Webinar Transcript

Building a right sized compliance and risk program for SMBs

So hi, everybody.

Welcome to our webinar today titled building a right sized compliance and risk program for an SMB, a small to medium business. My name is Sean McDonald, and I shall be your moderator for the next forty five odd minutes.

Firstly, though, thanks so much for attending today. We always appreciate the effort you make to be here for our live events.

During the session, if you have any questions, please try and use the q and a button on your toolbar. It's against chat. It just enables us to keep track of everything. And finally, if you stay through till the end, which we hope you will do, of course, and as is customary for our webinars, we have a special treat for you. By answering a really quick one minute survey at the end of the webinar, you'll go into the draw to win our beautiful gift hamper worth over four hundred dollars.

Now for those not too familiar with BoardPro, we are a board software provider sometimes called a board portal.

We serve around thirty five thousand users around the globe across about thirty four different countries.

We enable organizations to prepare for and run their board meetings more efficiently and effectively with less time and deliver more impact and value for the organization.

And as much as we are a board software provider, part of our wider mission is to make the fundamentals of governance free and easy to implement for all organizations, especially those with resource constraints. And one of the many ways we do this is by providing free access to over two hundred plus business templates, guides, and resources on our website.

And these website these, sorry, these webinars are also a great way of accessing key governance knowledge without the, necessarily the time commitment associated with in person events.

So for the next forty odd minutes, just relax and listen and try to add to the discussion by asking as many questions as you would like.

The full recording of the webinar along with the slide deck, and transcript will be made after the webinar. I'll be sending that out probably on Monday now.

So without further ado, I'm gonna have the team introduce themselves starting with Liz O'Callaghan. Over to you, Liz.

Thanks, Sean. Hi, everyone.

My name is Liz, and, I've been working in a, in risk and compliance for about fifteen years now.

But I spent the first ten years of my career working in those banking and insurance environment. So, obviously, they had a lot of resource, and they need a lot of resource in that risk and compliance space.

But then about, well, five or seven years ago, I I just found myself working and found a lead businesses and smaller businesses.

And what I realized, it was a very steep learning curve.

What I've kind of spent ten years learning on all those risk heat maps and all those kind of reporting didn't really mean much when you went into a smaller business, but I really thrived in the smaller business space. I always saw operations and sales being really valued in a small business, and I always wanted to have compliance bring that kind of same value, to small business. So I really took it on and decided, hey. Small business is for me and really showing, how compliance adds value in that space. So, here I am now mostly working in those small to medium businesses, also both regulated and nonregulated.

So it's really obvious why regulated businesses need those compliance frameworks, but getting to work with nonregulated businesses is even more special because you actually get to show the value from compliance. So that's been a little bit about my history.

Thanks, Liz. Mark, over to you.

Hi.

I'm Mark Benechevich, and I guess I'm here largely because I'm hosting a podcast series called Governance Bites, which is now on its hundred and fifth episode where I, interview executives and directors about various topics related to governance.

In my day job, I'm head of industry engagement at Partners Life, and part of what I do in that role is work with small financial advice providers to help them understand their obligations and how governance and compliance can help them meet those obligations and help their businesses thrive, mainly through a governance lens, working with the directors.

Fantastic. And last but by no means least, Rupert, over to you, sir.

Hi. So, Rupert Carline. I'm, managing director of a KiwiSaver provider here in New Zealand, called our KiwiSaver.

And, look, I'm a regulated business. Right? So, fundamentally, risk and compliance is is a core part of what we do. But I think the the main reason I think I've been invited here is to talk about our journey because I think we did a pretty good job with Liz's help, I must add, of creating a risk and compliance framework that adds quite a lot of value to our business now, but versus strangling us, which is, what the traditional method I think would have done to us.

Thanks, Rupert. So, Liz, back over to you.

Thank you.

So, I think what we'll go over today is, why compliance still matters and, actually, what is compliance in in a business.

Then we'll just look at what right side compliance framework actually looks like, and how it can create some value. And then, hopefully, we can just give you some step by step guidance as to, hey. Here's step one, step two, and some foundations on how to build that. And then, hopefully, if we have time, I've just got a bit of a case study of a business that I've worked with. This was a tech business that wasn't regulated and how we help them to build a risk, a right size compliance program and then your compliance action plan. So I think we'll just get straight into it.

And so yesterday, when Mark and Rupert and I caught up, we were like, hey. What what actually is compliance? And often when I hear about what compliance is, they say, you have to do it. You don't want your directors to go to prison. And and while that's true, I really don't want to throw that around too much as being the reason as to why you should have compliance.

I think we make a lot of promises, to our customers and, staff and suppliers.

And so, honestly, I think that is a big part of what what compliance is. It's not just about laws, but it is about the promises that we make. And I thought I'd just, get some input on Mark and Rubik. I thought you did have some really good comments to make on that yesterday around what compliance is and what it means for your business.

And, Mark, do you wanna start with that?

Yeah. Sure.

I it's a term that in our industry, particularly working with financial advice providers, they roll their eyes a bit when the word compliance comes up.

It's this thing that I have to do because the government tells me I have to do it. And I'd like to turn that on its head and say, as you say, you know, what are the promises you're making to your clients? Yes. What are the obligations that you have under the law, and and what is the service that you're offering? And the compliance to me is as a director or as one person in a business, how are you confident that everything in the business is operating the way that you want it to operate?

That it is meeting the the values or that you set out, that it is is following the processes that you've defined that give you comfort that you're doing everything the right way and looking after your clients. And all compliance is is is checking that that stuff is happening the way that you want it to happen and giving you confidence that your business is, you know, representing the values that you're you're putting out to the market. So it's a positive thing. It's something that really adds value to your business. It's not something that you do because somebody else tells you you have to.

Hello. For me, it's the same. Right? It's, hey. We're we're a regulated business. We have lots of people trusting us with their KiwiSaver, their their retirement savings.

For us, a compliance program is is really important because I need to make sure that I'm doing what my client my and my team are doing exactly what our customers expect. Right?

And so therefore, for us, compliance is all about making sure that we're fulfilling our promise to our customers.

And I thought I'd share a really good example of when I went in to work with a business.

So I got invited to help a business out. They had just obtained a financial services license. And prior to me coming in, they had got a compliance consultant to come in and write all of their policies.

And I guess what they got was a library of policies. They look beautiful. They're in a ring binder, and they they were great. And they're what I would call the Rolls Royce of policies. So this was a really small business. I think they only had, like, seven staff.

And so what happened is the regulator came in about six months later, and they said, you know, great. We gave you your financial services license. Now we wanna see how you've actually implemented what you said you'd do. And when they came in, they found out that most of the policies that were written were not actually implemented. And not only that, but the staff didn't even know what was in those policies.

And I would say that these policies, they were two ring binders like this, and they were a few hundred pages long.

And, so this was quite a long time ago, and this was actually what got me thinking. Actually, you are much better off to have a very simple compliance program and be compliant with it than to have this beautiful compliance program that's all documented a few hundred pages long, but, actually, the staff don't know what it says. They don't know why they're doing what they're doing it why they're doing what they're doing, and it's just not being done. So, actually, what we had to do is basically start over again. We had to strip all of those policies back, and, we started from scratch. And on the next slide, we're actually gonna talk about, I think, how how we did that how we did that. So the first thing we did before we wrote any of the policies is we went and we did a risk assessment.

I believe that you should always start with what are the risks in your business. Because if you don't know what could go wrong or what is going wrong, it's really hard to define then what policies you should at least start on. Like, I think we know all the policies that we should have, but risk really helps you to prioritize your resources. It helps you to decide, actually, we should start here because we deem this to be a really high risk to our business.

Because the honest truth about small and medium sized businesses is we don't have the luxury of all these all these staff members sitting here and and working on all these beautiful policies. And it's really important to bring your staff in. So, Rupert, I'm quite curious to hear from you in terms of when you started with looking at the risk in your business, how did you bring your team in on that? And did you were you able to get buy in from your team?

Yeah. I think so because so we ran workshops, as simple as that. So we we got our executive in the room or the senior people in our business in a room and to kinda go, look. What do you what do you think the risks are? Because at the end of the day, they're the ones at the coalface. They're the ones talking to customers, dealing with our partners.

They know it far better than we do.

And then when we kind of that what that did by making sure that they were involved in that that process of identifying the risks, then when we came in with kind of, controls or other things afterwards, we could go, well, you told us that was an issue. So this is what we're doing to make sure that it's we you told us that was a potential issue. So this is what we're doing to make sure it's not kind of doesn't turn into a real issue on the way through.

And then I think the beauty about that is then we rate we rate those risks. So very simply, you don't even need to be a risk, specialist to be able to do this. You can literally rate there's two types of ratings you can do. The rate of that risk, before you have any controls in place and then, hey.

Look at your controls. What mitigancy do you have in place to mitigate that risk? And then rate that risk again to see the likelihood and the consequence of that risk once you consider all of your controls because I think it can be really easy to get lost in the business. You're like, oh my god.

We've got thirty key thirty key risks, and we're gonna fix them all. And in fact, you probably only need to really focus on one one, two, or three risks at a time. And that's and and that's how you just don't overburden your staff with a whole lot of, risk and compliance work. Like, really focus on what matters.

And, Mark, do you think there's a risk that you have come across in the business where it started out small, but because it wasn't tracked early, it kind of escalated into something quite big?

Yeah. Absolutely, Liz. Just before I dig into that, one thing that always comes to mind for me is, you know, when you've got, as Rupert says, a a team of people that you can bring in and

discuss the possible risks, you're in a really great space because you you kinda need that challenging, the various views to get this right.

And often, I find myself working with people that are one or two man shops or person shops, and it's a real challenge to get that list out.

You know, I always find that you're looking at a blank piece of paper and saying, what could go wrong? You might get half a dozen things down, but you may not broadly think of everything. We have a really huge, strong tool that we can throw into the mix these days with the large language models. You know, go into your large language model, do it don't put anything confidential in but a quick description of your business and say you're a risky expert and identifying the key risks that are coming my way, and you'll get some really solid output that that will help you along this journey.

To come back to your question, one example, was, you know, working with financial advisers.

The a lot of advisers hadn't really devoted enough time to considering what the change in law could mean for their businesses.

There was you if if you watch near the press that was happening at the time and the commentary particularly around the press, you'd see a lot of advisers that were, oh, wow. It's me. This is happening, and, you know, I don't like it and and these sorts of things and kind of bearing their heads in the sand rather than saying, okay. This is happening.

What can I do to adapt to this change and and help my business thrive? So, that lack of early identification very much manifested in digging into what that change could mean for their business and and how they should adapt to it.

That's awesome. So I think, and I really like what you say around getting some tools to help you define the risk because there are so many tools out there now.

And then we go into obligations, and you probably could risk work on risk and obligations at the same time. But then you need to actually capture what do I need to comply with. And, yes, it is the law, but there's also contracts. You've also entered into some contracts with some suppliers.

You've got regulations.

Come up with the top regulations or top obligations that you need to track and then break them down into really bite sized pieces and put them in a register. And we're gonna go over registers in a minute and how you track all this data. But, the foundations I feel that you need to know is what are your risk of the business and what are the obligations that you need to comply with. And, again, I've gone into businesses, and I've seen especially in the banking world, I remember we tracked every single piece of legislation, and there were each there may be a hundred obligations, individual obligations under each of those piece of legislation.

I just think great for a bank. They've got multiple risk and compliance teams, but not helpful again to a founder led business or a small or medium sized business. They're not gonna care about all these all these obligations and just having a whole list of them, not that helpful. So let's risk rate them to start with the key ones, I think. And then, and then we're gonna go on to how can you show that you are compliant with those obligations. So when you're building your risk registers, you can also build your controls register at the same time.

So when you're building a risk, you're coming up with, okay. How what are the mitigants that we've got to reduce that risk? Perhaps some of those mitigants that you've also got in your controls register are the very things that help you be compliant with your obligations. So it's really important that you start mapping all of this risk data that you've got.

And there are some really great no code tools out there that you can buy that does all of this for you. We'll go over that. But if you've got your key obligations and then the most important thing is track very simply how you're compliant. What are the steps in your business that you're taking to be compliant, with those obligations?

So that if the regular regulator came in, you can very clearly say, hey. The we know we're compliant because these are all the obligations that we track, and this is how we're compliant, and this is the assurance. And next, you know, the next layer of risk maturity is then start testing all of those controls, and this is the assurance we've got to say that, yep, we've tested those controls, and we're really confident that we're compliant with those obligations.

Yes. Can I just pop an example there? Would that be okay?

One of the things that, you know, is applicable to almost every business, probably every business now, is the risk of cybersecurity.

So an example of this would be to identify cybersecurity as a risk, and then say, well what are the things that we do to reduce our chance that either we could get hacked? And that will be things like having up to date antivirus software, ensuring that all your staff have long strong passwords and are trained in looking for phishing and those sorts of things. So there's sorts of controls you may have in place. You may also have, controls that reduce the impact on your business, such as having cybersecurity, cyber risk insurance.

So these are the sorts of controls you can put in place. A risk around cybersecurity, what could go wrong, what What can you do to minimize the chance that it goes wrong? And then are you checking? Do you do you train your staff around understanding their, their their obligate well, how how they can keep themselves safe, training them in in safety around cybersecurity, and, you know, checking that the password's being changed, that your software is up to date, that kind of thing.

That's kinda how this ties together.

And, Rupert, how did you decide what obligations your business was gonna track?

Pretty simple when you're as regulated as we are, Liz.

We have at least four pieces of legislation with about a hundred pieces in each of them that we need to comply with.

Love it.

So, Liz.

I have a question that's come in from Mark, which I just wanna clear through.

Yeah. Go through.

Mark sorry. It's Marco, not Mark. By having such a broad definition of compliance, how do you distinguish between what compliance requires and what's ethically required?

I assume you might want to keep compliance and ethics apart. Thoughts on that?

Well, I think for small businesses, risk and compliance isn't really integrated. So, like, I I don't know of any business small to medium sized business that has a separate risk team and a and a separate compliance team. So in term I guess what I do is I come in and practically say, yeah, what what do we need to comply with? So that's our contracts, the promises we make, the rules and regulations.

But in saying that, we do have policies and procedures in there, and I do consider, like, code of conduct as part of as part of those core core documents that we should have. So ethics, I think, is very much part of it. Like, I think we want to be doing the right thing, but what the right thing is from an ethics point of view that's up to the business and can look so different across lots of different businesses.

Can I I've I've I've got quite a strong view on this one? Okay. And so we in our shop, right, we're we have what's right and what's wrong. And and it's kind of as simple as that. Right? And for us, if it's wrong, there's lots of things that we refuse to do and we because we don't think they're ethically right about our clients. And for my staff, if if we find them and we've got controls in place to make sure that they're not doing those things, because fundamentally, that that's breaking the promises that we've made to all of our stakeholders.

So to me, I think we get into these really vague and washy worlds if we try and say, look, that's legally fine, but it's ethically wrong. So look, try not to do it, but it's not the end of the world if you do it. That's you're gonna end up in a world of hurt. It it's very simple. And I think you've gotta be in a world of it's either right or it's wrong. And the role of a compliance program is to make sure that our team are not doing the things that are wrong. And wrong can be ethics, it can be regulation, or it can just be a a number of things, but it to my mind, it all sits in the same bucket.

But, also, that's where culture comes in. So, also, like, employing a compliance culture. So typically not just up to the compliance manager to say, hey. I don't think this is right.

You would hope that your team are stepping up and because they're used to this compliance culture, because they're used to the code of conduct, because they're used to regulations, because they're used to tracking all this data, the staff are now starting to say, hey. Is this right? And so that's also about, you know, another big topic is around culture and how do you implement a compliance culture into your business. And literally, by bringing your staff in on the journey, that's gonna happen.

It's just gonna naturally happen when your key staff are the ones saying, this is the key risk in my business. And, actually, it's keeping them psychologically safe because I know a lot of people when when we start implementing risk and compliance frameworks, the staff are really relieved. They're like, oh my god. I've been hanging on to this for, like, a couple of years.

I've known this has been going on, but I didn't know who to raise it or what to do. And now we're saying, well, we're giving you the avenue to raise it. We're saying that, yes, this is a high risk. Actually, we now recognize we don't have those controls in place.

So I think that if you start with these foundations, just a byproduct of that is you'll start to implement that compliance culture where I think that naturally happens.

And now just the next part of it was registers. I actually think registers are the unsung heroes of compliance.

But if I see another risk register on Excel, I will probably scream.

They need lots of formulas. They break. And then the person that built it leaves and and your registers are breaking. And the key to all of this is linking data.

So what we want to be doing is you build your risk register. You build your controls register. You build your obligations register. You build your policy register, which is just a list of all the policies you have, and then you're linking all the data.

So in your obligations register, then you you can link your controls. In your policy register, you also link all the controls that you've referenced in each of those policies so that when you go to update a policy, you know which controls also need reviewing and need updating. In the risk register, you've linked controls. So even if you you can build an incident register now and link link risk to it.

So at the end of the year, you can do a report very quickly saying, hey. We have forty five incidents.

Actually, ten of those related to this one risk. I think that indicates that we're not really managing at that risk that risk very well. So, I know I've used some tools. Like, I'm a big fan of monday dot com myself.

It's a no code tool. You kind of do have to build it and want to get used to it. It's really easy, to use, but it's you can just build all these registers and mirror columns and link columns, and and it's really easy. But there's other tools out there.

No code, really cost effective. Gone are the days where you need to pay fifty thousand dollars for a specialized risk management system.

But I believe in order to justify investing money into compliance, you really need to track and you really need to be able to show, hey. This is the benefit we've got of it. Or, hey. We need to actually put some resource over here because we're not managing this risk that well. So I don't know, if we've got any comments from Marco River around tracking and building regions.

And the companies that I work with are often doing things on a smaller scale than this even.

And we worked, at Partners Life, we put together a a a support program to help advisers document their businesses to get ready for licensing. And we worked with a compliance adviser who was fantastic helping us put this together. And she, put the policy the policy documents were one or two pages, nice and nice and lean for a very small business, and the controls existed in the policy.

They were repeated in the obligations register, which was the only better duplication that you had. But your controls, and the obligations register were all in one place. And then, the the person who was checking whether everything was happening correctly by by testing those controls, if they found anything wrong, they'd pop it in the incidents register. So it kept it really lean and clean.

The calendar simply says, you know, this month, these are the activities I need to do. I need to do my quarterly compliance testing and go through the obligations register and check it. Anytime they found something wrong, pop it in the incident register and raise it to discuss with and that's, you know, usually their directors could and a small business. So the tools are fantastic.

Linking all this stuff together is great.

You don't necessarily need to jump in at that depth, at an early stage. You you can do this quite effectively, at a at an even simpler stage, I I believe.

So even, I've I've done some work with, sole financial advisers who have decided to set up their own, financial advice provider, their own FAP. And even even though it looks like quite a lot here, you can still do all of this. And, of course, everything is right sized. So your your registers can be really simple. What you track can be really can be simple. It's up to you to decide what's important to your business as to what you wanna what you wanna track.

And I think that is the beauty of building your own registers, is that you get to decide what's important to your business.

And so once you've, decided once you've decided what your key risks are, first of all, I think we actually wanna start with the risk management policy. So before you go in, and start recording all of these key risks in the business, I think it's really helpful to say, actually, let's write a one page risk management policy that says that defines what risk is for your business, defines the roles and responsibilities, and then the escalation process. So let's set that all upfront before we even start implementing our risk and compliance framework.

So, there's lots of different categories of risk. There's financial, operational, regulatory. So we can categorize our risk.

And then I think it's really important to also set a risk appetite.

So what we want to what the business wants to know is when you're gonna escalate that risk, when you're gonna escalate it to the managing director, and when does it need to be escalated to the board? And so you get to come up with a risk matrix. And, again, there's lots of tools online as to how to create a risk matrix and, again, keeping it simple.

And then you get to define what a low risk is, a medium risk, high risk, and extreme risk is. So, in terms of financial loss, a medium risk could look like, hey. We don't wanna lose any more than twenty thousand dollars a year. If we lose twenty thousand dollars a year, that could potentially shut us down. So if that's the case, maybe maybe that needs to be escalated, earlier on.

But, you know, for banks, they have they can afford they can afford well, not afford, but they don't the board of directors don't want to be hearing about risks that are costing them ten thousand dollars. That needs to be managed by the managers, and so they have they have specialist escalation processes. So define for you what a medium, low, medium, and high risk is for you and the escalation points. And I just think that takes the burden of the staff, and so set set that upfront. So I would say that's step one. Step two, I would run a really practical workshop like Rupert described earlier. Identify your top risk, determine your obligations, and do that with your staff, and just document them in that very, in that very easy register that you've created.

Liz, there's a couple of questions just come in here, which I think we can, clear through. Jenny's asking, can you give an example of a control?

And John asks, where does your cap fit in?

Yeah. So a control is anything that you put in place to mitigate that risk. So a control can either be preventative or detective. So control so reconciliation is a very is a good example of a control for financial data. So So if you've got someone preparing, some payments, you might say a control is a reconciliation, and, that is to prevent that risk from materializing because, hopefully, that reconciliation someone someone does a reconciliation of the data. And, hopefully, if there's some wrong data in there, they're gonna pick up on that earlier on. And so then you get to change you get to change that process before the mistake even happens.

But then there is a detective control as well, which is if if the risk materializes, you're gonna pick up on that risk really fast and hopefully, fix it really allow you to fix it really, really fast. So, some

other controls are, quality assurance reviews. That's a really good control. Or segregation of duties.

Those are the typical types of controls that we'll see in the business, but I don't know if Mark and Rupert wanna add to that.

I I gave the example earlier of a few controls around cybersecurity, you know, things around password management and, making sure that you keep your antivirus software up to date, those sorts of things.

Having checks around and you you've got your complaints registered in step four here. But looking for things like trends in your register are are that you're getting a a series of common complaints. And if so, you can look into the underlying cause, and find out how you can adapt the business so those complaints are less likely to happen in the future. So there's a a number of examples that you could use there.

So I think it all comes back to where your risk sits. Right? So it can be all of those things or, you know what, you might have a business which high working capital and and needs cash. And so therefore, your controllers that your CFO is presenting or someone in your business, your accountant is presenting cash forecasts to you on a on a weekly or monthly basis.

Fundamentally, if you if you start with a view of, hey. Where are my risks? And then you go, how do I control and how do I mitigate those risks? And that's that's how I've always thought about it rather than starting at the templates or starting in what everyone tells you about it.

You you're the only person that can define that. Right? Because you're the only person that can define what's a true risk in your business.

And and I think in that vein, Rupert, a lot of people are doing this kind of activity anyway.

Yep.

It's just, not necessarily knowing the jargon.

Yep.

So you can type it by jargon.

And not documenting it. I think you'd guide it like, most businesses I'm most businesses I go into are actually already doing this stuff. It's not documented. It's not documented about how often.

So you have control frequency, and you have a control owner. And I think that's really important too. So often someone's doing the control, but it's not necessarily clear on who has accountability for that control. So it's really important when you're doing a control register just and and can literally just be a list of all the controls that you have in your business.

Just make sure you have someone that's ultimately responsible for that control because we won't, over time, wanna start building accountability.

And as for the compliance assurance program question, that's a great one, but I think that really does come as phase two. The first thing is to implement your risk and compliance program. Then your compliance assurance program is coming in afterwards and checking is our risk and compliance program working? How well are those controls being executed?

How well are those controls designed? And are they actually mitigating the risk that we, want them to mitigate? And so I always say, actually, let's build the foundations first. Because if you come in with the compliance assurance program too soon, that is when I think you do start overburdening the staff.

And you're testing stuff that's not quite implemented. You don't know how often, they're being implemented, or you don't know who's quite responsible for it. So I think it's really important to build the foundations and then and then move over to the compliance assurance program.

So I thought it'd be really helpful just to go over a case study. So I worked with the kit business. They weren't regulated. I mean, they do have to comply with the privacy act and, you know, like all businesses do and things, but they they didn't have a license. They they decided that, hey. We actually wanna start implementing risk and compliance into our business and start implementing that culture.

And so, hopefully, by now, you've known what we actually went in and did. We did first thing we did is we did actually write the risk policy. We worked out and that actually took, a lot from the business. So we we spoke to the CFO. We spoke to the board of directors.

We actually involved all the senior leaders even in that risk policy. And we said, hey. These are gonna be the categories of risk. This is how we define a risk.

This is what a low risk, medium risk, high risk. This is when we're gonna escalate it. So the policy and I think it was two pages defined all of that. Then we went and had workshops.

So, the director was actually involved in every single workshop. So that was really good for ensuring we got buy in from the from the staff. So we meet with each senior leader one at a time. So we met with the leader from marketing.

We met with the leader from finance. We met with the leader from all the different departments.

And then we said, hey. If you what were the top risks that, keep you up at night?

And we went through them, and then we worked out what the risk was, what the cause was. And if that risk materialized, what would be the consequence of that risk? Then we went and rated those risks, and then we said, hey. Do do you think you have any controls?

And that was a really interesting exercise because they did have controls. But in my mind, I would say, oh, is it documented? And they're like, no. It's just something we're trying to do in our head.

You know, I do a check, and if it's done, I don't document it anywhere. And so we would document that control down, but we would just make notes. Okay? If we wanna strengthen that control, this is what we need to do.

And we used we did a self assessment of all those those controls, and we used that information to then rate that risk of what would be the risk of this now materializing considering all these controls that we documented.

And if it didn't materialize, what what impact would that have on the business.

What came out of that was actually so we had, I think, seventeen risks, but three of them, even after we considered controls, still were rated as extreme risk. So that was quite eye opening for the board of directors. We're like, hey. We've actually got three risks. And one of them was about privacy. One of them was about how data is stored.

So, that actually justifies some money being invested into into mitigating that risk down to an acceptable level to the board.

And so, again, we escalated those extreme risks up to the board of directors.

So I think we've got some other steps on the next slide.

No. We don't. Sorry. So I think so, then what we did is we just tested those controls over time.

So I think that was that was really important. And the feedback that the feedback that we had from employees working there was phenomenal because they actually felt like a big weight had been laid off their shoulders.

They knew they knew there was these things going on in the business, and they were just like, well, I don't think we can do anything about it. So to see some things being done about this reset was really worrying them, I think, was was quite motivating to them. So that was definitely an example of a business that hadn't done anything before, who'd gone in and done something.

And by the way, they're still not at the point of their compliance assurance program, so they are still building those foundations. And I think in year two, they have a plan to then build a compliance assurance program and do some assurance on those controls.

So what could you do if you've got nothing, got nothing in place?

I would start with drafting that one page policy, that one page risk management policy, to be honest, because I do believe it all starts with your risk for the business. So start with that, and, there's lots of resources online on how to build that risk policy. And I think the most important

thing is how you rate those risks, make it really tailored to your business, and then clarify the roles and clarify the escalation points.

Then I would absolutely just run that risk and compliance workshop.

You don't have to be an expert as three components to a risk.

What's the cause?

What is the risk? And then what's the consequence? And if you can put that together or even if what is the risk?

And then I would also if you've got time with your staff, identify the controls and those risks as well.

And then, of course, set up your simple registers.

So, hopefully, you're a little bit more encouraged to try and find some of these really great systems that we have available now that are actually really cost effective.

There are no code, really easy to build registers.

I would just look for systems where it's easily able to capture data, but then also link that data. I think it's really important on that on that linkage.

Liz, we have a question in from Maddie. She says, one of our directors strongly believes that documenting risks is a risk itself, I e, if the business acknowledges the risk in writing, we might have greater legal consequences if that risk eventuates.

Oh, I love that. Think?

Well, I called Shine Compliance for a reason, and that is shine light on something that is already dark because that risk is there whether you acknowledge it or not. And so I think the worst thing you can do and it's really unfair on the staff to turn a blind eye to that risk as well. So I think you're in a much better position to say, actually, this risk exists. And in fact, everyone in this business knows it exists.

It's not hard to identify that and then shine light on it. And then then it is up to the directors to say, are we going to accept this risk, or are we going to treat it? And then it takes the responsibility and the burden away from the employees because, personally, I feel it's really unfair to have that, burden on the employees. They're the ones on the ground that know. They know this risk at this. So I think it's really kind to your staff to provide these escalation methods.

I think there's another really important point, which has actually just also been put in the q and a, is that, if it does go pear shaped and ends up in court, the the the directors will still get done, fundamentally.

If they don't know about it, that's on them. That's not on the staff. And I think that's that's what's really, really important. Right? Is when you look at a regulator, when you look at the courts, you look at anyone, their view is the buck stops at the directors.

And, fundamentally, it's not management's problem. And so, therefore, if the directors don't know what's going on in the business, then that's on them. That's not on anyone else. So that's, yeah.

If it were me, I'd be very, very, very scared getting that response from someone that I work for.

And you're in an even worse position if the issue was raised and evidence has shown that it was raised and you've and you've ignored it. So doing something about it and not necessarily succeeding is way better than ignoring it and sweeping it under the rug.

Yep. Back to you, Liz.

Alright. And then then we're just gonna link everything together. I honestly just can't stress this enough how important it is to link it, specifically your incidents to your risk because I think that makes it really easy to do some reviews on how well you're managing a risk at the end of each year or every six months, however you decide how frequently that is. Also, like, linking your your controls to your policy register.

Just so you know, oh my god. You know, we've got this policy. We've got our financial policy or financial advice policy, and we've got seventeen controls linked to that. That's a really important policy.

And, again, it just helps you realize where you need to put your resources because often in small businesses and medium businesses, you cannot be everywhere. You do need to prioritize. And so by linking everything together, that really allows you to do that.

And then, of course, report to the leadership and the board. Tell them what you're up to. Tell them what the risks are in the business.

Tell them the things that, we're working on. So reporting is really important to show the value.

And then I really think it's important to create accountability. But merely documenting all this data will automatically do that, especially if you have risk owners, if you have control owners.

All of a sudden, that person is now responsible for that data. So, incident owners. So if an incident comes in, it gets assigned to someone out in the business, and they become responsible for that. So I think, hopefully, if you're starting from from scratch, hopefully, that provides a a way to where to start. And, yeah, hopefully, that's helpful.

Can I add to the end there, Liz, that, when you are doing those checks of your controls, write down what you've done? You know, keep document your work so that you've got evidence that you have been doing those checks.

Absolutely.

I think probably my one big learning through our risk and compliance journey is actually and I think this is where businesses go wrong.

It's actually everyone.

The truth is that the the risk and compliance starts at the CEO at the directors, at the board, flows through the CEO, and then needs to flow through the rest of the business. That it's not something that's palmed off to a risk and compliance consultant or a risk and compliance manager or someone else. It's actually it needs to be driven by the leadership of the business because that's and then it needs to become an important part of the whole business.

And you'll end up with a much stronger business for it. And I think that's kind of where a lot of the businesses that I've seen in the past have gone wrong. They see it as something they have to do. And so therefore, it's it's palmed off into a corner versus something that actually can add a lot of value to the business and deserves a lot of time at the CEO and board level as well.

Fantastic. Well, that brings us to a close, team.

Thank you, Liz. Really appreciate your, presentation today. That was right on time. Fantastic.

Thank you.

Feel free to connect with, Liz, Mark, and Rupert, everybody on LinkedIn. I'm sure they'll appreciate, your connection there.

Monday now, you'll receive an email from BoardPro, which will include the transcript, the link to the recording, and the slide deck as well. So just as you leave the webinar, don't forget to complete our really short one minute survey going the draw for our hamper. We'll announce the winner on Monday as well. So thanks again for your attendance, everybody. I hope you enjoyed the session today with Liz, Mark, and Rupert Caroline.

Look forward to seeing you all at our next webinar, everybody. So have a great day.