Securing the DSP Ecosystem

ABSIA

Securing the DSP Ecosystem

- DSP Operational Framework: One Year Later
- Securing the Broader Ecosystem and Developing the SSAM
- SSAM for Greater Security Across Ecosystems
- Industry Panel: How to Keep the Ecosystem Strong and Secure
- What's Next for the Operational Framework

1.

DSP Operational Framework: One Year Later

John Dardo, CDO and Deputy Commissioner, ATO

Securing the Broader Ecosystem and Developing the SSAM

Matthew Prouse, Director and Treasurer, ABSIA

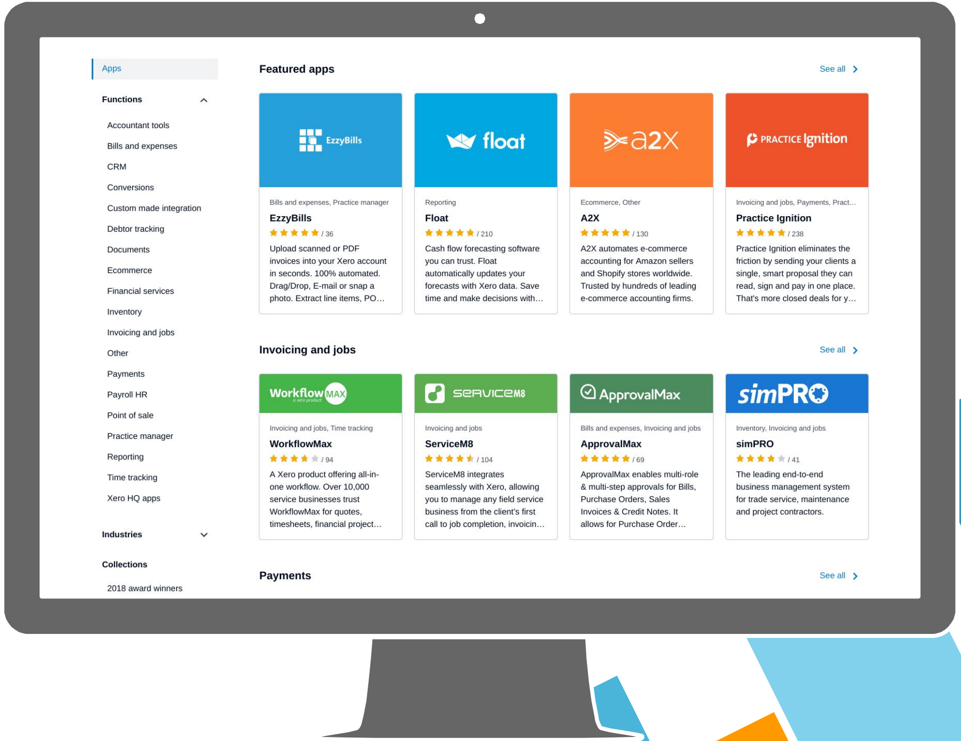
» Multiple DSPs with APIs and marketplaces.

» Over 1000 add-ons in DSP marketplaces.

» Mix of local and global companies.

» Thousands of developers working across the ecosystem.

» Inconsistent approach to security.



Featured apps See all ›

Bills and expenses, Practice manager
EzzyBills
★★★★★ / 36
Upload scanned or PDF invoices into your Xero account in seconds. 100% automated. Drag/Drop, E-mail or snap a photo. Extract line items, PO…

Reporting
Float
★★★★★ / 210
Cash flow forecasting software you can trust. Float automatically updates your forecasts with Xero data. Save time and make decisions with…

Ecommerce, Other
A2X
★★★★★ / 130
A2X automates e-commerce accounting for Amazon sellers and Shopify stores worldwide. Trusted by hundreds of leading e-commerce accounting firms.

Invoicing and jobs, Payments, Pract…
Practice Ignition
★★★★★ / 238
Practice Ignition eliminates the friction by sending your clients a single, smart proposal they can read, sign and pay in one place. That's more closed deals for y…

Invoicing and jobs See all ›

Invoicing and jobs, Time tracking
WorkflowMax
★★★★☆ / 94
A Xero product offering all-in-one workflow. Over 10,000 service businesses trust WorkflowMax for quotes, timesheets, financial project…

Invoicing and jobs
ServiceM8
★★★★★ / 104
ServiceM8 integrates seamlessly with Xero, allowing you to manage any field service business from the client's first call to job completion, invoicin…

Bills and expenses, Invoicing and jobs
ApprovalMax
★★★★★ / 69
ApprovalMax enables multi-role & multi-step approvals for Bills, Purchase Orders, Sales Invoices & Credit Notes. It allows for Purchase Order…

Inventory, Invoicing and jobs
simPRO
★★★★☆ / 41
The leading end-to-end business management system for trade service, maintenance and project contractors.

Payments See all ›

SECURING THE ECOSYSTEM

💼 Digital Service Providers

Software products that provide:

- Accounting, tax services (eg Activity Statements, Income Tax Returns).
- Payroll (eg STP reporting).
- Superannuation (eg Fund Validation, SuperTICK).

- **Direct or indirect API integration to ATO.**
- Desktop or cloud.
- Typically contains personal, financial and TFN data stored within software.
- **ATO regulated and certified.**

🧩 Add-ons

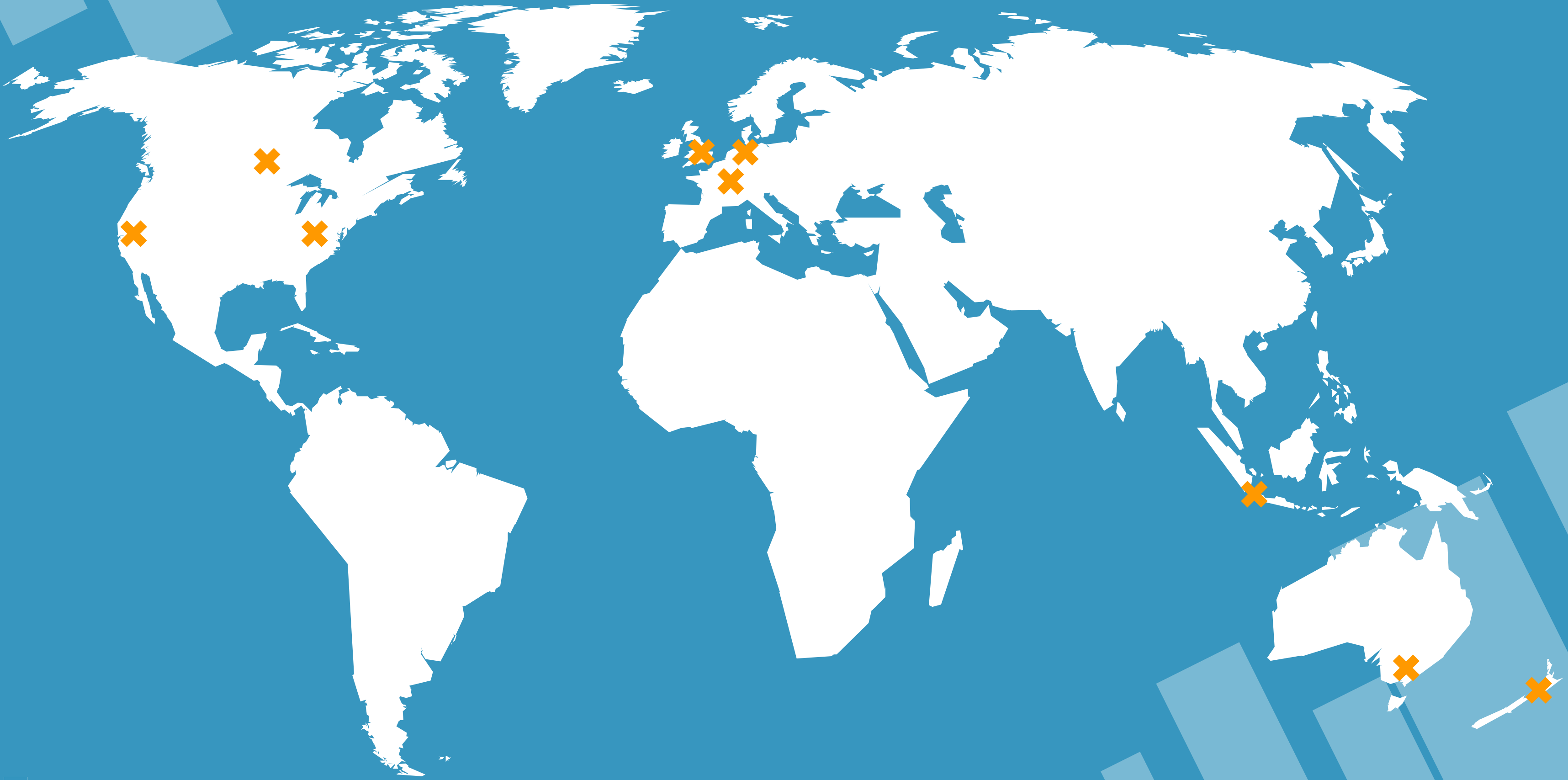
- Any other business purpose.
- Does not provide accounting/tax, payroll or superannuation services.
- No API connection to ATO - either direct or via a Sending Service Provider / Superannuation Gateway
- Cloud only.
- Consumes an API endpoint provided by DSPs.
- Typically may contain personal and financial information but does not normally store TFN within software.
- **Not directly regulated by the ATO.**

ABSIA

STARTING POINT

- Arose as an action item from the ATO Strategic Working Group in late 2018.
- Industry asked the DPO to facilitate a focus working group to work towards consistent guidelines and standards.
- Aim was to develop a broadly accepted and portable security framework to maximise security and minimise duplication for DSPs and Add-ons.
- Scope was limited to tax, payroll, accounting and superannuation.

GAP ASSESSMENT



Security Standard for Add-on Marketplaces (SSAM)

RESPONSIBILITIES AND OBLIGATIONS

Add-on Developers

- Implement best practice.
- Self assess software against the security requirements of the SSAM.
- Provide details to DSPs via self assessment or certification once a year.

DSPs with Marketplaces

- Certify add-ons once a year or ask for add-ons to self assess and provide evidence.
- Inform DPO of widely used addons as part of Operational Framework review.

REQUIREMENTS & SPECIFICS

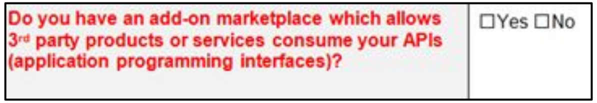
💼 For DSPs with Add-on Marketplaces

SELF ASSESSMENT AS THE NORM

- DSPs expected to have a certification standard for third party add-ons (ie. SSAM).
- Add-ons should self assess against the standard.
- DSPs to review compliance to standard annually for each certified add-on.
- Self assessment could standardize.

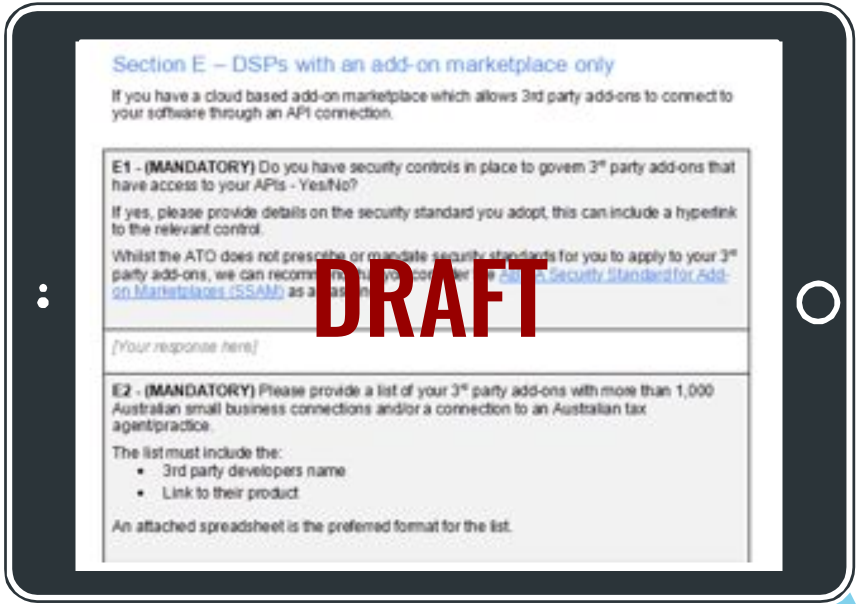
DSP QUESTIONNAIRE

» Additions to the DSP questionnaire



Do you have an add-on marketplace which allows 3^{rd} party products or services consume your APIs (application programming interfaces)?	☐Yes ☐No

» Only DSPs with an add-on marketplace will be required to report API connections to DPO.



Section E – DSPs with an add-on marketplace only

If you have a cloud based add-on marketplace which allows 3rd party add-ons to connect to your software through an API connection.

E1 - (MANDATORY) Do you have security controls in place to govern 3^{rd} party add-ons that have access to your APIs - Yes/No? If yes, please provide details on the security standard you adopt, this can include a hyperlink to the relevant control. Whilst the ATO does not prescribe or mandate security standards for you to apply to your 3^{rd} party add-ons, we can recommend that you consider the ABSIA Security Standard for Add-on Marketplaces (SSAM) as a bas[illegible]
[Your response here]
E2 - (MANDATORY) Please provide a list of your 3^{rd} party add-ons with more than 1,000 Australian small business connections and/or a connection to an Australian tax agent/practice. The list must include the: • 3rd party developers name • Link to their product An attached spreadsheet is the preferred format for the list.

DRAFT

WHO NEEDS TO BE REPORTED

DSP Add-ons

» Third party software that integrates with a DSP via API with more than 1000 connections.

Practice Add-ons

» Third party software that integrates via API with the practice client list (inc individual taxpayers) of a registered BAS or tax agent.

DISCLOSURE RESPONSIBILITIES

DSPs will provide the ATO with:

- a list of third party add-ons with more than 1000 API connections to their platform; and
- a list of add-ons with API integrations to a tax agent/practice client list.

Into the future, DSPs with Add-on Marketplaces will also need to report:

- the date self-assessment was last completed by each add-on;
- confirmation that the DSP has approved the self-assessment;
- details of any outstanding matters.

BREACH REPORTING

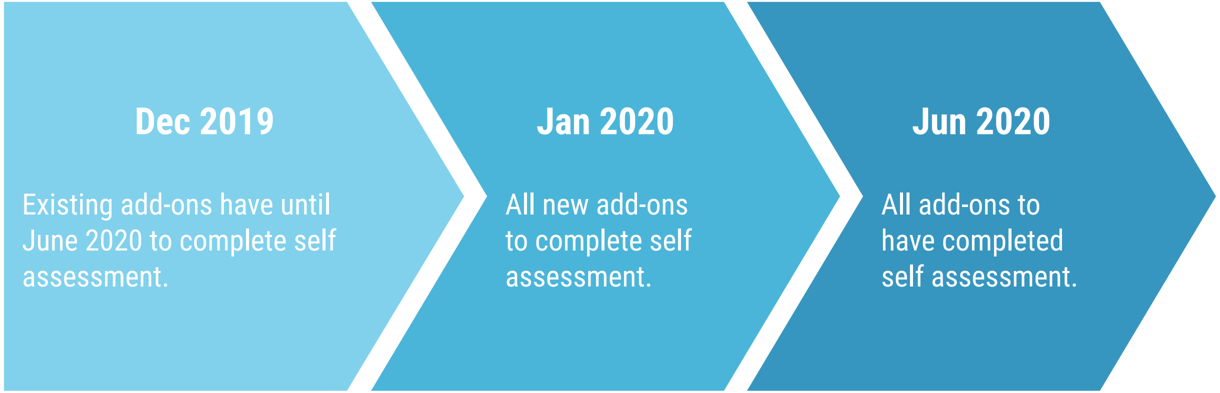
- DSPs must report any data or identity security breach of their own environment to the DPO.

- DSPs with an add-on marketplace must also report any data or security breach of a third party add-on.

IMPLEMENTATION

- » Add-on marketplace included as part of standard Operational Framework annual review process.
- » Updated Security Questionnaire will be published shortly.
- » DSPs will begin to recertify against Operational Framework before December 2019.

TIMELINE



Dec 2019

Existing add-ons have until June 2020 to complete self assessment.

Jan 2020

All new add-ons to complete self assessment.

Jun 2020

All add-ons to have completed self assessment.

KEEPING THINGS CONSISTENT

Preconfigured SAAS Hosting

» Amazon
» Microsoft

Working Globally

» New Zealand
» Singapore
» UK
» Canada

NEXT STEPS

3.

SSAM for Greater Security Across Ecosystems

Simon Foster, Founder and CEO, Squirrel Street
Director and Vice President, ABSIA

ABSIA

REQUIREMENTS & SPECIFICS

🧩 For Add-on Developers

ENCRYPTION KEY MANAGEMENT

- » Implemented policy for managing encryption keys & tokens
- » OAuth tokens or customer-identifying information must not be exposed within your app or shared with other parties.
- » Token management once a user completes the OAuth authorization workflow:
    - ◊ OAuth 1.0a
    - ◊ OAuth 2.0

ENCRYPTION IN TRANSIT

- » MANDATORY - App server is configured using https to support only TLS version 1.1 or higher.
- » RECOMMENDED - TLS version 1.2 using AES 256 or higher with SHA-256.

Translation:

- » Mandatory https
- » Use TLS 1.2 or better for your app server.
- » Use SSL Labs to verify best practice

AUTHENTICATION

- Ensure that strong customer authentication is enabled (minimum two step authentication).
- Single Sign On with DSP credentials is encouraged.

Translation:

- Require strong passwords.
- Implement two step authentication or SSO for login and sign up.

INDIRECT ACCESS TO DATA

- Third party access to customer data must be clearly stated within applicable policies and/or terms and conditions, and have a justifiable business need.

Translation:

- Add-ons must have a privacy policy and terms and conditions.
- Be transparent with users.
- Maintain consent.
- Be mindful and respect customer data.

APP SERVER CONFIGURATION

- » Ensure add-on server’s configuration follows industry accepted hardening practice for example:
  - ◊ National Institute of Standards and Technology – Guide to General Server Security
  - ◊ Relevant vendor recommendations

Translation:

- » Use Amazon AWS or Azure most of the time.

VULNERABILITY MANAGEMENT

» Follow an industry accepted standard for secure code development such as OWASP Top 10 to protect against vulnerabilities such as:

◊ Cross Site Request Forgery
◊ Cross Site Scripting (including reflected and stored cross site scripting)
◊ SQL and XML Injection
◊ Authentication, Sessions Management and Functional level access control
◊ Forward or Redirectors in use have been validated
◊ All app session cookies have following attributes set: Secure and HTTPOnly

ENCRYPTION AT REST

- Encryption at rest using NIST Cryptographic Mechanisms is mandatory for data repositories that hold or manage sensitive commercial or personal information.
- Examples may include; full-disk, container, application or database level encryption techniques.

Translation:

- Use Amazon AWS or Azure most of the time.
- Recommend database field level encryption

AUDIT LOGGING

- Audit logging should include both application level (access logs) and event based actions.
- 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
- Audit logs must be retained for as long as appropriate to enable future investigation (at least 12 months).
- Logs must be immutable and secure.

DATA HOSTING

» Consideration needs to be given to country, legal, contractual, access, sovereignty and counter-party risks.

Translation:

» In most cases, add-ons should not store data in Afghanistan, Iran, Syria, Russia, Mainland China or North Korea.

MONITORING AND BREACH REPORTING

- Demonstrate that you scan your environment for threats and that you take appropriate action where you detect anomalies.
- Monitoring can be at the network / infrastructure, application or transaction (data) layer.
- Where anomalies are detected, add-ons must report these to the DSP, providing enough information to enable further monitoring and/or preventative action.

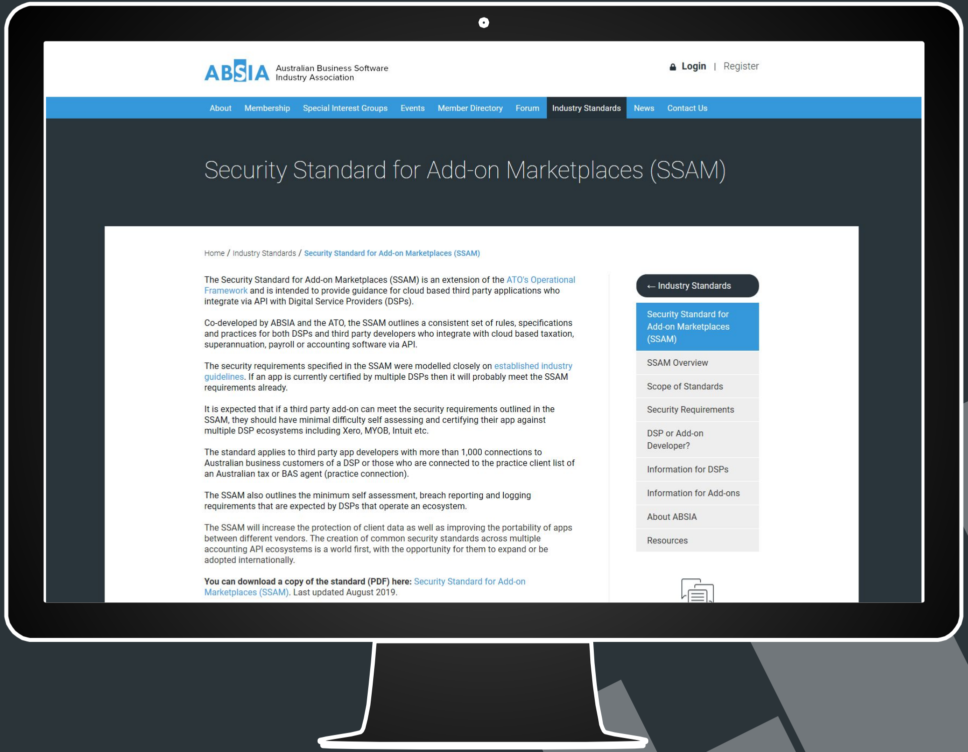
Translation:

- Talk to the DSP

Add-ons

MORE DETAILS

Read the documentation provided on the ABSIA website under Industry Standards.



Security Standard for Add-on Marketplaces (SSAM)

Home / Industry Standards / Security Standard for Add-on Marketplaces (SSAM)

The Security Standard for Add-on Marketplaces (SSAM) is an extension of the ATO's Operational Framework and is intended to provide guidance for cloud based third party applications who integrate via API with Digital Service Providers (DSPs).

Co-developed by ABSIA and the ATO, the SSAM outlines a consistent set of rules, specifications and practices for both DSPs and third party developers who integrate with cloud based taxation, superannuation, payroll or accounting software via API.

The security requirements specified in the SSAM were modelled closely on established industry guidelines. If an app is currently certified by multiple DSPs then it will probably meet the SSAM requirements already.

It is expected that if a third party add-on can meet the security requirements outlined in the SSAM, they should have minimal difficulty self assessing and certifying their app against multiple DSP ecosystems including Xero, MYOB, Intuit etc.

The standard applies to third party app developers with more than 1,000 connections to Australian business customers of a DSP or those who are connected to the practice client list of an Australian tax or BAS agent (practice connection).

The SSAM also outlines the minimum self assessment, breach reporting and logging requirements that are expected by DSPs that operate an ecosystem.

The SSAM will increase the protection of client data as well as improving the portability of apps between different vendors. The creation of common security standards across multiple accounting API ecosystems is a world first, with the opportunity for them to expand or be adopted internationally.

You can download a copy of the standard (PDF) here: Security Standard for Add-on Marketplaces (SSAM). Last updated August 2019.

ABSIA

4.

Industry Panel: How to Keep the Ecosystem Strong and Secure

Panel Participants

Matthew Prouse, Director and Treasurer, ABSIA

Simon Foster, Founder and CEO, Squirrel Street & Director and Vice President, ABSIA

John Dardo, CDO and Deputy Commissioner, ATO

David Martin, Technical Compliance and Audit Manager, Small Business and Self Employed Group, Intuit

Michael Wright, Product Manager - Handisoft, Sage Software Australia

Heather Smith, ANISE Consulting

ABSIA

Questions?

5.

What's Next for the Operational Framework?

Terry Seiver, Assistant Director and DSP Operational Framework Evolution Lead, ATO Digital Partnership Office

ABSIA