Episode Six:

Box-tickers

FINDING MEANING IN COMPLIANCE

POWERED BY:

Databarracks

B C P

Continuity compliance is not a script

Whilst it was generally agreed among the contributing experts that true resilience came down to actions rather than words, most still saw value in the concept of compliance, at least in terms of its ability to capture and enshrine best practices into replicable standards.

That's not to say continuity standards are especially accessible. Standards like ISO 22031 are a common stumbling block for small and medium sized organisations, for whom business continuity and disaster recovery planning are often peripheral activities. The processes seem like overkill; the documentation weighty and impenetrable – designed for organisations with a greater volume and variety of challenges than is typically found at the smaller end of the scale.

Before we get to the question of how suitable international standards are for smaller organisations though, it's worth asking the question – what are they actually for?

They're not, as Mel Gosling (amongst other contributors) was keen to point out, a step-by-step guide to achieve a pre-defined standard of continuity. As he explained, it's quite possible to be compliant with an ISO standard without achieving any real level of resilience.

> **"You can implement something like the ISO standards and not be able to recover a thing."**

"Like any management standard, it describes a set of processes, not a concrete outcome. That is to say, it outlines the journey without describing the destination.

"The JPEG standard is a good analogy: it specifies what a JPEG file looks like on a technical level, but not what the image represents, or how to produce it. In the same way, management system standards don't describe the outcome, but they do describe processes.

"To use another example, say you've got a standard for a screw or a nail or something. It tells you its material and dimensions, but not how you actually manufacture it. The ISO standards for all things like quality management and IT security tend to be very long on how you do something and what you do, without attempting to describe, in this case, a singularly applicable definition of IT security.

"What it means is, you can follow the standards, you can be compliant, and you can have useless business continuity, because the proof will only be when something happens, won't it?"

Compliance should not define scope

This is where a lot of box-ticking organisations fall down. The value in certification with standards is not in the piece of paper you get at the end, but in the processes involved. To put it another way, mindlessly passing an annual audit of ISO 22301 means you're good at getting audited, not that the organisation is inherently resilient.

For Vicki Gavin at the Economist, the reverse is true. Whilst she's not legally obliged to comply with any continuity regulations, she's arrived at many of the requirements on her own terms, as a by-product of the good continuity practices she's put in place.

Importantly, her continuity planning was never dictated by compliance requirements, but rather stayed closely anchored to the specific needs of The Economist.

"Many institutions plan upside down – they start with compliance, and think 'Let's get that tick in the box'."

"As far as I'm concerned, the scope for continuity planning should never be determined by compliance requirements. Compliance is simply a by-product of doing your job right.

“One of the things that attracted me to working at The Economist is that when I joined there were no regulatory requirements to be met – they choose to do business continuity because it’s the right way to run a business.

“And because I didn’t have regulators or the board breathing down my neck, it forced me to really think about the purpose of business continuity, and be sensible about it, rather than just saying ‘Well, we have to because the regulators say so’.

“I think whether you’re working in a regulated environment or not, being able to explain your business continuity program in terms of the benefits to the business is the best way forward. When you’re doing things in the best interests to the business, compliance almost happens almost automatically.

“The main thing to remember is that the regulators don’t require anything that isn’t sensible.”

“More often than not they simply state that you must have a plan in place to control your risks, and then it’s up to you to define how you do that. The regulations rarely say ‘Your business continuity plan has to be 3 pages long, it has to have this and this and that in it’. That’s why so many people who use compliance as a tick-box exercise end up in trouble, because you can have a piece of paper that says ‘Business Continuity Plans’ on top, with a list of names phone numbers, and you’ve met the requirements. Is it actually going to help you recover? Probably not.”

The trick with standards

John Robinson of Inoni furthered this understanding of compliance frameworks as retroactive reference materials. For him, compliance frameworks aren't a set of instructions to be consulted before planning, but rather a checking framework to drop over existing plans and measure any gaps.

"The trick with a standard is to use it as an audit mechanism, where you come along after someone's created plans and drop the standard over the top, to see which bits aren't covered.

"That might tell you what you've missed, but it doesn't tell you how to build it in the first place. You can infer from it how you should have built things initially, but I'd advise against using the standard as any kind of design.

> **"The international standards have to fit everyone organisation on the planet, that's what they're for."**

"And that's why they can't be specific in design."

In the long history of standards and compliance, business continuity is a relatively recent invention. In the UK, there have been two major standards that have attempted to capture best continuity practices: British Standard 25999, and the international standard that eventually replaced it, ISO 22301.

ISO 22301 is effective, as John mentioned, because it captures a universally replicable structure within which to create and maintain personalised continuity plans.

Compliance drivers

Some organisations are obligated to meet regulatory standards of compliance. Others, as Vicki Gavin of The Economist outlined, may subscribe to continuity compliance standards voluntarily, as a matter of good practice.

John Robinson went on to describe some other scenarios in which organisations might meet regulatory standards – both voluntarily and as an obligation.

"Some possible driving forces behind compliance with 22301 are: the regulator absolutely demands it – i.e., you cannot trade without it, and you must be able to demonstrate it.

"For instance, it has its own section in the FCA handbook, and it is absolutely explicit in what you must do.

"Another scenario is that counter parties – i.e. anyone you might deal with – will not do business with you unless they know you'll be around for the long term, and therefore 22301 acts as a kind of statement of longevity.

"Insurers are also increasingly pushing people down the compliance route, because in their eyes, if you aren't aligned with things like 22301, you aren't exercising the preferred level of governance often expected by senior stakeholders.

"More generally, it's a perception issue. Compliance with regulatory standards associates you with mature, top-tier organisations, particularly in legal and financial industries. It's a shorthand; series of stamps to put across your letterhead that effectively saves time in bidding for business with customers who value that kind of thing. For others, it's not that it's a preferred quality, but rather that it will disqualify you from a tender if you don't have it."

Certificating business functions

Assessing potential suppliers based on the stamps at the top of their letterhead might not be the best move, particularly when it comes to continuity standards. Paul Butcher from Fujitsu was keen to emphasise that organisations commonly apply business continuity to individual business functions on a discretionary basis, based on their operational criticality.

What that means is that just because a potential supplier has an ISO 22301 badge, it doesn't mean their entire organisation operates within that continuity model.

"The downside of standards like BS25999 and ISO 22301 is that organisations compartmentalise their functions and certificate only certain parts of the business. For instance, say an organisation like Sainsbury's might use a logistics company to ferry its goods around the country. They'd probably insist on a logistics company certified to 22301, amongst other things. This not only doesn't make Sainsbury's compliant with 22301, there's no guarantee that the logistics provider is compliant with 22301 beyond their haulage capability. The rest of the organisation could be running on a skeleton staff."

Exceeding the standards

It's one thing to fulfil compliance requirements on paper, but actually proving it during an audit is where many organisations start to sweat. There's a reputation in many organisations that being audited is always a painful experience – that you're being scrutinized by the big bad regulator who's waiting for you to make a mistake.

For the most part, this isn't true. Regulators aren't trying to trip you up, they're simply checking against a framework.

Even where regulators are assessing liability after an incident, their goal is not to meticulously scour a checklist of compliance metrics and try to catch you out. Everyone has incidents. What matters is that you demonstrably took continuity and resilience seriously prior to the disruption, and put robust mechanisms in place to anticipate and mitigate against risks.

Stewart Duguid spoke about the way this anxiety can drive senior stakeholders to over exert themselves.

> **"There's a self-driving fear of the regulator within many industries."**

"I've spoken to more than a few banking CEOs about their interpretations of what regulators require, and they're often much tighter than what is actually stipulated. I think information is getting filtered out, from requirements on the ground to perceived standards at the top, and it means many executives are driving a harder standard than is required."

Compliance as a path to investment

This fear of the regulator during audits was a particularly common response among senior stakeholders according the interviewees.

Fear can be healthy, so long as it's used productively, and continuity standards like ISO 22301 have in-built mechanisms that explicitly require the approval of senior business owners. This presents an interesting opportunity for continuity professionals struggling to secure the attention or investment required for good continuity, as it effectively mandates visibility.

As Stewart Duguid points out, this can be useful not only to ensure that the plans actually reflect what the business needs, but to loosen up tight budgets by forcibly directing the attention of the business to potential gaps in the plan.

> **"Standards can force you to double check that what you've done is suitable..."**

"...for the company by mandating a review at senior management levels. There's a specific requirement that senior executives must approve of the scope of planning, the risk assessment and the outcomes, failures and suggested actions following testing. Once senior management are actively engaged in the process, it becomes easier to reprioritise activities in favour of continuity, and provide funding where there was none previously available."

www.thebcpcast.com