Co-Presenter - Matthew Prouse (ABSIA): Hi everyone thanks for dialling in. We'll be kickin off this webinar in a few minutes time. Just waiting for a few more to join in.

Good to see your smiley, friendly faces.

Just as a reminder we will be recording this session. It will be made available on the ABSIA website shortly. Similarly, if anyone needs a copy of this slide pack as a PDF, we will be sharing the slides on the SSAM website as well as part of our ABSIA comms.

Okay Maggie, I think I might get started.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): Good afternoon or good morning for our guests from Western Australia or from Asia. Welcome to the ABSIA Security Standard for Add-on Marketplaces webinar for May 2020.

My name is Matthew Prouse, I'm a Director here at ABSIA. I'm also the Head of Industry at Xero.

Joining us in today's session is Maggie Leese, our Marketing Officer based in Adelaide. Maggie is responsible for a lot of the content that ABSIA's producing - our newsletters, a lot of the discussions that are occurring on the forums relating to the ATO and the things that are going on in the industry and of course, putting together such as this.

Also joining me is ABSIA's Vice President, Simon Foster. Simon in his multiple day jobs is the General Manager APAC at Storecove, which is an e-invoicing access point provider. He's also the Founder of Squirrel Street, which was one of the original add-ons for Xero, MYOB, Reckon, Sage and Quickbooks Online. So he's the right person to start talking about how the different security standards have evolved and changed and how they apply to add-ons in the new climate.

Simon and I are also industry representatives on the ATO Strategic Working Group, which is currently meeting weekly due to COVID-19.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): Before we get started, we would like to acknowledge the traditional owners of the lands where we're all sitting and where we're all meeting and pay our respects to their elders past, present and emerging.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): Today's webinar is an update on the Security Standard for Add-on Marketplaces. It's been with us since August last year, when we published the V1 or version 1 documentation and it's been part of the ATO's DSP Operational Framework annual questionnaire and review from September last year. So we're going to give a bit of a context around the state of the security standard and where it fits. Simon's then going to talk through the specifics and what they mean now that we have multiple vendors implementing it, multiple add-ons being required to comply with it. What it's meaning in practice and then we'll talk about how it's progressing. Some of the future state stuff that we're seeing inside the security standard and of course you have the opportunity to ask questions.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): Most of the attendees are regulars, but we do have some slightly different terminology for some of us.

When we talk about a DSP, that's an ATO term for Digital Service Provider. It's a software company that builds software that integrates into some of the Government infrastructure via API.

I'm going to use the word DPO a lot. That's the arm of the Tax Office that works closely with software developers. The Digital Partnership Office.

API we should know. The SSAM is the Security Standard for Add-on Marketplaces, the content of this session.

Add-on. We're talking about cloud-based software that connects via API to one of the DSPs that has an ecosystem. Specifically, an add-on is not taxation, accounting, payroll or superannuation software. If your product develops those solutions, you're classed as a DSP yourself and will need to go through Operational Framework with the ATO.

And when we're talking about an ecosystem, we're talking about the collections of add-ons and marketplaces that exist that consume those APIs offered up by a DSP. So the app stores that are in market from Xero, MYOB, Sage, Intuit, Reckon and others across the economy.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): So what is ABSIA for those of you new. ABSIA is the industry association for Australian New Zealand software developers. We're here to represent software developers in negotiations and conversations with government and with DSPs. And we were heavily involved in the development of the security standard and the Operational Framework that the ATO relies upon to regulate and sort of structure their engagement with the software community. We are continuing to expand internationally. ABSIA

Directors and staff are heavily involved in conversations across the region and around the world in a range of topics and industries.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): So where did the SSAM start? Where do we begin with a security standard for add-on marketplaces.

This arose as an action item from the ATO Strategic Working Group in late 2018. And this was broadly in recognition that with the introduction of the Operational Framework, the ATO had secured effectively the first point of connection or the direct connection from software to their APIs. But they had a broad understanding of how software is now working and how applications are connecting with one another that there was a need to secure the broader ecosystem that were connecting to a DSP and then ultimately connecting through to the ATO.

The industry asked DPO to help facilitate that working group. I had the pleasure of participating along with Simon and many other attendees and we were working towards a consistent set of guidelines and standards. The hope was that rather than each of the DSPs developing their own security standards and requirements, we could all collaborate and produce a consistent sane standard. And what we produced in the end was broadly accepted as a portable security framework that maximises security and minimises the amount of work that DSPs and software developers building add-ons need to go through in order to comply.

The initial scope was limited to tax, payroll, accounting, superannuation, corporate compliance and e-invoicing. So the things that are broadly covered by the Operational Framework but as things like the Modern Business Registers are expanded out of the ATO, as they retire ASIC's APIs and move them under ATO infrastructure, we expect the scope of the Operational Framework will expand to fill that space and as a result, the broader ecosystem that surround those new partners and those new players will also fall in scope inside the SSAM.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): The way in which the SSAM is separated out, we have a set of requirements that apply to Digital Service Providers, that's broadly the Operational Framework, they have a direct or indirect API integration to the ATO. They can be desktop or cloud and they typically are pushing and pulling information that includes personal, financial and TFN data. They're fully regulated and certified by the ATO. Doesn't have anything to do with ABSIA, all done through the Digital Partnership Office at the ATO.

Then you have add-ons. Software that provides features or solutions for any other purpose. Not tax, not accounting, not superannuation and does not have a direct API connection to ATO or a Sending Service Provider. Those are typically cloud only and their consuming API endpoints that are provided by a DSP. So add-ons they've historically been called or app marketplace

partners. They typically sync a range of information or exchange a range of information but it may include personal and financial information, but it does not normally store TFNs inside their software. If your application stores TFNs, you may find yourself as a DSP out of the box in which case the Operational Framework applies to you.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): The Operational Framework, that's the minimum security standards that apply to software developers that interact and consume government APIs. As part of that process, those software developers are asked to complete a security questionnaire annually to provide significant information about their ecosystems, their security practices, their certification, their operational processes and any ongoing breach activity. The typical cornerstone of the Operational Framework for many of the DSPs in Australia was the need to obtain ISO 27001 and have that independently certified. The Operational Framework continues to be evolved and change as there's broadly a review twice a year with the ATO where they add or tweak or change some of the specifications as the security environment changes over time.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): For more information about the Op Framework, as always ATO DPO website. For more information about ABSIA and the security standard, I point you to the ABSIA website.

And with that, I'm going to pop on mute and ask Simon to talk through the standard.

Slide Change

Co-Presenter - Simon Foster (ABSIA): Hi everyone, a way of intro, the Squirrel Street business we have been around just over 10 years now and integrated in with a number of DSP APIs. They weren't called DSPs in those days right at the beginning of the process.

And had noted many of the security questionnaires were the same and so as we were going through setting up the SSAM, we took the best of what everyone was already doing and also organisations like Telstra and PWC who have done the same stuff and most people are starting from the point of ISO 27001 and then getting a bit specific.

What you're also going to find as you go through this and I see we've got a mixture of DSPs and add-ons on the call is that each of them have slightly different ways of approaching the problem but you should find that a lot of it is very re-usable. The other thing that Matthew did mention there that I want to highlight, the exception of people who are connected to the ATO via API. So we have a new example here which is e-invoicing providers. E-invoicing providers also have to go through Operational Framework, that'll help with all of this, but of course they don't connect

to the ATO but to each other and so therefore sort of a little bit of an exemption to the SSAM. So still have to go through that process but it should be much easier cause you will have already had to do most of the things on this list for the e-invoicing version of the Operational Framework.

So. What are we doing here?

What we might do, Jason, I see your question we might wait until the end and take them all at once. So Maggie's watching all those questions and she'll bring them back and highlight them and we may open up and chat as well. Given the number of people on here is relatively small.

So what does this mean for add-on developers. Hopefully everyone has already received these and have probably received reminders from a number of your DSPs in the last couple of weeks. You're going to go through a self-assessment process. The questionnaires are subtly different between each. But I know since having just had to go through it, it shouldn't take you more than a couple of hours to do it for a second DSP once you've done the first one. That first one is probably going to take you several weeks. So don't leave it to the last minute because you now have till the end of June to begin that process. If you haven't started yet, you'll want to get a move on.

For DSPs with marketplaces, Matthew's actually going to through that in more detail later on so I'm going to leave that alone.

Slide Change

Slide Change

Co-Presenter - Simon Foster (ABSIA): Okay so what are the things. So we're going to run through it in a little bit of detail here what each of the requirements are. All of it is security best practice. Some of it are things, particularly if you're using Amazon, Azure, GCP, which you actually can't turn off they're going to be in there anyway.

So firstly, encryption key management. This is about ensuring that the tokens you are getting for the OAuth processes of the providers are encrypted. Pretty easy stuff. Sorry, not necessarily easy but pretty sensible stuff. You're going to understand why that's the case. If someone takes those, they're going to be able to arbitrarily get into DSP systems and therefore lodge tax returns or maybe do things like super, which has been in the press recently which didn't come through this particular ecosystem it's worth mentioning.

The other thing to note there is customer identifying information must not be exposed within your app. The definition of customer identifying information is worth digging into in the documentation there. Contact details can sometimes be in there because the ATO uses contact details to be able to identify customers when they phone up and things like that. So you should be very careful with customer info as you would anyway.

Let's move on.

Slide Change

Co-Presenter - Simon Foster (ABSIA): Encryption in transit. This one should be a slam dunk for everyone. Everything that's mentioned in here, I think now it's actually TLS 1.2 not 1.1. Very simple way of testing all of this, go to SSL Labs which it says at the bottom, type in the URL of your API endpoint and your main web server and it will prompt and tell you all the things you're not meeting are best practice. It will also link you to documentation for Appache, nginx and other very popular web application servers and web servers and how to fix it. That shouldn't take very, very long to determine if you're at the small end obviously and you can make those changes easily. And if you're on the larger end and you haven't already done this, I'd be quite surprised. They're all things you should be doing.

Let's go on next.

Slide Change

Co-Presenter - Simon Foster (ABSIA): So authentication. This is the one that's going to trip a number of people up. Which is why we are now expanding two step authentication beyond the DSPs into the add-on ecosystem. I'm not going to spend any time on why we should be doing two-step, I'm assuming everyone on this call understands why it's a good thing.

You do have an alternative though. Which is, most of the DSPs have a single-sign-on functionality as part of their API, so you can implement that, you're going to meet this out of the box and then they're taking care of the complexity. The added benefit for your customers is that mandate for implementing two-factor, they're already been through the pain because the ATO forced it on that community a year ago and so your client base should be much more familiar with this and used to the idea that they have to do it.

You have a few other alternatives out there so that you don't have to implement yourself. Auth0 is a popular one and another one is Authy. Both of which have STKs that let you do this, I think Authy is also free.

Co-Presenter - Matthew Prouse (ABSIA): Before we jump off that slide Simon probably the other thing that's worth flagging around two-step authentication. This can be a significant cost for a lot of add-ons from an ongoing support perspective. We all know that we like to replace our smartphones. So when everyone gets a new iPhone 12, you don't want to be having to support customers manually resetting accounts so they can go and re-enable two-step authentication because they gave their 12 year old their old phone and wiped it without bringing the codes across. We know from the DSPs it can be a significant cost for them to have to do all those account resets and re-activations. So, if you are a smaller add-on developer or you just simply

don’t like spending money, it might work out to be a bit cheaper to implement single-sign-on with the DSPs and single sign up because then, let’s face it the Xeros and Intuits and MYOBs their bearing the costs of those account resets rather than the add-on themselves.

Co-Presenter - Simon Foster (ABSIA): And obviously you need to bear that in mind for your business model as well because you are giving your authentication process to a partner and locking yourselves there. But, of course, that cost of supporting people and getting them through resets and all that type of stuff is pretty high.

You can also, potentially, use Google and Apple and so on that have … I say potentially because some of those providers do not allow you to force two-factor so you have no way of knowing that the customer has actually implemented and therefore you’re not going to meet the standard.

So lots of options for you there. At the end of the day, this is about connecting to the DSP, so the fact that you’re using their single-sign-on you know is going to make sense. They’ve obviously got to have a login in order to connect in the first place.

Slide Change

Co-Presenter - Simon Foster (ABSIA): Indirect access to data. So this one looks scarier than it is.

So very similar to what many of you will have had to do for updated privacy policies and GDPR and Privacy Act, you need to make sure that anywhere your sharing data is made clear to your customers, that it’s applicable in the policy t’s & c’s. You also have to justify it internally.

Again, pretty common. Customers are used to this already. I think we’ve actually reached the point where people click it away without reading it. However it is important that you do the assessment. That justifiable business need piece, a lot of us haven’t done that because GDPR doesn’t necessarily apply to companies that only operate in Australia and New Zealand and this part of the world. You’re now going to have to go through and do that. And you may find along that way that you’ve potentially got some connections in there that you don’t need anyway. It might be as simple as switching them off.

Slide Change

Co-Presenter - Simon Foster (ABSIA): App server configuration. So part of this I covered earlier, the SSL Labs will tell you that. But it goes a step further. So it’s looking at how you implement things like cross site scripting protection and all these types of things. I know that many, if not all, of the DSPs that have started this process now have automated tools in the background that test this and will tell you what to do and how to do better at it.

If you're using AWS or Azure, or GCP for that matter, this stuff is usually pretty easy it's done there out of the box. Just depends on how far into managing the virtual servers, or physical servers if you've got them, you've gone the further down that path you've gone the more work you're going to have.

Slide Change

Co-Presenter - Simon Foster (ABSIA): Vulnerability management. We just went into this a little bit already. OWASP is the standards body here that has been looking for some time at what are the top things that are actually being taken advantage of at the moment, what are those vulnerabilities and how to protect it. You're going to have to provide some detail about how you're doing this. Unless you are using something like a serverless environment, AWS or Azure, where this is taken care of for you in most cases you're going to have to implement something here. You're going to have to look at these. It's going to take a little while the first time you do this. But the end result is you're going to be much more secure, you're going to be in a better position to be able to do it. And once you've got into that, the next time round is considerably easier.

Slide Change

Co-Presenter - Simon Foster (ABSIA): Also keep in mind that this stuff does change over time. It gets updated.

I also know and suspect when we come around to our update, OWASP have just begun the process of releasing a top 10 specifically for APIs. Pretty certain that's going to make its way into the next version of the standard.

Encryption at rest. This one should also be a no brainer for most of you. So this is saying that either the underlying disk or the database itself or the container, at some level you need to be encrypting at rest. So that is in a desktop capacity, you're flicking a button which says that your disk is, when you're installing Windows 10 or MacOS it asks you that question. For AWS and Azure, you can't turn this off. So you're likely to have it there already. If you're running your own again, it's going to be slightly more complex.

This one yep, should be pretty easy.

It's worth mentioning when we began this process with the Op Framework 2 years ago, this one actually came up a bit. A number of DSPs were really concerned about database performance when they were managing their own databases and what encryption at rest might do. End result now, 2 years later is, it really hasn't impacted performance. No one's brought it up in about 12 months.

Slide Change

Co-Presenter - Simon Foster (ABSIA): Audit logging. Again this is the one that might take a little bit more time depending on the nature of your application. So this is a matter of putting some sensible thought into what logs you need. So that if something happens, and remembering it may not be you that's detected it, it might be the DSP that approaches you and says "we've seen a problem, we'd like to know what happened in this instance" or it could even be the ATO that's done that. And again, if you see what's in the press at the moment about issues around getting super early, this is the type of stuff that allows people to identify where it's come from and allowed that Tax Commissioner to come out quite strongly and say this was not the ATO or the ATO's ecosystem. They know it did not come from any of us, thankfully.

So you're going to need to give thought again to this and what you're tracking and you're going to need to prove that you've been doing it.

Once again, I hate to keep banging on about IAS servers, AWS, GCP, Azure have much of this stuff natively turned on by default. In some cases, you cannot turn it off. So you're going to meet these requirements out of the box. Particularly that last, immutable and secure.

Slide Change

Co-Presenter - Simon Foster (ABSIA): Data hosting. This one has gone a bit broader than Op Framework. So Op Framework you need to justify why you haven't stored data in Australia. We're not asking for that here and that's because the nature of DSPs are applying global processes. So a business in Europe that's only serviced European customers, having them justify why they don't store it in Australia doesn't make sense. But that huge community of Syrian data hosters, you're in trouble, you can't operate any more *(laughs)*.

Again this is pretty sensible. Should be a nice easy tickbox for you.

Slide Change

Co-Presenter - Simon Foster (ABSIA): And now this is the extension to what I mentioned earlier about access logging. You also have to be monitoring and breach reporting. Again, a lot of this stuff is out of the box. AWS, Azure, GCP do all of this. I know AWS and Azure pretty well. Both those have tools which would allow you to monitor your own infrastructure if you're doing it that way or things that are not necessarily using theirs. For Squirrel Street, we use all three providers for different parts where they have expertise. And we use AWS's CloudWatch and I've forgotten GuardDuty, that's the other app, and it's pretty simple to set it up to monitor all your logs and centrally do that and be able to meet these requirements. It doesn't just monitor breach reporting, of course, it also monitors your system for errors and other things and I can tell you it's really, really useful even beyond the cyber security things.

Once again, you're going to have to spend some time thinking about what you need here but there's a lot of stuff you can do today out of the box.

Co-Presenter - Matthew Prouse (ABSIA): And I think the other part to add to that. As you go through the certification process or the renewal or review process with your DSPs, have the conversation about how breach reporting works with that particular DSP. So under the Op Framework, the DSPs are obliged to notify the ATO pretty much immediately once they're aware of a breach or a compromise, including a compromise of an add-on or ecosystem partner. Understanding what that process is, with each of your DSPs is rather important. It might be an email for some, it may be logging a ticket with others. Just knowing what it is and having it inside your processes.

Co-Presenter - Simon Foster (ABSIA): Yep, absolutely.

We're getting some questions about that stuff. So this one's probably been asked to repeat what the tools are. So AWS has a product called GuardDuty and it's an automated analysis tool so it looks up the entirety of the infrastructure and then gives you various alerts on it. CloudWatch is AWS's log centralisation metrics tool. Both GuardDuty and CloudWatch have free tiers, which are pretty generous. I think in the order of millions of transactions a month are free and they do the job.

They all have little obscure names for both, all three of the platform providers, most of them do a lot of this stuff out of the box. If you really want to, and this would only be necessary if you're doing Operational Framework yourself, you can look up the IRAP assessment.

So IRAP is the, if you're delivering services directly to government, you'll need to meet a higher standard than any of this and a higher standard in fact that Operational Framework. That's called IRAP. It's an Australian standard. I'm not sure about Google but definitely Microsoft and Amazon both have infrastructure that meets IRAP and they have documentation that says how they do that. That is a terrific place to start about how you might implement security best practices in their infrastructure and what they do out of the box.

There's an obvious one. Everything we've just been through, except for where I've named specific tools, is on our website and it's in the documentation.

And I think at this point I hand back to Matthew. Let's go to the next slide to see if I got that bit wrong, I didn't.

Co-Presenter - Matthew Prouse (ABSIA): So, if you're a DSP rather than an add-on developer, what do you need to do with the SSAM? Because, of course as a DSP, you're governed by the Operational Framework, not the SSAM, it's your ecosystem that you're thinking about and need to think through.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): The first thing with the introduction of the SSAM and with respect to DSPs, this system of self assessment, your add-ons having to go through an annual self assessment or security certification, is the new norm. The ATO expects DSPs to have a certification standard in place for their ecosystems, if you have an ecosystem. So if you operate an API and an app store for your solution, you're going to need to have a set of codified security standards and a certification and self assessment and most likely self assessment process for those third parties as a condition of use.

The add-ons should be self assessing against those standards. So they should be completing that questionnaire themselves. The DSPs are required to review them and they're required to review the responses from their add-ons at least annually.

The self assessment between the different DSPs could standardise. So we know that, for example, Xero and Intuit have both implemented security standards that are almost entirely based on the SSAM. So a lot of the questions they're asking, a lot of the evidence that needs to be collected by add-ons is consistent between those two. However both Xero and Intuit, for example, operate different APIs. So in the Xero questionnaire, you need to answer with respect to how an add-on expects the integration between Xero and your application and vice versa for Intuit and your application.

And I know Simon's about to jump off mute.

Co-Presenter - Simon Foster (ABSIA): So what I'm about to say is if you haven't done this yet, my suggestion is you start with Intuit. And the reason for that is that they actually do some of the initial work for you. So their process has been around for a little bit longer, they've been doing it for quite some time. At least 7 years. And so what'll happen is, once you trigger it off, they'll give you a report. Whereas the Xero one, you start by filling in a questionnaire. And so what'll happen is if you start with the Intuit one, you'll have the answers for your questionnaire for Xero. So that's probably the process I would go through if I'm going to do it. You do still have to fill them in. And it's all still very new for everyone so you may find that the Intuit folks, if you've already done the Xero one, the Intuit folks are in New York from memory, they're not going to know what you're talking about and you may find conversely the Xero folks are more aware of the Intuit one but they're still going to push you back to filling in a questionnaire. Keeping in mind that both parties are dealing with thousands of add-ons here, they have to have a standardised process and that means you're still going to have a bit of work to go from one to the other. This is not a certification, so you can't go here's my certificate, I've already done this. You are going to have to fill in the questionnaires on everyone that you need to do this with. Thanks.

Co-Presenter - Matthew Prouse (ABSIA): So DSPs, we know that we need to complete an annual security questionnaire with ATO. They have made some additions to the questionnaire

as a result of securing the broader ecosystem. The first one you can see in Section E asking "does a DSP or does a product have an add-on marketplace with third parties that connects to an API." Simple yes or no. And then if yes, you're required to provide a list of your third party API integrations. So just a list of the software products that integrates with that solution that have more than 1,000 connections or consume what we would consider a practice client list or the client list or the sensitive information held by a registered tax or BAS agent. That's got a different security rating, you need to provide a list of those third party apps and a hyperlink to their product. That's what's in the current questionnaire. That is going to continue to be expanded in due course.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): Who do you need to report for your add-ons if you're say building business software? All of your third parties that integrate via API with more than 1,000 connections. So more than 1,000 API connections in most cases.

However if you build things like tax software or accounting practice software, third parties that integrate and can consume a practice client list, that includes individual taxpayers, so a list of businesses, a list of clients, a list of taxpayers that belong to a registered BAS or tax agent. You need to include all of those products regardless of how many integrations they have. So if they have one or more integrations, you need to include them in that security questionnaire list that goes through to the ATO as part of your annual review.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): You have obligations to disclose this information to DPO. Just restating as you can see there again, 1,000 connections, practice client list.

In future, so a subsequent update to the questionnaire that's in draft, will require DSPs to provide the date that the self assessment was last completed by each add-on. So as we roll out this certification process from 30 June, future annual reviews for DSPs, they'll be required to report the self assessment date for each of their add-on app partners. Confirmation, so a simple yes or no, that the DSP has approved the self assessment and flag if there are any outstanding matters and that may be remediation work that's in progress by one of those add-ons to comply with the DSP security requirements. They will also be disclosed as a part of that annual review process with the ATO.

The aim here is to give the regulator a clear picture of the operations of the ecosystem so that they can produce better threat modelling and so we can all keep each other, and more importantly our customer's data, as safe and secure as possible as a community of best practice.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): Breach reporting, of course, does apply in this case. Mandatory breach reporting is part of the Operational Framework, and just broadly law in Australia, DSPs are required to report any data or identity security breach of their environments to the DPO automatically using ATO online services for software developers.

DSPs with add-on marketplaces must also report any known data or security breach of a third-party add-on that's integrating to their ecosystem through the same mechanism. And it does say immediately. So if a DSP is detecting or is advised by one of their add-ons that some customer information has been compromised that there has been a security breach or a data breach, they're required to pretty much log in to the software developer portal, notify the ATO and in some cases they may need to notify other parties such as the OAIC or the cyber security centre that a security incident has occurred and the data breach has taken place.

Simon, you've appeared so anything you want to add to that?

Co-Presenter - Simon Foster (ABSIA): Yeah and of course, best practice is you're going to notify your customers as well.

Co-Presenter - Matthew Prouse (ABSIA): Yes, absolutely.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): Implementation of the SSAM. As we know add-on marketplaces have been included in the Op Framework annual review since late last year. The security questionnaire was last published in January. I do recommend all DSPs have a review of that. There are some new sections in there around single-sign-on for enterprise as the ATO begins to add more nuance to the Op Framework. There's also been some updates in terms of minimum security or technical requirements. The questions about marketplaces will expand, they will be part of that annual certification process going forward including as the Operational Framework is updated.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): In terms of timeline and where we are at, January 20, this year, broadly most DSPs are requiring all new add-ons as part of their certification process to complete a self assessment. So to go through a security questionnaire as a new software company onboarding on to an API ecosystem.

Most established add-ons have until about June 2020 to complete that self assessment with a DSP. That appears to be the consistent approach as DSPs have rolled out these frameworks. I have also been sent those in my day job at Xero from a number of our integration partners. So Xero, of course, integrates with other DSPs, we're having to complete the security questionnaire

as Xero to supply that information to some of those payroll companies or superannuation software products that Xero integrates with. So it's pretty standard to get these questionnaires. They're almost boilerplate the SSAM security checklist.

What we can expect however, so the security framework that the standard introduced was August last year. ABSIA will be conducting a review of the security standard towards the end of this calendar year. We'll be firing up some focus groups, talking to our members, talking to DSPs and add-on developers seeing if there's anything in security best practice that we need to change. Simon's already flagged the OWASP top 10 for APIs is probably going to feature quite prominently as part of that review. We can also expect that the consumer data right and the Open Data laws in Australia may have some impacts to the implementation of some of the security standard or some of the risk ratings or approaches that it takes. So we will be starting this review towards the end of this calendar year with an aim to publish an updated standard towards the end, so December 2020.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): For more details about everything to do with the security standard, visit the ABSIA website. It's under Industry Standards. There's also a link through to the Operational Framework. And we will probably summarise the ATO framework in more detail on our website in due course and probably the new OWASP top 10.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): If you would like to ask a question, now's the time. We do have some more slides to finish off this session and sort of talk through Consumer Data Right in particular. But if you've got questions related to the specifics, now is the perfect time.

Now I can't see the questions, cause I'm sharing the slides. So I'm going to rely on Maggie and Simon to be our eyes and ears and only chime in if I need to.

Co-Presenter - Simon Foster (ABSIA): So we've had some questions from the beginning. So one of them is talking about tax file numbers and saying if you store a tax file number, you're not classed as an add-on.

That's because if you store a tax file number, you come under the Operational Framework itself. And the question here is from Jason. Jason why don't we unmute you and you can ask it specifically.

Co-Presenter - Matthew Prouse (ABSIA): And this is why most DSPs removed tax file numbers from their APIs.

Co-Presenter - Simon Foster (ABSIA): Yep. So Jason.

Webinar Guest - Jason: Hi guys. So yeah look I suppose we have a number of onboarded partners that provide onboarding services to support payroll onboarding for the labour hire industry, that's where the question comes from. So they're third party vendors that are actually building onboarding packs if you like. They're capturing that taxpayer data and pushing that through to our APIs to obviously onboard the employee which includes obviously their tax file information. So that's probably where the question came from because I actually asked this question to the ATO when the framework was updated in October last year and I've actually had a different response from what you've provided today. So that's why I'm asking. If that's been further clarified …

Co-Presenter - Matthew Prouse (ABSIA): So if you're pushing and pulling TFNs in and out of ATO systems or they're simply pushing them into your system and then you're effectively …

Webinar Guest - Jason: So we're the DSP. We have a marketplace partner, an add-on, that's actually adding it in to our solution alright.

Co-Presenter - Matthew Prouse (ABSIA): Yep. And so your ecosystem has a security standard in place for those add-on partners that's consistent with the SSAM, I'm assuming?

Webinar Guest - Jason: Yes.

Co-Presenter - Matthew Prouse (ABSIA): So as long as there's a security framework. Historically the ATO has had a view that TFNs broadly don't belong to anyone other than the Tax Office and you sort of rent them and share them with third parties. So historically the Op Framework has considered them in scope but if that product is not consuming any ATO APIs, then yes it would fit inside SSAM instead of Op Framework potentially. The one thing I want to flag there is the ATO is conducting a review at the moment looking at the interactions between software and tax agent systems right now and things like practice management and document management systems that house TFNs are certainly in scope for a consideration under the Op Framework. So watch this space is probably the answer if you're building solutions in that.

I hope that answers your question Jason.

Webinar Guest - Jason: Sure. Thank you very much guys.

Co-Presenter - Simon Foster (ABSIA): Yeah and the context here is you may want to dig into some of the public statements around what happened with the super in the past week or so. That will give you an idea why they're starting to get more concerned again about TFNs.

So we have another few questions.

Alexander. Let me find you on the list here and I will unmute you and you can ask the question so everyone's aware of it.

You still there Alexander? I've unmuted you.

Webinar Guest - Alexander: Yes I'm here.

Co-Presenter - Simon Foster (ABSIA): Great.

Webinar Guest - Alexander: Thanks Simon. So I just wanted to ask an add-on that is not a DSP but connected to a DSP and then that add-on provides an API for fourth parties, so to speak, how does SSAM apply in that case?

Co-Presenter - Matthew Prouse (ABSIA): Ah, the good old supply chain question.

Co-Presenter - Simon Foster (ABSIA): Yes.

Co-Presenter - Matthew Prouse (ABSIA): So the ATO Op Framework has a wait and see section. They've been thinking about digital supply chain for probably the last two years and said watch this space, we'll provide some more guidance in future. To our knowledge, they're yet to finalise their view on sort of the third party that plugs into a third party that plugs into a DSP. I think if we apply some commonsense, we would say the bare minimum securing the broader ecosystem would say something like SSAM would need to apply. So SSAM is almost the wall around the outside and that wall may be one application thick or two applications thick or three or four depending on the kind of data that's being shared and the nature of that data.

So we do know there are some number of ecosystem partners that do have APIs themselves. What we are seeing is broadly they're following industry best practice and they're implementing security assessments and processes that are consistent with the ones you're seeing coming out of the SSAM that are being adopted by the Xero's and Intuit's and MYOB's and Class's of this world. If that makes sense?

Webinar Guest - Alexander: Totally. Thank you.

The second question was two-factor authentication. Is that required for every single, like every individual login or is there a time window of how often it has to be reused?

Co-Presenter - Matthew Prouse (ABSIA): So the Op Framework requirements for two-step authentication, as specified for DSPs, is 24 hours. Although we do recognise some software developers do have different implementations that have been accepted by the ATO. It will depend on the integration requirements from the DSP itself. So when they set out how they define two-step authentication or single-sign-on that will effectively provide the guidance there

for what the add-on will need to do specific to that particular integration. It does depend on the API.

Webinar Guest - Alexander: Yeah, okay.

Co-Presenter - Simon Foster (ABSIA): I would suggest you ask the DSPs you're integrating with what their expectation on that is. In many cases it's going to be bound by their own products and if you go and log in, you'll see what their remember me functions do. They vary between a week and 30 days for almost everybody despite …

Co-Presenter - Matthew Prouse (ABSIA): … 24 hours …

Co-Presenter - Simon Foster (ABSIA): Yeah ATO says 24 hours but I don't think I've seen a DSP that's actually implemented that. Please correct me if I'm wrong.

Co-Presenter - Matthew Prouse (ABSIA): Wolters Klewer, as an example. There are a few.

Any other questions?

Co-Presenter - Simon Foster (ABSIA): There are no more questions in the chat. Ah another one's just come in.

Alison, let me find you and unmute you. Gotcha.

Co-Presenter - Matthew Prouse (ABSIA): If you wanted to be unmuted. You can say "no I don't want to be unmuted" as well.

Webinar Guest - Alison: No, thank you for that.

So we are a smaller DSP. You hear of the likes of Xero and MYOB and that's great. So our entire ecosystem is a few clients using an API that provides access to a very limited amount of data. So we're talking a little bit of inventory, a little bit of debtor information. I guess I'm coming late to the party here but I'm trying to work out how this framework might be scalable so as we can still make sure that everything's secured but that we're not an excessive burden on what are honestly small time web developers using this functionally.

Co-Presenter - Matthew Prouse (ABSIA): So a way to answer that is, the Op Framework security questionnaire that you fill out Alison, as a DSP, asks do you have a third party ecosystem yes/no and then do you have a set of security standards and you have to provide a copy of those security standards. So a DSP, you can set different security standards if you wanted for your ecosystem. So you might take the SSAM as a starting point. Why not? It's broadly the world first ecosystem security standard and then maybe because you've got some

specific use cases because you have limits in your APIs, you may change that for your customers or use it as a template.

In theory, the SSAM reflects industry best practice and good practice in terms of the right sort of technical implementations, the right sort of approaches to logging and reporting and notifications. What we do know is that you have breach reporting obligations to the ATO that you will still need to meet and so will your add-ons.

So probably the first thing is, as a starting point for your ecosystem, make sure you've got terms of use for your developer API and good contracts in place that sort of set out what you expect and from a security standpoint through your ecosystem partners because as a bare minimum, you will need those to continue to pass the ATO annual certification.

Does that kind of answer your question?

Webinar Guest - Alison: Yeah it does. Thank you very much.

Co-Presenter - Matthew Prouse (ABSIA): The whole reason for the SSAM was, broadly, to stop the need for the hundreds of DSPs operating in Australia to have to go and invent their own security standards. Here is an off the shelf sane set that represents best practice and makes it easy for an add-on to comply with multiple DSP marketplaces.

Any other questions? If not, I might move on to our update. We can always come back to questions later.

Webinar Host - Maggie (ABSIA): Nothing new coming through the chat.

Co-Presenter - Matthew Prouse (ABSIA): Thank you Maggie.

Slide Change

Co-Presenter - Simon Foster (ABSIA): And I'm just going to have to excuse myself. The perils of working from home these days. I have a child bugging me who has something from school. So thank you everyone and I know there's only a little bit more to go and happy for you to reach out if you need any sort of assistance. I know Matthew is the same or just reach out to Maggie. And I'm going to say goodbye and thank you at this point.

Co-Presenter - Matthew Prouse (ABSIA): Thank you Simon.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): So my update relates to the Consumer Data Right. So the Consumer Data Right is a new legislative instrument that the Federal Government has

introduced that is designed to give consumers more access to their data. It's designed to open up the economy and facilitate freer exchanges of data between software products and more importantly between things like telcos, energy and financial institutions.

Consumer Data Right is often called Open Banking or Open Banking is the first cab off the rank from an industry perspective. It is being administered by the ACCC. And they've had a number of public consultations over the last six months looking at what kind of accreditation process should exist. What kind of rules should be implemented to govern, particularly third party access to Open Banking or Open Data derived information. So information that has been retrieved through these new required Open Banking or Open Data APIs pulled into other software and then potentially shared with third parties.

The ACCC did receive multiple submissions from ABSIA members and multiple submissions relating to third parties, suggested that the security standard for add-on marketplaces, the SSAM, be considered as part of the security and accreditation model for third parties. The ACCC, broadly, started with a blank sheet of paper and they've then had a lot of submissions from the banking sector relating to how the banks roll out their security and accreditation models for financial institutions. Of course, as you would expect, they are quite heavy for a lot of software companies, so the ACCC looked a little further afield and looked for alternative models. So the DSP Operational Framework and the security standard for add-on marketplaces are currently being considered by the ACCC and are in scope as one of the approaches that they may allow for third parties to use in the CDR / Open Banking world. Further announcements from the ACCC can be expected mid year but at this stage our observation is that the ACCC is taking a pragmatic and commonsense approach. They're also talking and working closely with other Commonwealth agencies including the ATO on the possibility of using the SSAM and the Operational Framework for third parties.

What this means, is not having to accredit your software product against multiple competing security and industry standards in order to go about your business. That's the hope that a DSP, for example, will be able to be accredited under the DSP framework and use that. Similarly an add-on would be accredited under the SSAM framework and could use that where applicable for third parties.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): We are doing everything we can as an organisation to help keep things consistent across the industry. We're continuing to have conversations with Amazon and Microsoft around pre-configured SAAS configurations of AWS and Azure that are effectively SSAM ready for new add-ons as they enter the market. We are continuing to work globally.

The security standard has been shared widely across the industry and across the other regulatory spaces in the Commonwealth and is being actively considered by New Zealand,

Singapore, the UK and Canada. Singapore's just put out a discussion paper relating to data privacy and security for technology. That's just gone out for public comment yesterday. It's designed to be aligned with GDPR but there also are dimensions of the SSAM that are in that consultation paper looking at third parties, apps, APIs and ecosystems.

So we're continuing to do what we can to advocate for a sane and consistent approach globally but also recognising we have something pretty special here in that the DSP ecosystem that operates in this little corner of the world and how that's applicable to the global software space and the global software industry.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): The last thing I want to talk about is a parallel initiative that ABSIA is currently running. All of our members would have received comms relating to this last bit on Monday. But we're conducting a survey with the support of COSBOA and the DPO at the tax office looking at the current and future impacts of COVID-19, both the health emergency and the economic response, and they're impacting the Australian software industry today.

The survey can be found on the ABSIA website. Just go to absia.asn.au. The survey's a big box on the front page. It takes about 15 minutes to complete and it can be submitted anonymously. We are closing submissions for the survey on the 1st of June. We already have a lot of responses from members and other software companies. The more responses we have, the better we can understand what's going on in the industry and that will allow us to share those insights and the conversations we are having at executive levels across Australian Government and with other key industry and policy stakeholders. We will be publishing the findings and sharing them with our respondents and with the broader community. Don't worry, we will not be disclosing individual responses or individual replies in any of our publications. It's just a pulse check of how COVID is impacting all of us right now.

Slide Change

Co-Presenter - Matthew Prouse (ABSIA): I do want to say thank you again everyone for your attendance. If you do have any other questions, pop yourself off mute or wave at Maggie and she'll pop you off mute.

Otherwise, ABSIA is on Twitter. Of course there is on the ABSIA forums on our website for members. Or just email info@absia.asn.au or reach out to Simon, myself or Maggie directly.

Thank you very much everyone and I think it now is afternoon everywhere so have a pleasant afternoon.

Are there any remaining questions?

Webinar Host - Maggie (ABSIA): Doesn't seem like there's anything coming through. So yeah, thank you again everyone for joining us and we will have everything up on the website shortly.

Co-Presenter - Matthew Prouse (ABSIA): Thank you everyone.