Take on Board

# Transcript – Susan Staples

**Susan Staples**

Thank you for having me. By the way, it's quite different when you first mentioned coming in, I certainly didn't expect to be doing it on zoom. So this is quite new. And I will admit that I do have my own boots on because my feet are cold. So that's quite a nice novelty to be able to speak about risk in my boots, I think I have spent a lot of my time in risk. Probably my whole career, if I think about it, starting really in the operational side of things I worked in finance and in the energy sector, before I moved to KPMG, where I was in their risk consulting practice for about 15 years.

And there is consulting practice at KPMG is quite broad. So I started in internal audit, and then I moved into sustainability. So that was when we were going to have a climate policy and then we weren't and we didn't know we didn't. So there's quite a lot going on in that space. But what I really learnt through my time in sustainability is that it is around risk management but around risk management of non financial risk predominantly and a lot of risk management has in it Cost focused on financial risk.

A lot of boards focus on financial risk. So what I tended to see with some great things happening in the operational space, particularly in sustainability, there was a lot of work going on within an organisation around starting with environmental risk, certainly around some of the other material risks that was starting to emerge a lot more.

And what I really understood there was this great stuff was happening at an operational level. Now a lot of people who really wanted to manage risk manage some of these long term and non financial risks, there was a really serious lack of engagement on that topic at the board level, which meant that not a lot of these things were getting traction or weren't interested in it.

They were much more interested in the short term shareholder value. And that obligation around operating in the best interest of an entity was really taken as being shareholder return or some sort of financial return.

What we're saying now, it's starting to get a bit of profile, the value of risk from a strategic and board level is certainly getting raised and the Royal commissions that we've seen recently, really bringing that to the fore. So it's great to see, from my perspective, something I've certainly been identifying as a challenge, particularly to get a lot of that just the recognition of how non financial risk is important and just as important as financial. But what's the board's role in that and the board has a really strong role in risk management, a lot of risk management tends to get done at operational level.

But this really this top down view of risk is critical. And that's essentially what I've seen coming out of the Royal Commission is that, that focus on top down risk, it has been overlooked, but it is essential. So yes, what I wanted to do today was really look at the board's role in risk, but obviously

aware that not everybody has the same level of understanding of risk management. So I'm trying to do a little bit of both trying to juggle a little bit of what I want and a little bit of greater insight, hopefully that you get that. Okay, so here's an overview of what I wanted to talk about and look at some of the trends in governance and that increasing focus on reasonable level.

And then I'm going to anchor the discussion around the best practice standards for predominantly around the ASX because that's where the better governance, the principles and recommendations sit and a lot of go better practices driven by that, look at some of the common challenges and then opened up for discussion, the board's role in managing risk, you know, how, how could a board or what's the role of the board into dealing with some of these unprecedented and unpredictable risk? And I understand you've been spending the morning talking about COVID, etc.

But what could have been done, what should have been done? And is there actually anything boards can do to help organisations really try to understand what some of these unprecedented, unpredictable risks, there's so much uncertainty and it's around trying to deal with some of that uncertainty. We're saying this whole board role move from a compliance focus and a financial focus much to a much more macro focus and this is where some of these things are coming into play because you can actually see the impact that these bushfires, droughts coronavirus, terrorist attacks, economic impacts, Brexit even and Royal commissions are having an organization's and they probably weren't in their risk register.

So what does that mean? I guess the trends that we're seeing and the expectations of boards and from a governance perspective and how risk fits within that a lot of the things that we're seeing will be around reputation, trying to protect a reputation, but I think one of the biggest things that I've started seeing is accountability.

So how are boards being held to account for some of the risk management practices or lack of and you see in the pack that I sent, you'll see that I put in a slide around some of the impacts on an organisation with respect to risk in relation to across the organisation, so there was a lack of candour. In some of the reporting, there was poor communication, there was siloed mentality. And all of those can be dealt with from a risk perspective. And there's an obligation on the board to be able to say that they know what that framework looks like and that they understand where those risks sit in their business. And I think you'll find that Haines and some even out of the Royal Commission. There was definitely a lack of oversight from the board on some of these risks.

The other two things that that we're seeing is this really a much greater demand for disclosure and disclosure. If you look at some of those indicators, there are some of those reporting frameworks. Their disclosure is around the non financial stuff. So we've got a six which is obviously for listed entities. They're being asked in the latest update last year to have a lot greater disclosure on a whole range of areas of their business, including non financial risk in that scene, seven points For explain that in a little bit more detail, but you can also look at the global reporting initiative, you also look at the right across them, you'll get into better reporting, all of these things are emerging because stakeholders, expectations of stakeholders that aren't even necessarily shareholders, just community just regulators really wanting to understand that and have a lot greater transparency.

So there's a risk part in that as well. And the final part is what I've talked to in terms of sustainable performance. So it's not just about financial return in the short term, it's much more broad than

that. So if we look to what the standards are saying, and sort of look at where, you know, ethics, corporate governance principles are essentially a good benchmark for better practice. They're not compulsory, but for listed entities, it's a reporter explain why you don't and it is actually adopted quite generally across many organisations that aren't listed as the standard of better practice.

So if we look at the last iteration of that, which was February last year, principle seven, which is around recognised and managing risk had been updated a little bit and strengthened. One of the key things in that was 7.4, which talks to disclosing any material risk.

One of the challenges that I'm going to talk about in that context is what is material because it's quite subjective. So understanding what materiality is for your organisation, it's actually a key part of that strategic top down risk focus that I was talking about from a board level.

The other elements of the principle are really around the governance structures that you have for risk management. So that's looking at making sure that you have a risk committee, making sure that it has some independent directors on that committee, that the chair of the risk committee is not the chair of the board to create that level of independence.

And then there's also the assurance function and the assurance function being that the board needs to oversee the risk framework in the organisation so that one assumes that you have one and two, that they can get comfortable. But that it's effective, and it's robust. And it's identifying all of these risks, because the market is expecting those risks to be managed.

And if you link it back again, to your fiduciary duty as a director, your obligation is to act in the best interests of the organisation. And that's actually being warned a lot more than financial interests. It's broaden to the sustainability of the organisation, the ongoing viability of the business now and in the future. And that can be even the economic place that your organisation has in the greater community. So there's a lot more pressure on boards than they used to be. And risk is playing a huge part in helping boards to, to get a handle on what that means to manage their disclosures to be more accountable. And this standard has actually ramped up quite a bit in terms of the expectation. So what I wanted to sort of focus on here with some of the challenges in those areas of governance, assurance and assessment, there are some common challenges.

And one of the things that we're seeing is that the value of risk management is increasing. There was actually a survey that I was reading today. And I'm really happy to share that with you guys. It's from the governance Institute. And they've done a risk management survey.

There was a statistic in there that said, the value of risk management to the board has gone up from 70% in terms of people understanding and yeah, we think it's valuable, gone up from 70%, last year to 84%. This year. That's quite a big jump. But it's great to see that that value is being recognised. But I think what's happening is the translation of that is difficult. So we know that it's important, but how do we actually get it embedded in our organisation? And what's our role as a director?

So from a governance perspective, I think one of the key things that we're seeing a lot of is the risk communities themselves, often their risk an audit or their Financing risk. And what tends to happen is it's just a, I think a legacy issue that we're still trying to move through, is that audit takes precedence that finance takes precedence. And anything to do with risk tends to get dropped down to the bottom of the agenda.

We've run out of time. It we'll look at it next time, look at the risk register, maybe we'll give it 10 minutes, but actually the risk register one, they're often way too big, and to be looked at in isolation, and not looked at, you know, with respect to the strategy with respect to performance against strategy, then it's really losing holiday value immediately. So we say that a lot and there's been a lot of discussion in terms of Do we have a separate risk? Or do we have a risk an audit committee and then make try to use the agenda differently to ensure that we get risk and give risk the priority that it needs. Secondly, around governance that risk is is not often a part of strategy development.

So in many organisations, I've seen strategies development, the risk guys come in and go, Well, yeah, there's a risk here, we'll update our risk register. But in actual fact, they're hand in glove. And if you have a strategy and you're looking at what is it that we want to achieve? What are we going to do? What do we want to what do we need to do to get there? The same conversation should be around what's going to stop us from achieving those objectives?

What is it around those scenarios that might influence how we shape them? And what are some of the opportunities that that might create from a business perspective? And one of the big things that you might have seen out of COVID, or even in the past 510 years is this evolution of online or sort of contactless stuff like Uber and Amazon where the strategy for many organisations particularly retail would have been, we're just going to go sell we're going to open up shops, not even particularly anticipating that Amazon might come.

So let's enter, coming to Australia, and then we're going to have to change our business model completely. We've done an assessment of some of those trends early on, from a strategic point of view, we might have been able to pick up some of that and being able to get ahead of that rather than having to respond quite quickly. Mine's now in a bit of trouble. There's a lot of retailers have been closing over the last 12 months.

So it's how do you use risk as part of that strategic discussion, and there's a real role there for the board to do that. The other one we see is that the risk culture is often poor. And when we talk about risk culture, we're really talking about people's understanding of risk. How risk is used in decision making, have risk is used as a management tool rather than as a blocker for doing something. And that reporting and awareness, and often even just as simple as and I've seen this quite recently. What is the definition that people have of risk management because I think you'll find a lot of people will define risk differently, even around the room, but particularly across an organisation. Often people will think of compliance some people think it's OH&S. Some people think it's strategic. Some people think it's operational. So it's about getting consistency within the organisation and leading that from the top.

The last one that we say from a governance perspective is that the risk return appetite is often undeveloped, or it's too static. And I'm not saying need to change that every week or every month. But it does need to be reviewed regularly, particularly in a context of an environment like externally here where it changes a lot. And does your appetite for risk and return change. COVID is a great example.

Would your risk appetite for investment change now that COVID is in place, with your risk appetite for opening up in a new area or closing down a particular part of the business? Is that going to change now because of that environment changing? So, as I said, it's kind of picking up on some of

these things around how you think about the risk strategy discussion. And how you can then use that in the boardroom to help really help with decision making racial shell allocation and alignment or realignment of strategic objectives. Because sometimes what you will see in the risk reporting context, so the risks that are coming up is that you can use some of that information to say, well, we were going to focus over here. But because we've got this risk situation, now we want to actually just redirect or maybe reprioritize, some about our objectives and taking that lens can be really useful.

So just to quickly touch on assurance, some of the common challenges in assurance are that Firstly, internal audit plans are not always based, all linked to outcomes. So the principle seven talks about assurance and it talks about internal audit, it talks about external audit. One of the things I get a little bit frustrated about is that assurance is often only seen as order and it's not so assurance over your risk management for Work is an important part and internal audit is an important part of that assurance programme.

My view is that assurance is much more than that it's a much more personal thing in terms of how do I, as a director, get assurance that our risks are being managed effectively, you can rely on internal audit for some of that. You can rely on representation from management for some of that. But there are other sources of information that you can look at. These are really good examples of doing things outside the organisation. It might be scoping for more what's happening in the media, what's happening in the industry, asking a lot of questions, even just from a culture perspective, walking around or observing what's happening in the organisation, looking at the dynamics between management and executive can give you a really good handle on what's the culture like in the organisation, and is that giving me some sort of indication? You know, it's not all about the audit report. And it's not all about you know, the formalities of it. There's some nuances in that as well. The other parts that I just wanted to pick up on was one that definitely came out of the pain review. Bad news is not reported. We see that a lot. We see management trying to, I guess, make it look a little greener than it normally is.

My view is as a director, if you were not getting any red, that's a red flag in itself. And you should be saying red. And if not, then I'd be asking, are we actually linking our internal audit plan to our risks? Are we wasting money looking at stuff we already know we do well, or is management trying to hide something? Or is there kind of a cultural thing there around performance, and then linking that performance from the outcomes of the audit to remuneration? So there's some leaders there in terms of what that might mean. Important to understand how that all works within your organisation.

The other part of it is that often you'll do an order and we'll say, Yep, management are going to do this, here's the recommendation management are going to do that great packed, there's nothing that's ever actioned and followed up.

Or another great example is that a recommendation might be well, let's put in a new policy. And we'll tweak this and we'll do that. But it's never actually followed up to to determine if that's actually had the right impact to determine whether that's been an effective response. So management have said what they're going to do. But are they actually is it the right action? And how do we track that, which is where some of the reporting and the measures come into play? I guess the last point there that I wanted to focus on that assurance is not always historical. A lot of people think about it.

Insurance is like, did we do this? Well, have we done that? Well, I think particularly in the internal audit space, there's a real opportunity to make it forward looking. So how do we know where the bad news is? To identify those gaps so that we can prove that and have a much more forward looking view. And using assurance from that perspective, I think there's still a lot of this backward looking assurance psychology that we're dealing with, I've seen quite a lot of the other thing is I think people confuse internal and external audit a lot.

This is a little bit of, I guess a bit of an overview for those of you who aren't familiar with this three lines of defence risk framework. And I think the important part of this is shows you where you can apply some of those assurance functions. So you'll see the board and risk and compliance committee sort of sitting across each of the lines of defence. Now the lines of defence are really just a metaphor for this sort of Castle in the moat. So you've got the first line of defence and they call that the first line because it's really where all the controls are happening. So if you think about when we think about a hospital situation, the first line of defence will be the nurses, the clinical people, the staff all out on the floor, putting in those controls every day.

That's the first line of defence without that you might as well Have risk management at all you need that that's the control environment. The second line of defence is around risk management function. So this is where you'll have the policies, the procedures, setting, the standards and the templates. And I guess that reporting function, so it's trying to join the top down, and the bottom up. That's the second line. So that's like a second check. The third line is your independent assurance. That's where you get someone from an external provider to come in and give you that level of comfort or a bit of a check to say, this is what we're doing. So from a board perspective, there should be those kind of three lines, you should have those in your mind about a three lines of defence. And we're some of those questions that you might have around risk management. You can direct them to those lines of defence. And then I just posed those questions there and how do you get that assurance of the director? It's about asking questions around how we going from a frontline perspective. Can you get some data on that, particularly if it's a risk, that's high risk. The second part is like, what's our risk framework? Is it robust? Do we have a right policy? Do we have the right reporting coming into a set some of the questions you could ask around the second line.

And the third line is obviously your assurance function, which you probably have some questions about what they would have found by looking and making sure that red is considered to be a good thing. Like we want to know what's going on. We want to know where the problems are, tell us where the red is. So we can help and we can maybe reprioritize and reallocate resources. I think from a risk culture perspective, that's really important. The last area is risk assessment. So I guess there's a real challenge around when we're looking at that 7.4 to an organisation to report its material risk. It's the question of what's material. Often what's considered material is what's Top of Mind at the moment, it's going to be pandemics. If you looked at the World Economic Forum Risk Report global Risk Report last year. Most of the risks that were in the top right hand box, were environmental, I think four out of five are environmental. That would have been relevant three months ago, when we have bushfires.

If they did that assessment again, now, we get a different result, presenters in this day, and it's and it's okay to be there. But you just have to be mindful that that's what it is. Interestingly, too, in that survey report that I was referring to, which I'm happy to link everyone up to talked about the fact

that there are still some fundamental risks that boards are struggling with. One is talent. One is environment. One is economic shock. And one is innovation and innovation came up in the context of Amazon, Uber disruption from innovation, whether it's digital, or whether it's just a different, you know, society's changing, so how do we respond? So it's interesting to say that those risks are still recognised as being some of the biggest ones in this recent survey. But obviously, organisations still struggling with having manage those.

The other thing that's starting to emerge in the risk space is that this acknowledgement that risks are interconnected. And we know that anyway. But what we find in the risk assessment context, within organisations is a lot easier to look at risks in isolation, it's a lot easier to say, well, this is a workforce risk. And this is an operational risk. And this is a strategic risk. And this is they're all quite separate. And we'll allocate each of those risks to different executives to take ownership on. But what you find when you start to unpack that is that they're all incredibly interconnected. And sometimes it's easier to well, sometimes it's, it's much easier to look at things in isolation. But when you try to address a particular risk, because you've done a risk assessment on a risk, that's in isolation, that you may actually be reading mysteries in your resources, because you're not actually looking at some of the interconnectivity of that.

The last one, there is risk issues versus events. And what I'm trying to get at there is, it's probably around how risks are defined. And if we look again, at this survey that I've got in front of me, one of the biggest risks that organisations talk about was reputation and brand and damage to that now, my view of that is that reputation and brand impact is probably more of an outcome than a risk in itself.

I think if you've unpacked the risks and looked at what what's the risk, but what's causing that to happen, so what would be a cause of reputational damage? And it could be a whole range of things. It could be an environmental disaster could be poor handling of your workforce, it could be modern slavery issues, it could be a whole lot of stuff. But really fundamentally, that's not so the reputational risk is not the issue in itself. The issue besides the fact that we haven't managed other risks, well, that's more of an outcome. So I think trying to unpack some of that is also really useful in this strategies that we can use to do that.

For those of you who are familiar, there is the risk management process there. That's really spelled out in the risk management standard. And I guess the risk assessment component there that you can see which is in pink, is where you're trying to identify, analyse and evaluate risks. So if we're looking at how we assess and identify risks, we have to be aware of some of the biases that sometimes a lot easier to measure and predict things that are simple, but actually, there's great, much better value and much greater value in trying to unpack those more complex interconnected risks. A good example would be from a government department. We did some work with KPMG with the Via, the Victorian legal authority. And they were doing a risk register which basically said if the government changes the policy and decides to invest a whole lot more in policing. So the police department get a whole lot more money. That's great. Get more people pulled in, we'll get more cases that need to go to court. But we're not getting any potential funding increase from the government. So we need to now deal with all of this extra demand in our services. So that interconnectivity hasn't actually been considered from a policy perspective, for particular organisations within that chain. I just think it's really important to try to understand that we might even see that, you know, in the back of COVID,

and those sorts of things, the interconnection between organisations is very important, and maybe risk management becomes much broader than an internal discussion. So yeah, I just wanted to leave you with a couple of things. Risk is more than compliance. A lot of people think that it's a compliance function, but it's absolutely a part of strategy development and performance. Risk management oversight can help prioritise your strategic objectives. Your role as a director in the risk context is not to be an expert. Your role is to ask questions and to bring challenge to the framework. My biggest advice would be to be curious and sceptical and don't accept everything that's put in front of you, particularly if it's all rosy from a risk perspective.