dspanz. digital service providers australia new zealand

Security Standard for Add-on Marketplaces

Summary of 2021 Review

Formerly ABSIA

Contents

Contents 1

Executive Summary 3

Part 1 - Context and Background 6

THE ECOSYSTEM 6
CONCEPTION 6
SECURING THE BROADER ECOSYSTEM WORKING GROUP 7
DESIGN 7
PURPOSE 7
RELEASE 7
SELF CERTIFICATION 8
HIGH LEVEL SUMMARY OF SSAM REQUIREMENTS 8

Part 2 - Current experiences of DSPs and Add-ons 9

OVERVIEW OF A CHANGING LANDSCAPE 9
ATO OPERATIONAL SECURITY FRAMEWORK VERSION 6 9
MARKETPLACE TERMINOLOGY 9
THE 2021 SSAM REVIEW 9
DSP EXPERIENCE 10
Communicating security requirements to third party developers 10
Reviewing security questionnaires 10
Change management processes with API consumers and end customers 11
DEVELOPER EXPERIENCE 11
Meeting the security requirements 12
Completing the security questionnaires 13
Additional security requirements 13
Change management processes 13
OVERALL SURVEY RESULTS 13
Changing industry perceptions 13
Manual processing 14
THE CHANGED RELATIONSHIP BETWEEN DSPs AND DEVELOPERS 14
Responsibility for security education 14
Working with accounting firms 14
Competitive pressures 14
ADDITIONAL DOCUMENTATION ABOUT SSAM WOULD BE WORTHWHILE 15
ONGOING SECURITY MONITORING 15
BREACH REPORTING TO ATO 15
PROPOSED TECHNICAL UPLIFT 15
PROPOSED UPDATE TO SSAM FOR 2022 15
TRANSITION PERIODS FOR DSPs AND ADD-ONS 16

Part 3 - Future directions to secure the broader ecosystem 17

OPERATIONAL VS SECURITY CONTROLS 17

CONSUMER DATA RIGHT SCHEDULE 2 17
INDEPENDENT CERTIFICATION AND AUDIT 19
INTERNATIONAL OPPORTUNITIES 19
SECURITY BREACH REPORTING 19
ENHANCED DOCUMENTATION 19
WHEN IS THE NEXT REVIEW? 19

Appendix **21**

GLOSSARY OF TERMS 21
CONTACT INFORMATION 21

Executive Summary

Following the review of the Australian Taxation Office's (ATO) Operational Security Framework (OSF), DSPANZ began the first review of the Security Standard for Add-on Marketplaces (SSAM) to reflect the changes of the OSF and other changes in the ecosystem.

The review process consisted of three working group sessions with industry and government representatives and was accompanied by two surveys to better understand the experiences of both DSPs and add-ons when implementing and complying with the API security standards included in the SSAM.

App Developer Experience

- Majority do not have staff dedicated to security, monitoring and compliance work.
- Security questionnaires took days to complete for the majority of developers
- Implementation typically took months not weeks to complete

83% of app developers believed that the security requirement improved security outcomes for their customers.

> **"Most of the work fell back on me with such a small team."**

> **"I think we have a responsibility to our clients to go through this process. We just have to work out how to make it achievable for the smaller add-ons who can't afford to hire people in the role."**

Digital Service Provider (DSP) Experience

- Many DSPs have manual self-assessment process
- Ongoing costs of the SSAM highest for DSPs
- DSPs felt that the SSAM improved security outcomes for their customers
- Terminology e.g. "add-on marketplace" and "third party app store developer" led to people/companies believing that the standard did not apply to them

20% of DSPs put automated processes in place for self assessments.

> **"We are now responsible for the security education of app partners."**

> **"Significant change to the relationship between DSP and add-ons."**

> **"The fact that third parties have an industry standard to work towards rather than several different standards for each DSP is particularly valulable."**

What the review process found is that both DSPs and add-ons wanted to see minimal changes to the SSAM requirements but add-ons were interested in having optional operational controls included in the standard. As a result, two requirements were uplifted (deprecating OAuth 1.0 and TLS 1.1) and two new requirements were added (entity validation and web application firewalls). It is also proposed that six operational requirements, that reflect existing ISO 27001 controls, will be added for add-on developers to self assess against. DSPANZ will work with security assessment providers and DSPs to create template self attestation documents for these controls to help reduce the work required for add-ons.

Revised SSAM

Requirement	End State
App server configuration	No change to technical requirements. Wording will be revised.
Authentication	No change to technical requirements. Wording will be revised.
Audit logging	No change to technical requirements. Wording will be revised.
Data hosting	No change to technical requirements. Wording will be revised.
Encryption at rest	No change to technical requirements. Wording will be revised.
Encryption key management	Legacy OAuth 1.0 based authentication processes must be phased out for all API consumers by 31 December 2022.
Encryption in transit	Encryption in transit must use TLS 1.2 or TLS 1.3.
Entity validation	If connected via API, applications can inherit or rely upon the entity validation already performed by the DSP. It is strongly recommended that applications collect and validate an email address and contact telephone number as part of their buy flow or registration process for non-trial customers.
Indirect access to data	Information added on why this requirement is important - to ensure that unauthorised third parties are unable to access customer data.
Security monitoring	Information has been updated with detail on the expected security monitoring practices and that these capabilities should be documented and/or demonstrated to a DSP as part of their annual certification and self assessment process.
Vulnerability management	Information added to requirement - developers must secure their applications against common vulnerabilities.
Web application firewalls	Applications must use a web application firewall.
Optional operational controls	Self attestation against the following existing ISO 27001 controls: • Information security awareness, education and training • Operational procedures and responsibility • Personnel security • Physical and environmental security • System access control • System acquisition, development and maintenance.

The review also identified a number of items where DSPANZ can help to resolve challenges or simply provide more guidance and supporting materials. Alongside the new version of the SSAM, DSPANZ will look to:

- Provide additional documentation for both DSPs and add-ons;
- Include more information around security monitoring and logging;
- Investigate options to make the breach reporting process easier; and
- Align the wording of the SSAM requirements with ISO 27001 controls.

While this review of the SSAM has resulted in minimal changes, there are a number of external factors that will impact both DSPs and add-ons, and therefore the SSAM requirements, over the next few years. Such factors include:

- Updated version of ISO 27001 expected to be released in early 2022
- Changes to CDR Rules to encompass additional sectors
- Further growth in the number of DSPs and add-ons operating across Australia and New Zealand

Considering the above, DSPANZ would expect to review the SSAM requirements again in 2023.

Over the following pages this report covers the introduction and purpose of the SSAM, the changing threat environment, the results of the survey from both the DSP and add-on perspective, key observations from the review process, the proposed changes to the SSAM requirements and future directions to secure the broader ecosystem.

Some quick numbers

20 DSPs with public APIs / operate marketplaces

2,000 apps listed in DSP marketplaces

20,000 developers operating in the DSP ecosystem

Top 50 most used apps are consistent across multiple marketplaces

Part 1 - Context and Background

Key objectives of the SSAM

- **Develop a set of consistent and practical security requirements for add-ons and API consumers that takes reasonable steps to secure tax, accounting, superannuation and payroll data;**
- **Enable add-on developers and API consumers to rely upon a single set of security requirements to integrate with multiple DSPs; and**
- **Reduce the cost of implementing best practice solutions through scalability and common sense.**

THE ECOSYSTEM

According to the ATO's Digital Partnership Office (DPO), as of September 2021, there are more than 20 DSPs with public APIs or who operate add-on marketplaces. Among the largest and most well known are the Xero App Store, MYOB App Marketplace, Intuit QuickBooks Apps, Sage Apps, Class Partners & Integrations and the Reckon Add-on Marketplace. Between them, more than 2,000 third party apps or add-ons are certified and listed in these marketplaces.

The apps listed in these marketplaces provide a range of features and capabilities to users of cloud based accounting, payroll and tax software. It is widely stated that more than 20,000 developers operate in the DSP ecosystem. It is also recognised that the Top 50 apps in most marketplaces integrate with more than one DSP or cloud accounting ledger.

Example add-on feature sets include: agriculture, bills and expenses, bookings and reservations, CRM, debtor tracking, document management, e-commerce, financial services, inventory, invoicing, job management, payroll and HR, point of sale, practice management, property management, reporting, rostering, time tracking and workflow management functionality.

These applications are often industry specific and can integrate with multiple tax, accounting or payroll systems.

CONCEPTION

The initial version of the SSAM arose in late 2018 from discussions within the ATO's DSP Strategic Working Group (SWG), following the initial introduction of the DSP Operational Security Framework (OSF). The imposition of the ATO's OSF materially changed the security environment imposed upon software developers with direct API access to ATO systems. The uplifted requirements introduced significant protections for taxpayer data contained within DSP systems and greatly reduced the risk of identity theft, privacy breaches and other cybercrimes against Australian businesses and taxpayers.

The industry and SWG also recognised that the uplifted security requirements, created by the introduction of the OSF, would make alternate attack vectors more attractive and potentially put software applications and users (such as accounting practices) with indirect access to taxation, payroll and superannuation data at an increased risk for attempted cyberattacks.

SECURING THE BROADER ECOSYSTEM WORKING GROUP

The creation of an industry working group was an action item from the SWG aimed at "securing the broader ecosystem". With the support of the DPO, DSPANZ was asked to identify or develop a companion cybersecurity standard for API consumers within the DSP ecosystem.

In 2019, the working group of DSPs and other interested software developers met monthly for almost six months and co-developed the *Security Standard for Add-on Marketplaces (SSAM)* following a lengthy consultation process. Prior to settling on the self-assessment model contained within the SSAM, the working group had considered introducing the DSP Operational Framework or ISO 27001 for the entire DSP ecosystem.

Ultimately, it was determinated that the significant overheads imposed by these frameworks would exceed the risk and likelihood of significant cyber breaches. There was also limited appetite from DSPs operating API marketplaces to enforce operational security requirements on their third party app developers and API consumers given the risk profile of the data contained within their public API.

DESIGN

The SSAM is considered to be a practical, scalable and sensible approach to uplifting the security environment of independent, third party API developers. It took a risk based approach and focused on API consumers who are highly leveraged (have API access to more than 1,000 business datasets) or consume highly sensitive taxpayer client lists and personally identifiable data.

PURPOSE

The intended purpose of the SSAM was to help secure the broader API ecosystem around Australian DSPs by:

- Developing a set of consistent and practical security requirements for add-ons and API consumers that took reasonable steps to secure tax, accounting, superannuation and payroll data;
- Enabling add-on developers and API consumers to rely upon a single set of security requirements to integrate with multiple DSPs; and
- Reducing the cost of implementing best practice solutions through scalability.

RELEASE

The initial release was based upon the security standards employed by Intuit for its QuickBooks Online app store and had a clear focus on specific technical solutions that represent best practice for cloud-based business software development.

Security breach reporting obligations and ATO specific risk ratings were incorporated and the implementation period and transitional timelines were developed based on consultation with DSPs. DSPs initially had 18 months to roll out the SSAM to their third party app ecosystem.

Reporting and disclosure requirements for DSPs were subsequently added to the ATO Operational Security Framework in 2019. DSPs were obliged to document the participants in their API ecosystem and provide a list of the integrated third parties with either more than 1,000 API connections and/or access to practice level APIs.

SELF CERTIFICATION

Ongoing compliance with the SSAM relies upon self assessment and self certification by app developers as part of their annual recertification process with a DSP. Third party developers are required to complete a security questionnaire and demonstrate that they meet the operational and security requirements specified in the SSAM. The mechanism for the annual certification process varies between DSPs but ultimately, it is a self assessed security questionnaire that is reviewed by the marketplace provider.

HIGH LEVEL SUMMARY OF SSAM REQUIREMENTS

Consideration	Guidance/specification
Timeline	These requirements apply from: • 1 July 2020 for those connections in place as at 31 December 2019. • 1 January 2020 for all other considerations.
Responsibility	**3rd party app store developers:** • with more than 1,000 connections to Australian small business customers of a DSP, or is • connected to the practice client list of an Australian tax or BAS agent (practice connection) • should provide a completed self-assessment on an annual basis to that DSP **The DSP should, as part of their annual certification with the ATO under the Operational Framework, provide:** • a list of the applicable 3rd party app store developers with more than 1,000 small business connections or a connection to tax agent/practice client list (including inviduals); • the date the self-assessment has been completed; • confirmation that the self-assessment has been approved by the DSP and details of any outstanding matters or remediation plans.
Non-compliance	**Where a 3rd party app developer does not adequately comply with these specifications:** • DSP will issue a written notice giving 30 days to advise the treatment plan and up to a further 60 days to complete the required work.

Requirement	End State
Encryption key management	Ensure effective key management is implemented to protect client data.
Encryption in transit	Ensure that sensitive client data in your app is protected during the transport process.
Authentication	Ensure that users who have access to your app are authenticated.
Indirect access to data	Ensure that unauthorised third-parties are unable to access customer data.
App server configuration	Ensure that your app server is secure.
Vulnerability management	Ensure that your app is secure against the common vulnerabilities.
Encryption at rest	Ensure that sensitive client data in your app is protected while at rest.
Audit logging	Ensure that appropriate audit logging functionality is implemented and maintained.
Data hosting	Ensure client data is not hosted in high risk areas.
Security monitoring practices and breach reporting	Ensure you have security monitoring practices in place to detect and manage threats.

Part 2 - Current experiences of DSPs and Add-ons

OVERVIEW OF A CHANGING LANDSCAPE

Since the initial implementation of the SSAM, we have seen a number of changes in the industry to improve security (e.g. uplifts to security standards) but there have also been changes to the threat environment. There has been a major increase in the number of developers and therefore in apps consuming DSP APIs. DSPs themselves have also been busy creating new APIs of which new use cases are continuously emerging.

A number of industry trends have transformed the DSP marketplace and introduced new challenges and new opportunities. These include:

- Work from home and bring your own device policies becoming increasingly standard practice for most employers - large and small.
- The cloud has gone mainstream and is considered to be the default platform for business software.
- The use of public cloud infrastructure, as provided by Amazon AWS or Microsoft Azure, has become commonplace
- A number of industry security standards have been refreshed and updated to address the current technology environment.
- Cyberattacks have become more sophisticated - and more commonplace. Customers are more aware of cybersecurity than previously.
- Additional regulatory frameworks have been introduced to manage data privacy, data consent and data governance.
- Cyber Insurance has become more available for small business.

ATO OPERATIONAL SECURITY FRAMEWORK VERSION 6

In 2020, the ATO engaged PwC to independently review the OSF. Across 2020 and 2021, the ATO then conducted more than 12 months of consultations with DSPs, DSPANZ and other industry stakeholders to validate the PwC recommendations. The ATO has since published the sixth version of the OSF which came into effect from August 2021.

MARKETPLACE TERMINOLOGY

An interesting development in the last few years has been the change, or mix, in terminology used to describe add-ons. The ecosystem no longer refers to them as just add-ons as a business may use an app to primarily run their business with the DSP's software in the back end or the app may consume a private API. DSPs now tend to use the following terms interchangeably: apps, add-on apps, API consumers, add-on developers and third party app developers.

THE 2021 SSAM REVIEW

Following the publication of version 6 of the OSF, DSPANZ commenced a review of the SSAM in August 2021. As a part of this review, three working group sessions were held across August and September 2021 with industry and government representatives.

During the review, DSPANZ also ran two surveys and conducted interviews with developers to better understand the experiences of both DSPs and add-ons when implementing and complying with the API security standards included in the SSAM.

The survey responses can be considered as representative. Responses were received from many of the most used apps and add-ons listed in multiple DSP marketplaces. These software developers have hundreds of thousands of users and customers in Australia and New Zealand. The survey also received written responses from DSPs with the largest marketplaces who represent the vast majority of cloud accounting customers and third party API consumers in Australia and New Zealand.

DSP EXPERIENCE

A quick summary

- Processing up to **500 security assessments** each year
- Only **30% had dedicated staff** for this work
- Majority of DSPs **process self-assessments manually**
- Spending between **$100,000 and $1 million annually** on compliance efforts
- Introducing mandatory **two-factor authentication (2SA) was challenging**

Overall, the DSPs considered the introduction of consistent ecosystem security requirements to be a positive development that has helped to secure the broader API community. Survey responses from DSPs focused on communicating security requirements to third party developers, reviewing security questionnaires and change management processes with API consumers and end customers.

Communicating security requirements to third party developers
The introduction of the SSAM in 2019 meant that DSPs were responsible for developing their implementation and creating or revising their security questionnaire process. They were also required to communicate these requirements to their API consumers and co-ordinate the annual review and self assessment process.

According to the survey, for some DSPs this was an entirely new set of interactions with their API consumers. One of the biggest challenges for many DSPs was becoming responsible for the security education of their API consumers. Some DSPs were required to explain why the requirements were coming into effect and manage the knowledge and skill gaps whilst guiding their API consumers through the implementation process.

The documentation published by DSPANZ was helpful for most survey respondents. However, the SSAM review has identified multiple areas for clarification and improvement, which are discussed later in the report.

Reviewing security questionnaires
When implementing the SSAM, most DSPs developed a new security questionnaire or updated their annual recertification process for API consumers and add-on developers. The security questionnaires were sent to add-on developers and DSPs reviewed the responses.

The survey results showed that the annual review and certification process is very manual for most DSPs. Some DSPs are processing up to 500 security assessments each year and the security questionnaires represent a considerable percentage of the workload for dedicated DSP staff. Noting that only 30% of DSPs had dedicated staff for this work, the remainder relied upon a mix of relationship management, security and technical staff to process these questionnaires. This workload continues to increase as more apps enter the API ecosystem and meet the reporting thresholds for the SSAM e.g. have more than 1,000 customers or begin to consume higher risk practice APIs.

Automated tools can sometimes assist with collecting information or assessing some aspects of the security configurations of a third party app. However, the majority of the assessments are reliant upon a DSP staff member manually reviewing the responses provided by developers.

The implementation costs of annual security assessments are significant for DSPs. DSPs are typically spending between $100,000 and more than $1 million annnually on compliance efforts. However, one survey respondent processes more than 500 self assessments each year which significantly increases their costs. The bulk of these costs have been spent on building internal systems, reviewing the responses to security questionnaires and ongoing relationship management and education for add-on developers.

It is likely that ongoing compliance will continue to rise for many DSPs as more developers enter the market and integrate with DSP controlled APIs. Based on the survey, it is certain that lowering the 1,000 API connection threshold to the limits required by Schedule 2 of the Consumer Data Right (CDR) (effectively 100% of API consumers) will immediately introduce unsustainable compliance costs to DSPs and developers.

Change management processes with API consumers and end customers
Like the OSF, the SSAM introduced external security requirements for software developers that imposed changes to user experiences for customers and end users. For most users, the most notable of these changes was the introduction of mandatory two-step authentication (2SA).

Both DSPs and app developers commented in the survey that mandatory 2SA was a cause of frustration and change management for new and existing customers. It changed the user experience for all users and may have altered the workflow within third party software which affected its performance or efficiency. Moreover, implementing requirements like 2SA for add-ons is often accompanied by the need for additional support, education and marketing resources to support customers through the change.

Large DSPs had to make decisions about whether they applied their security questionnaire globally. Those DSPs that implemented the SSAM globally have faced push back from add-on developers who do not have customers in Australia or are not party to Australian regulations.

The timelines contained within the transition period in the SSAM meant many DSPs had to impose hard deadlines and some app developers were frsutrated that their product roadmaps had to be compromised to comply with the imposed security requirements. Not all add-ons had the same resources available to them to complete the work in time and COVID-19 further impacted the ability of some add-ons to meet the recommended deadlines.

All things considered, it is also worth noting that DSPs and developers commented that they already had security work in their roadmaps. One respondent commented that their partners were planning to meet many of the requirements but that the introduction of SSAM made them bring this work forward.

DEVELOPER EXPERIENCE

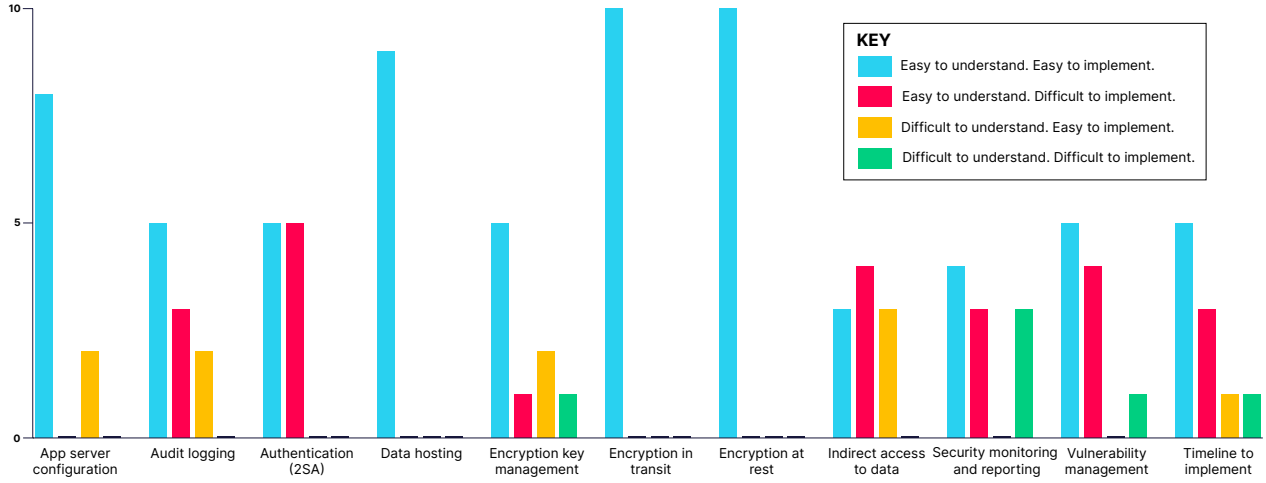
- **50%** of add-ons integrated with **four or more** different DSPs
- Completing an average of **five security assessments each year**
- **30%** had independent ISO 27001 or SOC2 certifications
- **Less than one third** used single sign-on provided by a DSP
- **More than 70%** built their own 2SA solution
- Surveys took **hours to days** to complete
- **46%** took between **3-6 months** to implement the security requirements

Overall, API consumers and add-on developers found the introduction of consistent ecosystem security requirements a positive, more so than their DSP counterparts. Survey responses from developers focused on the technical security requirements, the overlap with existing security certifications, providing the required documentation and change management with customers.

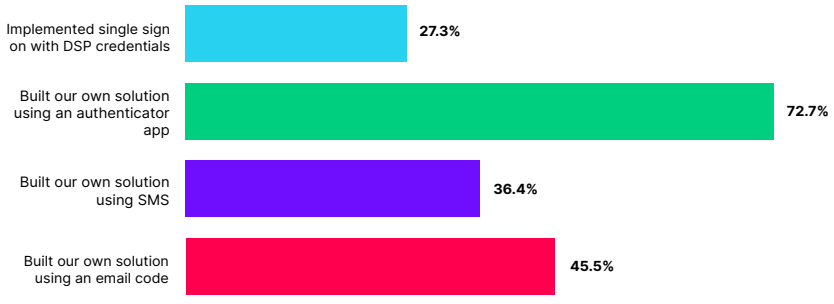
It was noted in most survey responses that many app developers have small teams and limited internal development and security resources. This impacted their ability to meet security requirements and make changes to their software in a timely manner.

The majority of survey respondents integrated with multiple DSPs. More than 50% of survey responses were from add-on developers who integrated with four or more different DSPs and were asked to complete more than five security assessments each year. Also, among the larger and more established app developers (with many thousands of customers), more than 30% had an independent ISO 27001 or SOC2 certification.

Meeting the security requirements
According to the survey responses, app developers found that industry standard, cloud infrastructure providers such as Amazon AWS and Microsoft Azure could be preconfigured to meet the SSAM requirements. Most app developers found it relatively easy to meet the server configuration, audit logging, data hosting, encryption key management and encryption at rest/in transit requirements by relying upon features within their infrastructure solutions.



The roll out of two step authentication for all end users was a more complex undertaking. Many DSPs allow, or require, third party applications to use single sign-on credentials provided by the DSP (e.g. sign in with MYOB) and pass through a multi-factor token as part of this process. However, less than a third of survey respondents had chosen to implement this. More than seventy percent of respondents had elected to build their own 2SA solution. 72% of these implementations relied upon an authenticator app such as Google Authenticator, 45% used an email address as a second factor and 36% had implemented SMS based authentication instead.



Some DSPs also introduced additional requirements for add-ons and applications that wish to consume or access practice or client list APIs. For example, several DSPs require add-ons to be independently ISO 27001 certified or complete the DSP OSF before being granted access to practice level APIs. Additional terms of use or contract conditions may also apply to access these APIs.

Whilst this is aligned to good industry practice, it was not the initial intention of the SSAM. App developers have commented that these additional requirements can create confusion or they can present as restrictions and impositions on customers that are not always clearly communicated to developers by DSPs.

Completing the security questionnaires
The majority of survey respondents integrated with multiple DSPs. Add-ons were completing, on average, five security assessments each year with the typical survey respondent taking between hours to days to complete each questionnaire. The questionnaires are mostly completed by the business owners or development teams. Some of the larger add-ons relied upon their in-house security teams.

There is significant variation between security questionnaires. Many developers commented on the need to routinely transponse information from their security documentation into different questionnaires for different DSPs. Differences in terminology and wording are commonplace between DSPs. This led to significant duplication of effort by app developers. Almost all major DSPs have security requirements in-line with the SSAM but these differences in wording, questionnaire layout and design led to developers needing to reword answers or seek clarifications from DSPs with respect to security controls or questionnaires.

Additional security requirements
A number of larger app developers who responded to the survey were independently certified against ISO 27001 and/or SOC2. Some expressed frustration at being asked to complete a DSP specific security questionnaire whilst holding a globally recognised independent certification. Similarly, with the majority of app developers integrating with multiple DSPs, it is hoped that they can reduce the amount of repeat work and the industry can move to either a free-standing security assessment independent of DSPs or multiple DSPs will begin to accept each other's security assessments. The majority of add-ons (55%) would like to see DSPs accept security assessments from other DSPs and integration partners.

Change management processes
The majority of app developers surveyed (46%) said it took them between 3-6 months to implement the security requirements within their software. However, larger DSPs with bigger marketplaces commented that add-ons took anywhere from weeks to 12 months to comply with all of the SSAM requirements. DSPs noted that some add-ons had a much better security posture and were able to implement changes rather quickly while some had far more work to do resulting in some requesting extensions.

OVERALL SURVEY RESULTS

Survey participants acknowledged that the introduction of the SSAM had improved the overall security environment for DSPs, their app developers and their end users. There was a broad consensus that it was beneficial for the industry to embrace a consistent set of security requirements and controls for DSPs and their API consumers.

Changing industry perceptions
The survey also revealed that perceptions of the SSAM had changed over time. The initial reaction to new security requirements was neutral or less than favourable for more than 50% of DSPs. However, after they had been rolled out and implemented by DSPs they were viewed

favourably or very favourably by more than 88% of DSP respondents. On the other hand, the number of add-on developers who viewed the additional security requirements favourably or very favourably (more than 82%) remained almost the same pre and post implementation.

Manual processing
The biggest insight from the survey is how manual the security questionnaire process is for both DSPs and add-ons. While both said they utilise tools, staff were still required to gather and enter the majority of the data (in the case of add-ons) and review the information once questionnaires are completed (in the case of DSPs).

Overall, both DSPs and add-ons believed that the security requirements had result in improved security outcomes with an overwhelming 91% of add-ons believing this to be the case for their customers. One DSP said, “at the end of the day it is protecting us, our clients and the individual.”

Key observations

THE CHANGED RELATIONSHIP BETWEEN DSPs AND DEVELOPERS

Responsibility for security education
An unintended outcome of implementing security assessments for third parties has been the change in relationship between DSPs and add-on developers. As DSPs are the ones enforcing these requirements on their add-on developers, they have found themselves responsible for the security education of these developers. This development has introduced unintended consequences for both DSPs and app developers.

In most cases, DSPs have built free and public APIs to connect to their app store or marketplace. They provide documentation, testing environments and software development kits (SDKs) for third party developers to create software that use these APIs. They have published terms of use or technical requirements for third parties and in many cases, marketing guidelines that third parties must follow in order to be listed in their app store and promoted to their customers.

Many DSPs have tiered marketing and support programs that incentivise developers or provide differing levels of support and relationship management based on tiers in a developer partner program. With the rollout of the security requirements, DSPs were asked to treat all of their ecosystem partners consistently and provide extensive support to all of them.

Working with accounting firms
These challenges were particularly pronounced for DSPs with open APIs and deep connections with the accounting and bookkeeping industry. The lower tolerance for risk with respect to practice client lists and registered agent data sets meant that in-house, bespoke or home brew developers within accounting practices who were building software for their own users, were required to meet all of the SSAM requirements from the outset regardless of the number of connections. In many cases, these developers were not sophisticated, had limited development experience and saw their software as little more than an Excel macro designed to rearrange their own data.

Competitive pressures
Most DSP app marketplaces contain vertical specific or niche software meaning there is often increased competition between the apps. Many apps wanted to see an even playing field when it came to meeting the SSAM in time with DSPs revoking API access for those that were unable to meet the deadline. One DSP commented that while they had expected this level of competition, they did not expect apps to ask for compensation when they met the

requirements in time when others were given extensions.

ADDITIONAL DOCUMENTATION ABOUT SSAM WOULD BE WORTHWHILE

Multiple respondents commented that additional documentation, definitions and example security questionnaires from DSPANZ would be extremely helpful moving forward. Respondents provided the following examples:

- Explainer on the difference between 2SA and MFA
- List of useful tools
- Webinars on enhancing security
- Example security questionnaire and expected documentation

More information about the proposed enhanced documentation can be found in part three of the report.

ONGOING SECURITY MONITORING

Throughout the review, some add-ons noted that they have a limited ability and resources to undertake security monitoring at a high level. How logs should be stored and what they should contain was also not clear in the SSAM documentation. It was noted that by not having this information in a useful and searchable format, it meant that it could be difficult to track potential issues.

This was a difficult requirement for some add-ons and it required significant and ongoing changes to their software. In the enhanced documentation, we will look to include more information around security monitoring and audit logging.

BREACH REPORTING TO ATO

Throughout the review process, it was brought to our attention that it is not clear how add-ons are expected to report breaches. It was qustioned whether an add-on is required to report to each DSP they connect to or if they should be reporting to one DSP and expecting that this information is shared with other DSPs.

As many add-ons do not have a direct relationship with the Digital Partnership Office (DPO), it did not make sense for them to report to the ATO even though they could be interested in this information.

DSPANZ will be investigating options to make this process easier for add-ons.

PROPOSED TECHNICAL UPLIFT

Based on the updated requirements to version 6 of the OSF, the review group decided on the following changes under encryption key management and encryption in transit respectively:

- Deprecate OAuth 1.0 - now OAuth 2.0
- Deprecate TLS 1.1 - now TLS 1.2 or higher

The applicability of entity validation, a new control added to the OSF, was discussed and it was agreed that full entity validation does not belong in the SSAM. Instead, DSPANZ will look to include a recommendation on collecting email addresses and phone numbers from users.

PROPOSED UPDATE TO SSAM FOR 2022

The proposed updates to the SSAM can be found below. Two new requirements have been

added to the standard: entity validation and web application firewalls.

To better align the SSAM with ISO 27001:2013, DSPANZ will look to reflect the wording used in ISO controls where appropriate. Improvements will also be made to each of the requirements to ensure they are clear and provide detailed guidance material where it is needed.

Once the changes are confirmed by the DSPANZ Security Sub-Committee, additional materials and information will be made available through the DSPANZ website.

DSPANZ will look to create template self attestation documents for each of these requirements to reduce the work required for add-on developers. DSPANZ intends to publish a template, pro-forma SSAM security questionnaire before June 2022. It is hoped that this document can be used by DSPs to streamline and standardise the annual review process.

Requirement	Proposed Changes to Requirement
Encryption key management	Legacy OAuth 1.0 based authentication processes must be phased out for all API consumers by 31 December 2022.
Encryption in transit	Encryption in transit must use TLS 1.2 or TLS 1.3.
Entity validation (NEW)	If connected via API, applications can inherit or rely upon the entity validation already performed by the DSP. It is strongly recommended that applications collect and validate an email address and contact telephone number as part of their buy flow or registration process for non-trial customers.
Indirect access to data	Information added on why this requirement is important - to ensure that unauthorised third parties are unable to access customer data.
Security monitoring	Information has been updated with detail on the expected security monitoring practices and that these capabilities should be documented and/or demonstrated to a DSP as part of their annual certification and self assessment process.
Vulnerability management	Information added to requirement - developers must secure their applications against common vulnerabilities.
Web application firewalls (NEW)	Applications must use a web application firewall.

TRANSITION PERIODS FOR DSPs AND ADD-ONS

The expected deadline for add-ons to comply with the updated version of the SSAM is:
- 31 December 2023 for existing connections/APIs
- 31 December 2022 for new connections/APIs

DSPs should look to implement the uplifted SSAM requirements within their annual security questionnaire processes within the next 6-12 months.

Existing API consumers and app developers should be granted six months to make the necessary security upgrades and complete their self assessment. Additional time can be granted by the DSPs on a case by case basis.

DSPANZ will look to create template self attestation documents for each of these requirements to reduce the work required for add-on developers. DSPANZ intends to publish a template, pro-forma SSAM security questionnaire before June 2022. It is hoped that this document can be used by DSPs to streamline and standardise the annual review process.

Part 3 - Future directions to secure the broader ecosystem

OPERATIONAL VS SECURITY CONTROLS

Add-on developers were keen to see optional operational controls added to the SSAM to help their businesses meet other security requirements. Given that it may be difficult for a DSP to remotely determine how some operational controls have been implemented by a third party developer, it was agreed that self attestations were the most appropriate way to demonstrate this as part of an annual security questionnaire process.

We are proposing to add the following operational controls, which reflect ISO 27001:2013, to the SSAM:

- Information security awareness, education and training
- Operational procedures and responsibility
- Personnel security
- Physical and environmental security
- System access control
- System acquisition, development and maintenance

An updated version of ISO 27001 is expected to be released in early 2022 (with corresponding updates to ISO 27002/27017 implementation guides). It is proposed that it is at the discretion of the DSPs to include updated versions of these security controls in their annual security self assessment questionnaire.

DSPANZ will look to create template self attestation documents for each of these requirements to reduce the work required for add-on developers. DSPANZ intends to publish a template, pro-forma SSAM security questionnaire before June 2022. It is hope that this document can be used by DSPs to streamline and standardise the annual review process.

CONSUMER DATA RIGHT SCHEDULE 2

As part of the SSAM Review surveys, DSPs and app developers were asked if any additional security controls should be considered to be within the scope of the uplifted SSAM requirements. Among the options presented was the CDR Schedule 2 security controls proposed by Treasury/ACCC as part of the Open Data regime.

The controls under Schedule 2 of the CDR were analysed for their applicability under the SSAM. While some of the controls are currently reflected in the SSAM and in proposed updates, there are a number of controls that were considered too onerous for developers and DSPs to reasonably include in the SSAM.

It was also noted that unlike the completely unregulated personal finance software industry, business software and the DSP ecosystem has a working regulatory and security framework already in place. Moreover, both the ATO and the DSPs have taken a risk based approach and adopted security requirements that scale with business size and complexity, allow for innovation and bespoke and custom development, and strike a balance between eliminating cyber risks and encouraging participation and adoption.

The results of the survey are presented in the table below.

Schedule 2 Control	Type	Supportive	Not supportive
Restricting administrative privileges	Technical	**90%**	10%
Access security	Technical	**80%**	20%
Security patching	Technical	**80%**	20%
Prohibit customer data in non-production	Operational	**70%**	30%
Data loss prevention	Operational	**70%**	30%
Limiting physical access	Operational	**70%**	30%
Password authentication	Technical	**70%**	30%
Roles and permissions within software	Technical	**70%**	30%
Security training and awareness	Operational	**70%**	30%
Anti-malware anti-virus	Technical	**60%**	40%
Data segregation	Technical	**60%**	40%
Firewalls	Technical	**60%**	40%
End user device policies	Operational	50%	50%
Unique IDs	Technical	50%	50%
Human resource security	Operational	44%	**56%**
Acceptable use of technology	Operational	40%	**60%**
Information asset lifecycle management	Operational	40%	**60%**
Application whitelisting	Technical	30%	**70%**
Customer verification processes	Operational	30%	**70%**
3rd-party management framework	Operational	30%	**70%**
Minimum insurance and indemnity	Operational	30%	**70%**
Web and email content filtering	Technical	30%	**70%**

It was noted that Schedule 2 does not currently take a risk based approach and requires all API consumers to meet all of the requirements irrespective of the number of API connections. This imposes significant costs on DSPs and their ecosystem and prevents many individuals and smaller developers from participating in the CDR regime and make it unsustainable in the medium term.

Under the current requirements, both DSPs and third parties receiving CDR (including CDR derived) data will need to seek an accreditation pathway, which in some instances will include the sponsor-affiliate model. The current definition of CDR derived data may mean that DSPs, who operate app stores and allow third party software to connect and share data, will have to sponsor between 20,000 and 30,000 API developers and consumers (including private and bespoke integrations). Moreover, third party developers who integrate with multiple DSPs will need to be sponsored multiple times. This mechanism will be extremely costly and inefficient.

There are a number of challenges for DSPs looking to become accredited under the CDR with the rules as they currently stand. DSPANZ, together with the ATO, will look to have further conversations with Treasury and ACCC about how these rules will affect DSPs and ultimately their add-on ecosystems.

INDEPENDENT CERTIFICATION AND AUDIT

Whilst the introduction of the SSAM has reduced the amount of work required for an app developer to self-assess against multiple DSPs, the SSAM has not achieved its ultimate goal of allowing developers to self-assess against one DSP's security requirements and have this accepted by other DSPs.

We recognise that this may not be possible due to the differences in API architecture, legal requirements and additional requirements from DSPs. Instead, we intend to explore independent certification and audit options in 2022 to make the assessment process easier for both add-on developers and DSPs.

INTERNATIONAL OPPORTUNITIES

There are potential applications of the SSAM outside of Australia and the ATO ecosystem. These opportunities include New Zealand, Singapore and the UK and also within Peppol as they look to adopt security standards.

SECURITY BREACH REPORTING

There is an opportunity to make the breach reporting process as easy as possible for add-ons and DSPs. DSPANZ will investigate options for a centralised reporting mechanism for add-ons. Further, it was agreed that a definition for breach reporting is needed under the SSAM.

ENHANCED DOCUMENTATION

The updated version of the SSAM will look to include revised and expanded documentation for both DSPs and add-ons to make the process easier and to leverage template materials.

Such documentation and materials include:

- Model security questionnaire from DSPANZ
- List of equivalent controls in other standards
- Graphics, factsheets and information to utilise for add-ons and end users
- Attestations for operational requirements

In the enhanced documentation we will also look to reflect the changing terminology for add-ons. We will predominantly look to use "add-ons or API consumers" in the documentation to accurately capture who should meet the SSAM requirements. However, while we may use one term, we understand that DSPs will continue to use the term that resonates with their marketplaces and app stores.

WHEN IS THE NEXT REVIEW?

It is anticipated that the SSAM will be reviewed in full in 2023 to better reflect future good practice and address the challenges of the future cybersecurity environment.

An updated version of ISO 27001 is expected to be released in early 2022 (with corresponding updates to ISO 27002/27017 implementation guides). This may impact how DSPs are independently certified using ISO 27001 under the ATO's DSP OSF. Once the implementation of ISO27001:2022 is made clearer, DSPANZ will consider its impacts on the SSAM requirements in 2022/23.

It is also expected that the CDR Rules will be updated in 2022 to encompass additional sectors and address many of the concerns raised by participants. It is hoped that these changes will

better align CDR Schedule 2 requirements with the established industry standards created by the ATO OSF and the SSAM.

It is also anticipated that there will be hundreds more DSPs operating in Australia and New Zealand with the creation of the new ATO Digital Services Gateway and the next phase of the New Zealand Inland Revenue Department's business transformation program.

Appendix

GLOSSARY OF TERMS

Acronym / Term	Translation
ACCC	Australian Competition and Consumer Commission
ACSC	Australian Cyber Security Centre
ATO	Australian Taxation Office
AWS	Amazon Web Services
CDR	Consumer Data Right
DARG	ATO Digital service provider Architecture Reference Group
DPO	Digital Partnership Office
DSP	Digital Service Provider or software developer interacting with ATO or other Australian or New Zealand government APIs.
GNGB	Gateway Network Governance Body - organisation managing the integrity of the Superannuation Transaction Network (STN)
IRD	New Zealand Inland Revenue Department
KMS	Key Management Service
OAIC	Office of the Australian Information Commissioner
Peppol	Set of artifacts and specifications enabling cross-border eProcurement. Currently used by Australia and New Zealand for eInvoicing.
SDK	Software Development Kit
SSL	Secure Sockets Layer
SWG	ATO Digital Service Providers Strategic Working Group
TLS	Transport Layer Security - evolved from previous Secure Sockets Layer (SSL) protocol.

CONTACT INFORMATION

Website: www.dspanz.org

Email: hello@dspanz.org

Report authors: Maggie Leese, Matthew Prouse and Simon Foster.