Audit Logs:

1. Specific guidance on expectations of log preservations.
2. Mapping industry standards.
3. ATO to establish baseline controls.

Outcomes from industry discussion:

- DSPs generally agreed:
  - User access controls to be tightened to ensure individual user can be identified through audit logs.
  - Shared log-ins are not to be permitted.
- Guidance will include link to support DSPs in creating their log management plan e.g. Australian Cyber Security Centre guidelines for system monitoring.
- DPO will provide additional information including examples and scenarios in a newly created Operational Framework support page in the knowledge hub.

Further consideration is needed for:

- Requirements will provide further guidance for:
  - What should be logged e.g. Are logs required when sensitive information is viewed or only when changes are made.
  - Storage of logs i.e. how stored, evidence, timeframes etc
  - When a user logs in multiple times through different browsers

Agenda item: 4 – Breach Notification Guidance

The group discussed previous feedback on the opportunities to improve the breach notification process and guidance:

1. Timeframe to report breaches.
2. Guidance on risk thresholds for reporting breaches.
3. Clarification on what action the ATO takes when a breach notification is received.

Outcomes from industry discussion:

- DSPs generally agreed breach notifications needed clarification on:

  - Specific details required as part of reporting a breach
  - Using the word ‘immediately’ with context
  - The DSPs responsibility for reporting breaches from Add-on marketplaces.

Further consideration is needed for:

- Ability of incident notification to be created directly by a third party / add-on marketplace. DPO will explore improvements in OS4DSPs.

Agenda item: 5 – Wrap Up & Close

Outcomes of working group to be published and circulated.