dspanz. digital service providers australia new zealand

Introduction

Belinda Stewart - Host (DSPANZ): Welcome everybody. Thank you for joining us.

We're going to get going today because we've got a lot of content to get through and we know everybody's very keen to get that done. We'll be recording this as well, so anyone late joining us will be able to get a copy afterwards.

So, welcome, just a bit of housekeeping to start. All attendees are going to be on mute for the duration of our webinar.

We would love your questions. So, throughout the webinar, if you have any questions, please submit those during the chat function and we'll have time at the end to cover those questions.

The recording and slides for this webinar will also be made available after from our website. We really hope you enjoy our morning.

Slide Change

Belinda Stewart - Host (DSPANZ): I'll start with an acknowledgement of Country. In the spirit of reconciliation, DSPANZ would like to acknowledge the traditional owners and custodians of Australia and their ongoing connections to land waters and communities. I would also like to pay my respects to elders past, present and emerging.

My name's Belinda Stewart and I'm a DSPANZ director and a GNGB director, I'm here today to host this webinar for you.

Slide Change

We have some really exciting guests with us today, so we'll start with Dushyant Sanathara who is the Head of Digital Trust, APAC - BSI. He draws on his extensive leadership experience in technology and a background in EBUS and business management, bringing a distinctive perspective to the governance of technology governance risk and compliance. He's widely recognised for his capacity to craft innovative solutions that enhance outcomes and propel business achievements.

Slide Change

Following from Dushyant, we have Lucas Rowe, who's the governance and risk compliance practice lead from InfoTrust. Lucas has over 15 years of expertise excelling in assessing and proposing practical security strategies aligned with industry standards. He specialises in security, architecture and advisory services, providing clients with practical solutions to effectively mitigate security risks. He possesses extensive knowledge in designing and implementing and leading security advisory services contributing to the management of effective cybersecurity programs.

Slide Change

And our final guest is Charles Gillman, the Chief Information Security Officer at Super Choice. Charles also co-hosts our securities group here at DSPANZ Charles has over two decades of expertise in information security specialising in financial services. He's led security teams at major institutions and held Chief Information Security Officer roles in diverse settings, offering a comprehensive perspective from a background as a penetration tester. He provides practical solutions for current and emerging cybersecurity threats.

So welcome this morning and we will kick off with Dushyant. Thank you so much.

Slide Change

Dushyant Sanathara - Speaker (BSI): Thanks Belinda. If you can give me a heads up, if you can see the slides, that'll be fantastic.

Belinda Stewart - Host (DSPANZ): Yes, they're there now. Thank you.

Dushyant Sanathara - Speaker (BSI): Okay, perfect, perfect. So good morning and good afternoon from from from everybody.

Slide Change

Transition and Beyond

Dushyant Sanathara - Speaker (BSI): I'm just going to touch on the transition as we all know with the initial aspects but I think that one of the key questions a lot of people ask is what is transition as in the word, transition.

So transition is usually used as the terminology used when any standard. When any existing standard changes to a new version of the standard, fairly simple, but there are a lot of other terminologies people use as well.

For example, you may have heard a lot about migration. So migration is when one standard is obsolete, totally obsolete and goes to an entirely new standard itself, not a new version, but a new standard. That's so they are used interchangeably but I would suggest that to use word transition because that's the right way to look at it.

Slide Change

Now, coming back to some of the media questions that you may ask, but, I just wanted to touch on it at the start which is around the transition issues or questions So the standard, which is the 27001:2022 version of the standards was published last year October, the first assessment was started rolling out from November of last year. As we speak, there will be all the certificates will be withdrawn against the old version, which is the 2013 version, which is three years from the time when the original standard was published, which is around October 2025.

A couple of other important things for any organisation. I'm sure most organisations here would have gone through are certified already but if you aren't and if you're looking to get certified, this a key timeline, which means should I choose the 2013 or 2022 version of the timeline for us at P si post April, it will not be possible.

So any organisation that would want to go through or get certified for the first time ever will have to choose the new version of the standard around transition duration. I'm sure we'll touch on it at a later time as part of the Q and A, but, just want to highlight that it depends on the organisation's size and complexity and can be done at any time as at the time of the annual audit.

Slide Change

The transition end date is the 31st of October 2025. What does that mean for us? We need to make sure that for any organisation going through the audit or transition audit, all non-performances have to be addressed, and closed out and a certificate must be issued prior to 31st of October.

So, that's a timeline for us, but as in us, what I mean is by certification bodies, but in most cases, what we would do is we would ensure that all audits for transition are completed on or before August of 2025 to ensure that if there are any non-conformance or any of the any of those sorts, we will address them.

I think the risk period for us is any audits that are occurring after 1st May of 2024 and these are BSI timelines, they are not an iso timeline. So, clients and organisations can choose what they like, but from our perspective, we see that there is a greater risk if any organisation is going through the transition at the very end timeline, which is Post May 2025.

Slide Change

Digital Trust, I think this a question I get asked a lot, as in, what is digital trust? You know, digital trust, as far as BSI is concerned, is about instilling confidence in an organisation where we are making sure that people are empowered. We have systems and technology in place that ensure safety as well as security, compliance, privacy, as well as, ethical requirements. So that's kind of what we mean by a digital trust.

Slide Change

Transition and transition changes. So the first thing that popped up when we looked at the standard itself and even when it was in draft, I think the most, the first thing that popped out for us was the fact that the name of the standard changed, which is privacy protection was highlighted, which is new, but that also sets the tone of what the standard is going to look like or what, what was going to be important as far as the new version is concerned.

Slide Change

So why is the change needed? Obviously, the last version was in 2013 and 2022.

A lot's changed, especially post-pandemic. So I think the way we live, the way we work has changed, you know, tremendously, obviously, the cybersecurity industry has matured a lot over the course of the last 8 or nine years. But we also need to understand that a lot of our workers or people now work from home, they also have their devices, and sometimes they use BYOD, which means their own devices, which is probably another challenge that we come across a lot.

So there are a lot of things that changed but the positive aspects are if you look at the latest version of ISO it aligns or looks pretty similar to some of the aspects used in the NIST cybersecurity concept out of us.

So NIST is a cybersecurity framework that comes out of us, which focuses on you know, detect, respond, recover, identify and protect. Which I think is fantastic because those frameworks that are globally accepted are coming closer to each other than ever before.

The ISO27001 is also now taking on the new harmonised approach as far as the management system is concerned. What that means is that it is easier than ever for organisations to integrate standards, especially if they are certified over and beyond 27,000 months.

For example, if you have other management system standards such as quality management, which is 9001 or safety or environment management system, it will be much easier to adopt the harmonised approach.

Slide Change

Now, if you look at 27:000, month, the way we would look at the structure and key areas of change. So, that is the main body of the document has changed with some clarification on processes. So not a whole lot, there is some then we have Annex A controls that are updated in line with the 27002:2022 Standard.

One of my recommendation is if you haven't already, I would suggest everyone at least look at or download a copy of the 27002:2022 standard because the guidance in that document is fantastic and really helpful, we have editorial changes throughout the document and there are some further clarifications which we will touch on today.

Slide Change

So now when you look at the standards of just highlighted things in red, which talks about some of the changes, so you know, a clause 4 in terms of IMS there is a bit of change there and then when you look further you within planning or planning of changes, that there are some changes and I'll touch on on the changes in detail as well.

Slide Change

Then you have clause 8 which is operations where you can see a bit of change but the whole lot of changes that Lucas will later on, touch on or focus on would be in and around Annex A controls.

Slide Change

So let's jump on to the clauses and inclusions. So 4.4 which IMS is in, clause 4, reads that the organisation shall establish, implement, maintain and continually improve an information security management system. Now, that wording was already there, what it now says is that it should include all the processes. Okay, and also explain the interaction of these processes.

So, that's a key change that is highlighted. Okay, so we need to understand the number of processes that we operate as a management system and there has to be some form of understanding of how they interact, I think the biggest benefit of understanding the integration and interactions is that we do remove any duplication of processes and try and make sure that there are some redundancies and we don't include them as part of our day to day operations as well.

Slide Change

6.3 which is new, which is the planning of changes. It touches on how an organisation determines the need for changes in the IMS, which is the management system. The changes that you make shall be carried out in a planned manner. So any changes that then include changes such as transition. So, if you are working on transitioning from the old to the new standard, which I'm sure most of you are already, those changes should occur in a planned manner is what and how it's highlighted.

Some of the other examples that I can cite are, that organisations very often review the scope of operations and say, ‘OK, we would like to add another subsidiary or another aspect that was not previously covered under the scope and would like to include that as part of ISM is, I am sure you certainly can, but it needs to occur in a planned or phased manner where possible. I think from our perspective, the auditor should be able to see that in terms of what the planning has been done and how it's going to be carried out, this is what we be looking at.

Slide Change

Clause 8.1 which focuses on operations and control talks about two key things. The first is around establishing criteria for the processes. We touched on criteria and their interactions in class form, but we now we're talking about what is the criteria and we need to establish that, in making sure that the controls are implemented in those processes in accordance with the criteria.

So, if there are any instances where the criteria that you've set does not work, happy for you to go back and review those criteria and amend the criteria. But when we are implementing it, we need to ensure that the controls are implemented as per the criteria and if it goes beyond that, it may lead to risk as well. So I think that's probably how we would foresee it.

So, there is no right or wrong in terms of having a set criteria in place and it doesn't mean that you can't amend them, but if you do make sure that it goes through the review process again, and reestablished the revised criteria. If need be, the last bit is the organisation shall ensure that externally provided processes.

This is highlighted in the standard now, products or services. So anything that you do, which is, the way I look at it, is outsourced that is relevant to your SMS is controlled. Now how they are going to be controlled and who controls it, is entirely up to the business.

Obviously, that's not stated within the standard, but from an audit standpoint, it's something that we would like to see around, you know, how those are controlled and who controls them, what is the periodic, how periodically there those are reviewed? So that can form part of your, let's say if you're talking about your supply chain or supply chain onboarding processes, what's involved? How do you make sure that the existing suppliers go through a certain change control? And when you bring in new suppliers, what happens? and as long as they're part of IMS, how do you make sure that they meet the criteria that you've set and that the controls are implemented as well with those supplies?

Slide Change

Now, the control and the control structure. So, I'll touch on the left-hand side first, which is about, there were 114 controls in 14 groups as per the 2013 version of the standard. What's happened now is the number of controls have reduced from 114 to 93.

There are four core groups which I think makes perfect sense and it's a lot easier as well. Which is, organisation, people and then physical and technological controls. So the output of those 93 controls is that we've got 11 new controls, we've got 24 controls that have merged now and there are about 58 controls that are maintained.

It does mean that any organisation that's going through the process needs to review their statement of applicability in accordance and, obviously, review the risk assessment as well. And making sure that the entire Annex A control standards are being looked at, within clause 5, clause 7, clause 6, and clause 8, we've highlighted in terms of the number of new controls in all under organisation controls are about three. You have one physical control, people based controls are essentially the same.

There hasn't been much change and then you have seven new technological controls now that there is, an aspect of control attributes that is very, very new that you may have not seen before, which touches on type of control, the properties as in IMS properties, your cybersecurity concepts, as I said earlier, which aligns with your NIST framework, your operational capabilities and your security domains.

I think the best way to try and use it is to tag them. So, which makes it really, really easier to manage any of those controls that you may have implemented within the organisation and the other aspect is making sure that the organisation-wide view is there for each one of those controls is extremely important. So in interdepartmental mental visibility of controls and control implementation is increased.

Thank you, Lucas, over to you.

Summary of Changes & Implementation Guidance

Slide Change

Lucas Roe - Speaker (InfoTrust): Thanks Dushaynt, really appreciate that. Good morning or good afternoon, everyone from wherever you're joining us. I'm going to share my screen and talk through some of the implementation changes.

I'm very lucky to be joined, I should say I'm really lucky to be joined today by Charles Gilman, who's recently gone through this audit process himself and throughout this discussion or presentation, we're going to ask some questions that are related to some of the changes Dushyant has kindly gone through with us.

Slide Change

So, if I can confirm that I'm sharing my screen and you can see a summary of the slide, essentially picking up from where Dushyant had picked off.

Belinda Stewart - Host (DSPANZ): Yes

Lucas Roe - Speaker (InfoTrust): Thank you kindly. So without going over content that's been covered previously, I do want to take a moment just to reiterate some of the key changes, particularly in the title change.

Privacy protection is a material or a big change, it isn’t a name change or a title change but beyond that, allowing for information and security professionals to understand their privacy objectives and how you can use those privacy objectives, to enable security capabilities is quite important and does help organisations to look at the end state where privacy may well be an outcome that supports by security controls. Though, if you're looking at the end state and your target and what privacy capabilities you have, It's a great place to start.

I just wanted to call that out from the beginning before we get right into it. Similarly, the interested parties' focus in the revised version of the standard, does allow for so some dives to be taken into the responsibilities and the shared nature of some of the successful operations of an IMS.

Slide Change

So I'm going to just spend a little bit of time going through those categories again, which Dushyant introduced these four categories within 27002:2022 organisational, people, physical and technological, all need to be considered in how they're applied to the information assets that you've got within your organisation and I think the attributes component and the control criteria that Dushyant just walked through does allow for some of the right sizing to be done for the controls that you select.

Slide Change

So, I did want to take a brief moment to touch on the important relationship between 27,001 and the Annex A or the controls defined within 27002:2022. The recent changes have allowed for, in my opinion, and many other colleagues of mine allowed for more efficient, well described use of the controls, that'll help to meet your management system objectives and your risk management goals.

So, I, think if you can look to try and see Annex A, as not a walkthrough of exactly what you need to do and how you do it, but more of a guidance as to what you can do to meet the objectives that are described, it becomes a lot more workable. It does, however, require a fair bit of insight and forethought when it comes to completing those activities.

Slide Change

So, ah again, we're not going to go into these changes in great detail because Dushyant has kindly summarised some of these changes, though, I did want to take a moment to mention some of those because an important one was raised around the planned changes.

So, I think it's a welcome change to the standard, though that said like anything, ensuring what changes you're planning and what risks you're actually trying to manage and maintain needs to be extremely clear for yourselves. Otherwise, you run the risk of ironically overshooting the controls that you apply to manage the risk. So, I think it's an important thing that whilst change absolutely needs to be completed in a planned manner. You also want to make sure, when you determine that control criteria, understand what you're doing and when and that it is concomitant to the risk that, it makes sense and it's not leaving yourself stuck in the mud.

I think that's something that we've seen and heard, which we'll touch on, perhaps a bit later. So, I won't go into all of these details but you will receive the summary, a recording of this. So please take the time to read through some of those changes and understand what it means to you.

Slide Change

So, I would like to now get into some of the meat of the conversation and I guess what I hear or what we hear from a lot of clients or colleagues struggling with some of the changes and how to implement them. It's good to always take stock and look at the control objectives that have been newly introduced.

So, there are a lot there, that Dushyant introduced, there's 11 new control objectives that have been introduced and a lot of this new, not just for the adopters of the standard, but similarly, for those going through and auditing your IMS.

So I think whilst there is a lot of almost a material rework in the way that the controls of frameworks have been designed, it lends itself to a really good opportunity to try and take that effort and the time to unpack what's involved and what those control objectives mean to you if they're to be in scope.

So, I mean, we can go into some of these in more detail a little bit later, but I think it might be, you know, well worth asking someone who's been through this, them themselves quite recently. Charles, do you have anything you'd be able to share with the attendees in terms of unexpected challenges or what you weren't expecting when you came up against these new control objectives?

Charles Gillman - Speaker (Super Choice): Yeah, look, I think for the transition, it took a lot longer than anticipated, you know, I came back from Christmas leave at the beginning of this year, I allocated two weeks to cut across and it took a lot longer than that.

So it's not just a matter of simply renumbering your controls and your policies. It'll really depends on how you're managing your IMS and how you evaluate the effectiveness of your controls. But for our organisation, it meant that we ended up standing up a fresh IMS. We use Confluence and then we migrated our policies, procedures and standards across into that new IMS and then we implemented new policies and procedures for the new controls, where it had the most impact on us, especially froma time perspective was measuring the effectiveness of the control. So, we use a ticketing system to assign controls to control owners and then those control owners attach evidence for control effectiveness. So, user onboarding and off boarding, for example, that required us to rebuild that whole process from the ground up.

I think we ended up with something like 188, you know, evidence request tickets that we had to kind of build from scratch and that was kind of exacerbated where a lot of those controls, two or three controls had been merged into a single control. So, it kind of changed the type of evidence and the number of tickets. So, yeah, it wasn't as straightforward as I thought it was going to be.

Lucas Roe - Speaker (InfoTrust): Thanks Charles. That is, I think, that's a common conception, a misconception, perhaps. “I've heard that the number of controls has reduced 114 to 97. Easy. Great. No worries.” I think it's safe to say there's, there are a lot of challenges involved or time that needs to be spent, but, I guess on the flip side, were there any unintended benefits or, improvements that you saw as a result of doing or taking the time to do that material rework and meet the new requirements.

Charles Gillman - Speaker (Super Choice): Yeah, look, I think it's a really good opportunity to critically evaluate your IMS.

So, we normally, you know, tend to build the IMS, we just keep it running, year after year and the business changes and sometimes we don't update, you know, the IMS to keep in track with that and in sync with that. So, it's a really good opportunity to go and really just re-evaluate everything as you're migrating across. “Does this make sense? Can we get rid of it? Should we be adding something else?” So, I think that was a really good unintended consequence and I feel like our IMS is a lot easier to operate now than it was previously.

Lucas Roe - Speaker (InfoTrust): Cheers Charles. I think that's a good call out and what I've heard too in that initial underestimation of what's required to take is SMS from current state to future state is, always a little harder than you expect. You make some assumptions and you dig down into, you know, the depth of your ticketing systems and realise that the practical implications can be real and, time is well spent planning early and upfront to try and determine the impact and indeed what you're looking to actually apply.

Slide Change

And so, we've got a, a number of these control objectives that I mean, I'm not going to go through each of these one by one but there are some that do require you to take the time and understand. Importantly, in the context of your IMS and what you're aiming to achieve are, these control objectives relevant for your business operations? Have you selected the controls? Knowing that these are, this something that is going to assist you in meeting the objectives, because making sure you have got the relevant controls is, goes so much towards ensuring that they're actually helping you, otherwise, you end up with a liability or a control objective, that's not necessarily helping you achieve the business objectives or risk objectives that you've defined.

So, I think we'll go into some of these a little bit later and I'd love to hear questions to be raised about some of the challenges or practical implementation issues that you'll face if you're looking into the new requirements of the standard and again, to a point that I think is worth mentioning is when you get that as Charles mentioned when you get the understanding of your, IMS what you're doing and why you're doing it, you're then similarly able to help communicate to or auditors or assessors or even internal and external stakeholders, what you're doing and why you're doing it. But I think that's a very good call out and something that, we can all take away to try and make sure that we're going through in a relatively consistent approach to try and make sure we're achieving some of the effective outcomes that the standard describes.

Slide Change

So I think Dushyant mentioned earlier that there's some really well-defined implementation guidance that's defined in 27002:2022. We'll touch on some of that a bit later, But I think going in to solve a big problem requires breaking it down into different phases and stages to try and make sure it works for you.

Slide Change

Lucas Roe - Speaker (InfoTrust): So, I'm going to now move on to a slide that tries to highlight some of the practical pragmatic migration advice. There are four things that we've got up here on the slide, that we've just introduced in terms of a plan for a migration to be leveraging useful resources and assessing the controls that are relevant for you too as we've just described.

So, as I mentioned, some of those detailed implementation guidance that's available in the new standard is quite well described and gives you multiple options. So, Charles, did you come across or use any of that detailed implementation guidance from Annex A to assist you or to help define and apply controls?

Charles Gillman - Speaker (Super Choice): Yeah, definitely it was actually one of the kind of drivers for us to move early because we found that the new standard was a lot more usable than the old standard, and the guidance really made implementing the controls and the control testing a lot easier. It just really helped accelerate that process for us. W found it, it just made life easier which is not something you normally use in the same sentence as iso

Lucas Roe - Speaker (InfoTrust): Yeah, no, that's a common theme I'm hearing too and I think it's the changes are welcome from a practitioner's perspective in terms of understanding what can be done, not what the previous implementation guidance or the way the annex A controls were defined seemed quite rigid and this seems to allow for quite a more of a modular approach, if you will and I think that's probably what it was intended to be, to begin with, but perhaps after years of learning, then we've got to this point and do see it as welcomed change.

So I guess we're going to now touch on, I won't go through any of these suggestions in detail but it points back to the earlier comment, around understanding and planning for the changes and leveraging what resources you do have available to you.

There are, multiple things out there to help you but until you've understood your requirements, you don't know what you'll end up needing to ask for help with. So, taking that time and moving to a point where you're going into control selection and adoption, that's right for your organisation helps in multiple ways, as we've mentioned.

Slide Change

So, now going to touch on some of the controls in more detail and again, don't want to go through these one by one, but I do want anyone who is on the webinar to, raise their questions or provide their, you know, thoughts or, queries. I think that's largely what we're trying to get out of today, to try and highlight and share some of the challenges that we've seen in moving towards this new standard and the teething pains that come with it, to try and make sure that we're all as best prepared to use this standard as it's intended.

So, I think one of the challenges that Charles mentioned earlier was around configuration management, for example, understanding the ticketing system, not necessarily configuration management, but the impacts on practical service tooling and processes that are impacted by the change need to be well understood.

So, perhaps Charles, I could ask you to get started with some of these. Did you find applying these newly introduced controls actually helped you to prioritise and determine what you already had and what you may not have?

Charles Gillman - Speaker (Super Choice): Yeah, most definitely. So, I think what you need to look at when you're implementing these, is how much of this are you already doing. because there are probably really good opportunities to take what you're already doing in terms of controls and then bring that into your IMS. A good example for us was, threat intelligence feeds. So, we were consuming threat intelligence but the new control was actually really good because it actually made us document how we were using the threat intelligence feeds and why we were using them. That, you know, kind of brought us to this epiphany about the difference between threat intelligence and actionable intelligence, for example, and so, we've included that into our threat intelligence standard, what is actually actionable intelligence and similarly with things like cloud services.

I think, you know, most businesses are consuming a cloud service or a SAS service already, this is kind of the norm for a technology business. So, all we did was took what we were already doing and incorporated, what we were doing around those cloud and SASS vendors and put them into our existing supplier security policy. So, I think you can run, really ease your implementation, if you just kind of have that critical look at ‘what are we doing?’ That's kind of close to this already.

You know, can you configuration management?, for example, if you're running a window shop, you've got group policy most likely or, you know, you've got Microsoft Intune or something like that. So, you've already got configuration management, you can actually just kind of, bring things that you're already doing into the scope of our IMS and I think that will really help ease some of those implementation hurdles.

Lucas Roe - Speaker (InfoTrust): No, thanks Charles. That's a good call out.

I think in my experience too, I've often found try to have a clear understanding of what you are doing and why you're doing it. It allows for any misinterpretation of the control and how it's applied within the context of your organisation can help from even withstanding.

I'm aware that BSI **is** on the line but some auditor challenges or fixations on certain controls that can often sometimes, I guess, distract from business objectives. But again, the takeaway from that way that I found to be quite useful in managing those distractions at times I probably could summarise, is to be clear on what controls you're using and why you're using them. Then it becomes a lot clearer to say to the business that we have these risks and these are the controls that we're accepting to apply and then becomes more of an objective discussion and unless these are well defined and understood, it can become quite a distraction and ironically move away from the ultimate goal of an IMS which is trying to introduce a repeatable information, security management system, where you can measure and improve.

So, I think as long as those are the goals and that you can use and apply these controls, the newly introduced objectives in a way that helps you to have repeatable capabilities. These control objectives aren't included just because they were pulled out of the air. These are, standards and objectives that are in the updated version and to be transitioned to, for good reason, I suppose.

So, again, there's a lot of a lot of controls to go through and I don't want to go into each of them in detail through business continuity efforts and planning and testing it. It's not necessarily a new objective though, the way in which understanding business impact and planning and testing continuity efforts is well described.

I like BCP and disaster recovery or business continuity and disaster recovery and so do a lot of adopters or those who are aligned to this standard because it can differentiate between business objectives and some of the technical teams, when they're responding to a disaster and what's available. So, I just like the way that it's been referenced in these new or revised standards.

Slide Change

So, there are a number of new controls, I'm moving onto the second lot of newly implemented controls on newly described controls and there's a number of them: data masking, data leakage prevention, strategies, not a technology. Again, monitoring activities and some other web applications and secure coding objectives.

So, there were these, obviously, the challenge involved in applying these controls is dependent on your, IMS and your activities, though, I think some of these are from what I've seen are largely commonly required and depending on the information assets that you maintain. But the data masking is one that's particularly come up quite a lot or been quite impactful and fortunately, there is some good implementation guidance there too.

So, perhaps Charles, what were some of the challenges that you may have had with adopting or applying data masking? or data leakage prevention objectives that were introduced?

Charles Gillman - Speaker (Super Choice): Yeah, look, I'll speak to the data masking because I think the data leakage is probably well understood. There are plenty of technologies out there for implementing that, but, I think, the guidance for data masking is really helpful, but I think the implementation is going to be difficult for a lot of organisations.

For us, it was pretty straightforward, we were able to turn on masking at the database level. It was a feature of our DBMS. So, that was really good, but I think this going to be the hardest control for almost all organisations to meet and implement. It's potentially going to require a third-party solution, It's going to require code rework, it might require changes at the database level and it's to the extent to which you data mask and then you need to think about what you data mask.

So, when we went through that data masking process, we've got now, our primary database with a lot of schemers in there, we really went down and masked down to the field level, which was a lot of work to kind of work out what makes sense to mask and what doesn't. So, yeah, I think that's certainly, the real tough one that people are going to have to work out. What and how are they going to implement that in their organisations?

Lucas Roe - Speaker (InfoTrust): Yeah, that's a great call out Charles. I think, and at risk of sounding like a broken record, it's going back to understanding the assets that you have and taking that time to say 'what requires us to look at protecting this data, at the field level or the column level or road level or not at all.'

I think it's understanding what you're doing, where and why it helps you, to then at least make the task a lot clearer, because the effort and understanding and unpacking those is what ultimately can identity and access management challenge is and using multiple technologies that are available, right? or solutions that you may need is not the problem.

It's just again, understanding the requirements, what you're doing it and, and why so that when you come into the surveillance audit or the certification audit that, that you know, partly to appease the requirements of that standard, but more importantly to appease your objectives of protecting the assets that you have, that you want to look after and manage the integrity of.

So, thanks for those insights. I wish we were able to go through all of the controls in detail and I'm sure in time, a lot of those on the call will do. Again, it can seem quite daunting, but from what we've seen, there's useful guidance in the standard. It can benefit you greatly to take the time, I guess to to meet these requirements.

But, I think what I like to say and share with customers or anyone who listens to me, really is, that risk is not a dirty word and that IMS is here to help us manage our information, and security risk. It's there to enable objectives, business objectives or risk objectives. It's not there to restrain it, all of these controls are there to enable and I think there's one comment that I hear frequently, that I really like, apologies if you've heard it a number of times before. But I remember a question asked was, “What are brakes on a car there for? Often the answer is, “Well, brakes are there to slow you down” and you're saying “No, your brakes are there to allow your car to go faster. It's not there to slow you down” and I like to look at the controls in an IMS in the same way, these controls are here to allow us to go fast.

So, select the right ones work out how big your brakes need to be and go as fast as you can within the risk tolerance that you've defined and that can move a lot of the inherent sort of views of security professionals being the naysayers and the people that will slow things down. Well, you need to slow down when you're going around a corner at 200 kilometres an hour. So, it's good for us to do that sometimes and I just want to try and link the IMS and the updated standard in terms of risk, which is how the standard is, to be best interpreted in my opinion.

So thank you. Look, all, I'm hoping we've got some time for some questions that would have been put into the chat already. But perhaps to close this part of the discussion, Charles, did you have any final thoughts? Having gone through all this yourself and successfully navigated the challenges of the certification audit. What can you share for security professionals to make the most of their IMS and prepare for the new standard?

Charles Gillman - Speaker (Super Choice): Yeah, sure, Lucas, great question.

Look, my advice is to plan for the migration before your next audit, as in, before your next 2013 audit. If you're going to delay your audit against the 2022 standard, make sure you allocate plenty of time because it's not just the migration to the new standard, you actually have to be operating the IMS under that new standard before you come to your audit.

You know, there's no point in coming to be operating it right up until the last minute and then trying to be audited against the new standard. So, operating against the old standard and then audited against the new and my advice is to start the migration the day after your next audit against the 2013 standard if you can.

Lucas Roe - Speaker (InfoTrust): That's some good practical advice, Charles.

The other comment that I would add is if you want to have artifacts ready, to enable alignment with the revised version of the standard, you can keep them, have them there ready in staging and ratify them at times. That will allow you for that control to be met in some cases for these new controls.

Unlike Charles, you may not have already been consuming threat, intelligence feeds or you may not have already been looking at what DLP technologies or strategies you're adopting. So just, you know, also be conscious of the fact that we do have until the end of October 2025, but do, don't, don't let that delay you.

There is a bit of work to be done but also be conscious of the fact that you don't have to throw it all everything to begin with, allow yourselves time to learn and get used to the new processes and control objectives that are defined. Thanks, Charles for sharing your insights and practical advice and I'm hoping we've got some questions on the line that may have come through. Belinda, have you seen any?

Belinda Stewart - Host (DSPANZ): Yeah, that's no problem. So I'm just going to share my screen again. It won't be a second. It doesn't want to work for me today. Here we go.

Slide Change

Q & A

Belinda Stewart - Host (DSPANZ): We do have a couple of questions, but please, if there, if there is any more, please put them in the chat.

One of the questions we had is, ‘Do we need to do a transition audit with our existing surveillance or recertification audit or is it perhaps better to go through a gap analysis before your audit to transition to the new standard?’

Dushyant Sanathara - Speaker (BSI): Yes. A very good question. I think we get asked that question very often, any organisation can go through their transition audit at any time. Preferably, I think most organisations choose to go it at the same time as the next audit or upcoming audit, which could be a surveillance audit or a transition audit.

Absolutely, no issues with it. As far as the gap is concerned because it's the new version of the standard, organisations can choose to go through the gap. I always suggest that's probably one of the best practices to try and understand where the gaps are. Most organisations obviously are with regards to resources, you know, may have their own challenges. I'm not talking about financial resources, I'm talking about people as well. And I think an ag output of a gap analysis gives you a clear insight into what are the areas that you need to focus on to address to meet the requirements of the standard, and not worry about things that you've already got covered. So, yes, I think gap analysis could be a fantastic start to understand where the gaps are.

Belinda Stewart - Host (DSPANZ): Excellent. Thank you, Dushaynt. Another question we've got here is, ‘What happens if you're unable to transition during audit?’

Dushyant Sanathara - Speaker (BSI): Okay, so, it depends when you don't transition. Obviously, as I said, if someone's gone and organised an audit on the 25th of October of 2025 and not being able to transition, obviously, the license will not be active and they have to go through the process again, but we're not talking about them, we're talking about in general, what happens?

So, if you go through an audit and if you're not able to meet against all the requirements of the transition, your current certificate remains as is in terms of valid because if you're meeting all the requirements, but what you certainly can do is if there are any nonconformer or any areas that are identified that needs to be addressed, that can be done via follow up audit and then a revised certificate can be issued. I think that's probably an area where we always insist that you ensure you've got sufficient time on your hand. As Charles and Lucas already said, the changes may seem that they are fairly simple and the number of controls may have reduced, but the reality is every business is different, their implementation may be different as well. It is important to understand those changes and implement them thoroughly because at the end of the day, it's not about an audit. It's also about making sure that we are working to protect our business too.

Belinda Stewart - Host (DSPANZ): Excellent. Thank you Dushaynt**.** Can you tell us what happens to your current certificate? Once you've done the transition to the new standard.

Dushyant Sanathara - Speaker (BSI): Yep, pretty much everything remains the same, which is the name of the organisation, the scope, everything remains the same. The only difference is that the new standard will be reflected on your copy of the certificate. The expiry dates on the certificate will also remain the same, but you will see a change in the issue date of a certificate because the certificate has been issued in the middle of a cycle, a three year cycle.

So, that's the only change that you will have, everything remains the same. If you are going through the change or transition audit as part of your recertification audit, which is at the end of every three years. In that case, the new standard will be reflected, your expiry date will be amended to next three years and whatnot. So, I think that's probably how the changes will be reflected on your certificate.

Belinda Stewart - Host (DSPANZ): Thanks Dushyant, just to clarify with that, if you go between your recertification, so if you go on a surveillance year, essentially, you're resetting that three year cycle from the date you transition.

Dushyant Sanathara - Speaker (BSI): Yeah, for surveillance, you don't need to reset three years. So your expiry date remains the same. For example, if an organisation goes through the surveillance audit in January of 2024 and their certificate is expiring in 2026. When a new certificate would be issued? it will still say Jan 2026 in terms of expiry date. But the reissue date is where you see the change which may say that the certificate was originally issued at XYZ time, which is when the first time you are certified and then the reissued date will say January or February of 2024 whenever that change would have happened.

Belinda Stewart - Host (DSPANZ): Excellent. Thank you.

Lucas Roe - Speaker (InfoTrust): Belinda. I can actually see a question, a couple of questions in the Q and A. I'm sorry, I'm not sure if I picked that up. It may have come through during, I'm assuming, it could have come through in the data masking discussion only because it's around, the question is on encryption. How do you write controls and encryptions? Are you separate ones for data, rest data and transit monitoring keys etc.

The question relates to trying to find the right balance of count versus quality of controls and want to understand your thoughts about hashing. Now, this a trick you want to unpack not knowing what, where and why and how you're using those tools. But can I just ask or confirm if you wanted to add to that? Was that the question in relation to the concept of data masking?

And if so, my advice and I'll see what Charles would have to add to this too, is understanding what cryptography can be, where you're using cryptography and why you're using it because where you're using cryptography for transport layer security, it is going to be different to where you're using it for database and encrypting data within a table or a database, for example.

So, understanding where or why you're using those encryption controls is important and then defining what you're doing around generating the keys where your standards lie, what you're accepting of how you're managing them through their life cycle and protecting them and then similarly disposing or rolling off them.

There's a lot to unpack there but defining the standards and then writing controls that ensure where you're using encryption or data masking techniques is meeting your requirements and having measurable controls that will help meet those objectives is an easy thing to say and a hard thing to do in practice.

So, Charles, do you have anything to add to that question? I'm assuming it's about data masking.

Charles Gillman - Speaker (Super Choice): Yeah, I'm reading it as encryption at rest and encryption in transport. So, I'll kind of answer it in that context and that is, don't overcomplicate it. I would have a cryptography policy that defines when you're going to encrypt and why you're going to encrypt and you should be encrypting pretty much at rest.

And, in transit, so, you know, SSLs everywhere, it's not difficult to actually have encryption at rest now on most operating systems. So, that's pretty straightforward. A key management policy saying, you know, how are you going to manage those keys and then a key management plan, as you said, when you're going to rotate them and roll them, there's a lot of good advice out there for what good looks like in terms of cryptography.

So, you know, things like TLS 1.3 and there's similarly a lot of information about what looks bad in cryptography, you know, so some of those old ciphers, TLS 1.0 for example, the old SSL suite. So, just having those in your policy and just saying these are the banned encryption algorithms, this is what good ones look like, just kind of keeping it simple. I think just having those three things for me, the cryptography policy, the key management policy and a key management plan.

Lucas Roe - Speaker (InfoTrust): Yeah. No, thanks, Charles. That's, awesome. Then to the flip side when you're going to go and test them understanding how that's being applied because it does actually creep beyond into a few areas.

For example, having a bit locker recovery key available to users is going to be a problem. So, understanding where your key material is, to begin with, and how you're restricting that key material and the key and secrets management processes has multiple touch points, but you can keep it simple, but just also take the time to validate where and how you're meeting those objectives too because you might find some simple changes that can help I improve security objectives quite materially.

So thank you so much Charles for those insights and sorry to interrupt Belinda. I just saw that question. Did not want to leave it unanswered.

Belinda Stewart - Host (DSPANZ): No, that's good, thanks for that Lucas. Another question we've got here is, ‘is there any recommendations for tools potentially to handle threat intelligence?’ Obviously, that's newly put into the standard. So is there anything you can recommend for our members?

Charles Gillman - Speaker (Super Choice): Oh, if I can jump in there. Look, there is plenty of vendors out there. Spruiking their Threat Intelligence services and feeds and they'll happily charge you for it, but at the same time, there's a lot of open-source threat intelligence. There are things like Dragon News Bytes, there's, I think called Threat Mirror. There's quite a few, I think if you just do a search for, you know, free or open source threat intelligence, you'll actually find quite a, quite a few that come through as newsletters or RSS feeds or similarly, you can join the ACSC.

So, the Australian Cybersecurity Center, and you can set up what's called an MISP server and the ACSC will start sharing threat intelligence with you through that MISP server. That's free, you know, you're just downloading a VM or a package to go and install MISP, which is the malware information sharing platform. But it's beyond malware. It's a lot of tools, techniques and procedures that the bad guys are using.

So there is, I'm pretty much using almost all open source or free threat intelligence and I'm getting some really good info from those and we've actually written some internal tooling to go and actually make sure that we're getting the threat intelligence that's relevant to our organisation's assets and applications and operating systems, you know, I don't want to just be flooded with lots of information.

And certainly trying to get that threat intelligence for our vertical, which is financial services. So being a bit targeted otherwise, if you're not, you'll kind of be overwhelmed with a tsunami of, you know, a CVA has been released and you gotta remember there's like 29,000 CVAs that have been released in the last 12 months. So pick and choose carefully.

Belinda Stewart - Host (DSPANZ): Excellent. Thank you so much.

Slide Change

Conclusion

Belinda Stewart - Host (DSPANZ): It looks like we're out of questions. So, thank you very much for everyone joining today. I've just put up quickly a little QR code, for anyone to scan and it will also be sent around after the webinar. We are just after a little bit of feedback from our survey.

Slide Change

So thank you for joining us. It's really lovely having everyone on board today and I just really want to give a massive thank you to Dushyant, Lucas and Charles for coming on today and sharing your wisdom with us. You're all a wealth of knowledge and I know that in every interaction I have with the three of you I’ve learnt so much. I'm sure that all of our members online today have really enjoyed listening to you today and providing some insight on the changes to the standard.

So, everybody on the call today as well. Our friends at BSI run some training with this transition to the standard. They also have a very special offer which we will email around to everybody as well following on from this webinar. So keep an eye out for that. So thank you.

I hope everyone has a great afternoon and hopefully, this is the first in a series of many things that we will be looking at next year with our cyber group at DSPANZ**.** So thank you for joining us. And we'll see you next time. Thank you.