DECISIONFOCUS

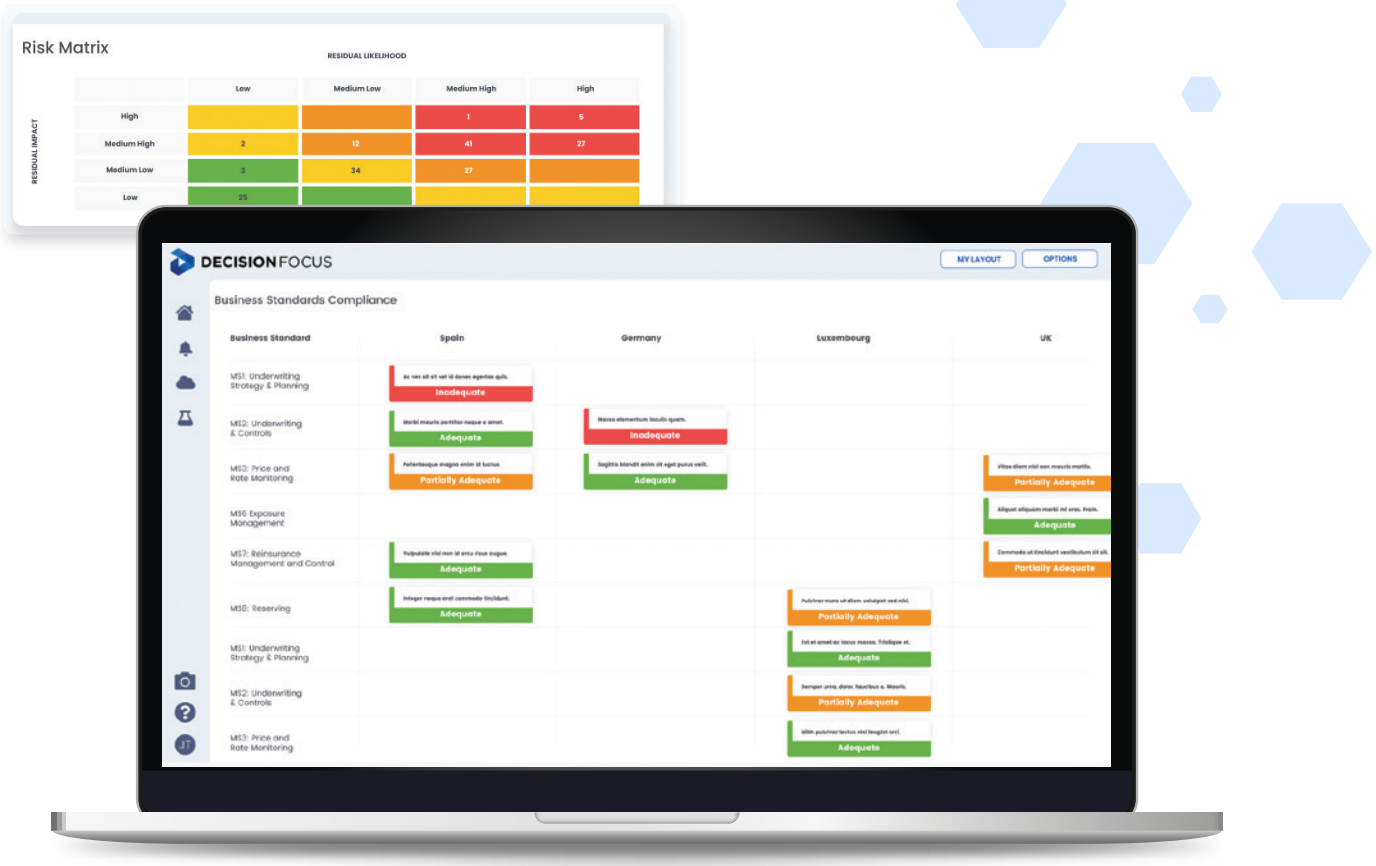
Building a Good Risk Culture – a CRO's perspective

Firstly, what do we hope to gain from the right culture? In my view we hope to improve the quality of risk thinking in the organisation, as that will lead to better decision making, and all the positives that follow. It's as simple as that.

Red is OK, really

My earliest 'deep thoughts' about risk culture arose when newly appointed to my first CRO role, 15 years ago. We were rolling out the organisation's first ever 'proper' risk framework and tool set. In a training session I was asked a question I hadn't anticipated: **if my risk goes red, will I be fired?** My answer was 'absolutely not, we need to know about your red risk so we can help you manage it down'. I added that 'what would draw criticism, is a false amber or green. It's very unhelpful, so please don't be tempted. Bring out your red'.

This conversation told me that **the openness you need for an effective risk culture may not be everyone's first instinct.** Building the trust that will permit that openness was my key task. Nothing would work without it.



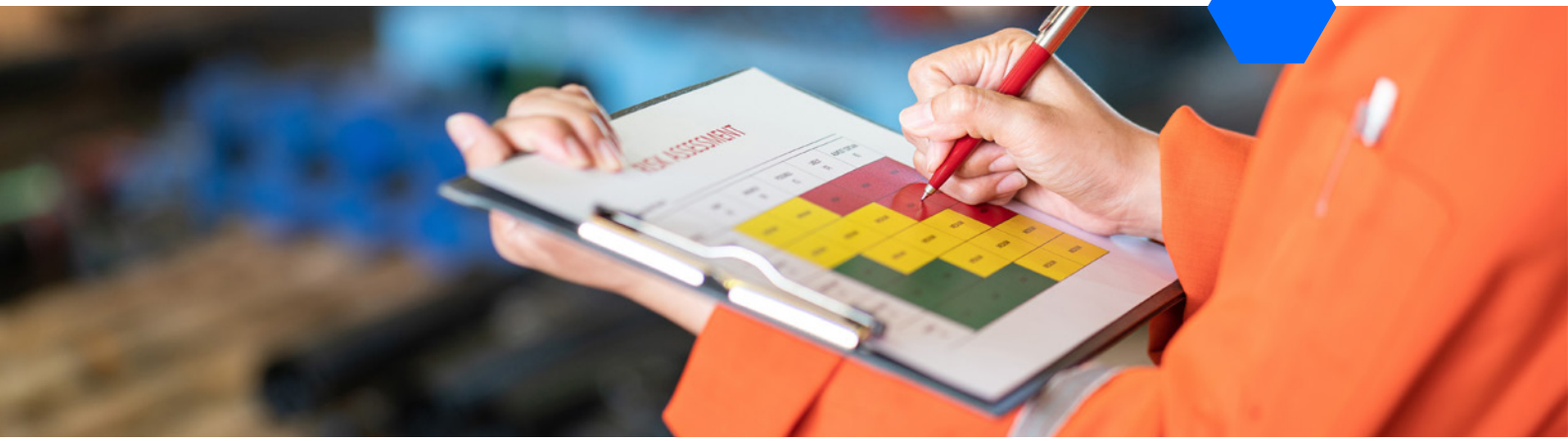
Some Attest, Others Assess

Just semantics, or does it matter? I think it does. Dictionary definitions of 'attest' include phrases like: to certify by signature or oath, to give testimony, and prove that something is true. I don't feel that requiring someone to attest encourages the openness we need. They may feel you have put their back to the wall and said 'sign here'. People are generally cautious regarding what they will attest to.

Attestation does have its place, of course. For example, in the legal requirement for SOX certification, or the corporate requirement that staff attest to having read and understood the company's Code of Conduct. But is this the right approach within your risk framework, when you are seeking an open and honest assessment of a risk's status, or a control's effectiveness? I'm for assessment, not attestation.

Even in a framework where assessment is the order of the day, some may still be reluctant to 'wash their dirty linen' under the gaze of senior management and governance machinery. I've found the best way to counter this is to be clear about what happens to their risk or control assessments once they have pressed 'submit'. If they suspect that all red risks go straight the Board's risk committee they will hesitate. If they understand there's a balanced process, their risk will only be escalated with their knowledge, and the motive is to get senior management's support, not censure, they may be more forthcoming.

We did get there, but not overnight. An early turning point was when we took operational risks raised by IT (arising from infrastructure under-investment) to the committee, and budget was approved. Opportunistic appeals from other risk owners followed. People were now queuing to have their risk discussed at committee! The key thing is that openness secures help, not censure. Gradually the openness took hold. I would bring issues from across all 11 European countries to my boss and he would ask 'how did you find that out'. I would say 'from our risk system'. The system gained an oracle-like reputation (which I did not dispel), but of course it was just the means of communication. The fact is, people became comfortable about sharing negative risk assessments.



Keeping Control, Without Stifling Thinking

A key goal for a risk framework is consistency. You need a common language for describing and assessing risks to have any hope of relative assessment, aggregation, and objective reporting. We need apples and apples, not apples and pears. The typical solution is a centrally controlled risk library. All risk owners are allocated responsibility for managing risks drawn from the library and placed in their local risk register. In the organisation that was victim to my attention as a new CRO we had claims handling hubs in 5 of our 11 European locations. Our group head of claims had a clear view of the associated risks, defined them in the library and then 'cloned' them out to the 5 hubs. The cloned risks all had the same name, description and category, but were allocated a local owner and lived a local, independent life within our assessment regime.

Some organisations stop there, taking the view that consistency has been achieved, and nothing should disturb it. But consider the claims manager in Spain. You've made them a risk owner because of their experience and ability, **you want to engender improved risk thinking in the organisation, but you've told them what their risks are. What about their view?**

We took care to configure our tool so that risk owners could declare their own risks, at will. Have we now lost control you ask, as spurious risks proliferate across Europe? No. User declared risks sat in a holding bay for the central risk team's review. Sometimes the 'risk' was just a moan or a gripe. Other times the user was on to something but needed help to better define the risk and conceive appropriate mitigation. In this case the risk may have earned its place in the library, at the risk team's discretion. Only then was it formally part of the framework and allocated via the tool back to the person who raised it, for continuous management and assessment. It might well have also been cloned to other locations and owners if appropriate.

This seemed to let us have our cake and eat it. **We retained central control, but people were able and encouraged to do their own risk thinking, and we learnt from it.**

Devolve, Democratise, Embed

Who is the right owner for a given risk? As we rolled out the organisation's new risk framework, **some would-be risk owners developed a distinct slope in the shoulders.** Again, in training, one new risk owner felt their responsibilities had been expanded and they should be compensated. I explained that 'becoming a risk owner is not an additional task to your day job. You can't succeed in your job without thinking about these risks. We are just giving you a more explicit way of reasoning about them that will help you'. And, I added: 'no, you won't get a pay rise'.

In contrast others got possessive, saying 'I'm the manager, the buck stops with me, I must own those risks'. Well yes, and no. If you manage a team of 50, in apportioning duties amongst them you are implicitly delegating responsibility for managing risk. I think it's best to explicitly devolve day to day management for many of the risks in your sphere to your team members. You can't do it all yourself. Don't go too far down that ranks though; they must have sufficient experience and authority. Risk thinking, and the risk framework that facilitates it, must be embedded, as any regulator will tell you. Managing risk is not the sole province of the senior few. To embed you must delegate, with trust. Of course, you will need to retain certain key risks for your personal management attention. But where you can, delegate.

However, a risk delegated is not a bullet dodged. You can't just let go. We configured our tool to provide those 'for whom the buck stops' with real-time oversight dashboards. They could see the status of all the risks that they had delegated and tell at a glance what was 'spiking up'. They could converse directly with the risk owners via the tool to better understand the situation and lend their help to bring the risk back into the comfort zone. If that didn't work they could escalate the risk to the central risk team for further help. It's that theme again; open escalation in return for support, not censure.

Prior to my two CRO postings, which spanned more than 10 years, I spent several more years in 'big four' risk consulting. I saw organisations operating frameworks where the risk library dictated to all, managers could override their team's assessments, the risk team marked everyone's homework by signing off assessments, attestation countered openness, and risk thinking and responsibility was not adequately embedded. In my view these characteristics militate against a positive or effective risk culture. When I took up my first CRO post my goal was to avoid them.

I could go on. People tell me I do, so I'll close with a final observation. These 'deficient' cultural traits were sometimes simply the result of buying a tool that had them hard coded into its workflow. They were never the organisation's actual intent. Think about the culture you want to create when selecting tools. They can make a difference.

Needless the say, the tool I refer to in my reminiscences does not force these process constraints. It's called Decision Focus, as is the company that owns it. Workflow is entirely configurable, so you choose where to sit on the spectrum between openness and prescription. As you can tell, I opted for openness and the tool served me exceptionally well for over a decade in the CRO seat. I'm such a fan that work now with Decision Focus to further the tool's value to financial services. Our approach is quite different. Take a look.

About Decision Focus

Decision Focus delivers enterprise SaaS solutions for managing risk, assessing controls, and optimising all aspects of audit. Decision Focus is an intelligent GRC management tool, offering small and large companies and enterprises a scalable, futureproof approach to GRC – for all industries and sectors. It enables organisations to meet the increasing GRC demands - smarter and with fewer resources. As it should be.

Embedding innovation through agile GRC

See how Decision Focus can support your business. Please get in touch to book a demo.

DECISIONFOCUS