Australian Government
Australian Taxation Office

Digital Service Provider (DSP) Operational Framework Review

Operational Framework Review Focus Group – Fraud Detection and Monitoring

Presented by Diana Porter & Jarrod Wellings

13 November 2020

What are we trying to achieve?

There are 3 opportunities to investigate and improve information security documentation relating to fraud detection and monitoring controls

1 Expanding Security Monitoring

Explore benefits in expanding scope of security monitoring control to all DSP controlled cloud environments.

2 Preservation and retention of log data

Investigate and improve guidance on:

a) protection and preservation of audit logs
b) retention periods that align to legislative requirements
c) accessing information to share in the case of a security incident

3 Breach notification guidance

Improve process and guidance to assist DSPs:

- Respond to breaches.
- Notify and report a security breach.
- With incident response and fraud investigations.
- With supporting information for clients

1 Expanding security monitoring

How is the security monitoring control applied and what is required

This control seeks to detect and respond to cyber-attacks, channel misuse and business threats. It is applied to web based hybrid solutions and all DSP controlled solutions excluding low risk and low volume solutions

Evidence requirements

- **Network / infrastructure layer**:
    - screen shots of an intrusion detection system or firewall that generates alerts. If a DSP uses a third party a screenshot from within the solution showing the monitoring capabilities, dashboard etc.
    - photos of your Security information and event management dashboard
    - leveraging off a cloud provider you can provide either an invoice or screenshot from within the environment showing the type of monitoring captured.
- **Application layer**:
    - screen shots of the function page in the application, and
    - reports from the backend system.
- **Transaction (data) layer**:
    - reports from the backend system
    - screenshots of an anomaly detection system.

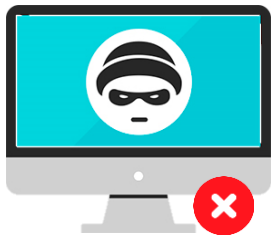
Has this control been effective?

What are the current risks and potential benefits through expanding this control?

The following table explores current risks and benefits in expanding this control to DSP controlled cloud solutions that consumes low risk APIs and are interacting with less than 10,000 unique tax or super records

Current state risks

Increase in time to identify breach

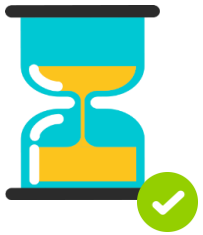


Increased data breached

Reputational damage

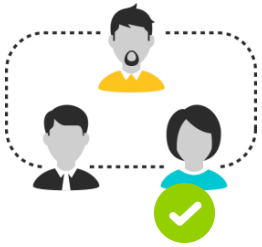
Cost to manage security event are significantly higher

Benefits of expanding the control



Reduction in time taken to identify and contain breach

Hardening of systems to prevent future incidents



Enhanced trust and confidence

Reduced costs to supply chain

Consideration to improve documentation and future proof against emerging threats

Consider risk based application of controls

Improving existing evidence requirements

Responding to emerging threats

To note:

Australian Cyber Security Strategy

Increased risk of malware and ransomware with introduction of 5G and number of Internet of Things devices to increase from 21 billion to 64 billion devices between now and 2025.

Office of Australian Information Commissioner

From January to June 2020 150% increase in Ransomware attacks from prior period (July to December 2019).

Final thoughts and feedback

2 Protection and preservation of audit logs

What is the current documentation relating to audit logging

This control seeks to ensure traceability of access and actions within software to assist in the case of a security incident

Application of the control

All DSPs will need to consider their environment and what logging should be implemented and ensure that the logging records include the following where applicable:

- Date and time of the event
- Relevant user or process
- Event description
- Success or failure of the event
- Event source e.g. application name
- ICT equipment location and identification
- Data identifiers (product ID, Tax File Number (TFN))

Evidence requirements

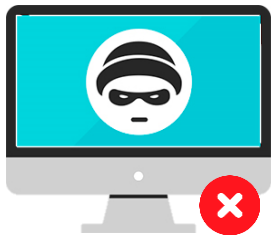
- Sample dummy access and event log
- Data dictionary that describes the data attributes and maps against key audit log components.

Has this control been effective?

Why do we need to improve guidance on protection and preservation of audit logs

a Explore risks and benefits in relation to guidance on protection and preservation of audit logs

Risks



Unauthorised access and tampering

Loss of integrity of data

Log data not retained for cyber incident

Staff and clients not trained to access logs

Benefits

Authorisation and authentication controls

Maintain integrity of log data in transit and at rest

Data is retained and available to assist in cyber investigation

Hardening of systems and processes

What industry standards support DSPs make risk based decisions around audit logging

(a) Investigate if industry standards provide sufficient coverage to assist DSPs make risk based decisions around protection, preservation and retention of log data

Industry standards already implemented as part of the Operational Framework

Audit logging controls relate to:

- Event logging
- Log protection
- Administrator and operator logs
- Clock Synchronisation

Audit logging controls relate to:

- Log content
- Log processing
- Log protection
- Error handling

Audit logging controls relate to:

- Event logging
- Log details
- Log protection
- Log retention

Logical and physical access controls

Other industry frameworks or standards

What legislation supports retention periods audit logging

b Identify and investigate legislative requirements that support retention periods

Superannuation Industry (Supervision) Act 1993

Provides record keeping obligations which applies to gateways in the Superannuation Transaction Network.

Archives Act 1983

Provides record-keeping obligations that apply to Commonwealth records.

Tax administration Act 1953

Provides record keeping requirements that apply to individuals and entities

Privacy Act 1988

Protecting the handling, collection, use, storage and disclosure of personal information about individuals.

Digital Service Providers

May have contracts with clients in regards to retention of data.

In general not covered under legislative requirements

To note:

Australian Cyber Security Centre

The 2019-20 annual report reported 59,806 breaches reported at a rate of one breach every 10 minutes.

Office of Australian Information Commissioner

January to June 2020 report identified that:

- 77% of entities identified breach within 30 days
- 19% of entities identified breach within 31 to 365 days
- 4% of entities took longer than a year

IBM 2020 cost of a data breach report

The average time in Australia to identify and contain a breach is 296 days, up from 283 days in the prior period.

Final thoughts and feedback

3 Breach Notification Guidance

What is the current process and documentation relating to breach notification

DSPs must notify the ATO immediately when a breach is identified by any means as outlined in the operational framework terms and conditions

What's the process?

Raise a ticket through online services for DSPs, notify account manager or DPO@ato.gov.au.

What is required?

Information to provide includes:

- appropriate contact person (specialist IT security/fraud representative)
- nature of the incident
- number of affected records
- date and timestamp
- session ID reference
- host Services (Internet Service Provider)/IP address
- device ID (ESID) if available
- TFN information
- non-TFN information (name/address/biographical information)
- product name and type (desktop or cloud)
- what format the data was in (e.g. CSV or encrypted)

Has this process been effective?

What are some of the opportunities to improve the process and guidance

Seek feedback on the breach notification process and opportunities to improve the process and guidance to support DSPs and mutual clients

Clarity on what is a breach, when and how to notify

Timeframe to report a data breach

Risk thresholds for notifying the ATO

Other obligations and legislative requirements

Supporting guidance for clients

Streamlining of processes

Final thoughts and feedback

Open Discussion

Do DSPs agree with the opportunities to improve?

- **Expanding security monitoring**
- **Protection and preservation of log data**
- **Breach notification guidance**

Are there any other improvements DSPs would like to see made?

Next steps