

RAISING STANDARDS

Chris Newton-Smith *reveals why security certification should be a milestone, not a goal*

Security certifications serve several purposes. They help organisations demonstrate maturity, streamline regulatory compliance efforts and even open up new market opportunities. But the value of standards like ISO 27001 and ISO 27701 can only be realised if businesses approach them in the right way. Too often, all the effort goes into achieving compliance. But this should never be a 'one-and-done' effort.

Organisations must think harder about what happens next. That means continuous governance, monitoring and human oversight to build and maintain resilience even as circumstances change. As they inevitably will.

In this context, certification is a moment to celebrate a milestone on the journey to resilience. But it's not the finishing line, because the journey doesn't have one.

It should be clear to security professionals why best practice standards and frameworks like ISO 27001, SOC2 and NIST CSF are good for business. They are designed to help organisations improve cyber preparedness and resilience at a time when the threat landscape is evolving and attack surfaces are expanding at speed. Both trends can be traced in part to AI.

Government figures suggest most medium (65 percent) and large (69 percent) businesses experienced a cyber breach or attack in the past 12 months.

Cautionary tales like Marks & Spencer remind us of the potentially huge corporate impact a major incident can have

And many are neglecting best practices like supply chain risk management, incident response, security awareness training and boardroom oversight of cyber.

In these terms, a formalised and structured way to manage cyber risk is what many organisations need not just to satisfy regulators, but also to minimise the financial and reputational risk attached to serious incidents. Recent cautionary tales like Marks & Spencer and Jaguar Land Rover (JLR) remind boards of the potentially huge corporate impact a major incident can have. For critical infrastructure (CNI) providers, the government has signalled time and again it is increasing both scrutiny and expectations of best practice.

Yet certification to a standard like ISO 27001 offers benefits that extend well beyond compliance. It can help organisations comply more easily with the various industry and international (ie EU) regulations that apply to their business. And it can help to attract new customers in new markets, as well as potentially lower insurance premiums.

All of which explains the growing interest in certification. IO data reveals that over two-fifths (43 percent) of organisations now require their suppliers to have Cyber Essentials, while a third (34 percent) say the same about ISO 27001 and over a quarter (28 percent) expect ISO 42001, which governs secure AI.

But our latest research reveals a more worrying trend: 21 percent of senior security managers told us that third-party certifications quickly become outdated post audit. A small number (5 percent) even claim that certificates reflect documented compliance more than day-to-day operational reality. Could it be that organisations are rushing to attain certification without thinking about what happens next? Less than a third (31 percent) cite continuous monitoring of controls as the best indicator of an organisation's security compliance resilience.

Not only does a race for certification lead to gaps in security posture. Ignoring post-audit cybersecurity will also erode long-term resilience. That's why standards like ISO 27001 are explicitly designed for continuous improvement cycles. Organisations must treat governance and oversight as an ongoing process that evolves as threats, infrastructure and regulations change over time.

The past few years has shown just how fast things do change in cybersecurity. In 2020, no one was talking about the AI attack surface, LLM-powered phishing campaigns and frontier models collapsing the exploit window. Today, "securing emerging technologies" like AI is one of the top challenges facing UK and US organisations, cited by two-fifths (39 percent) of those we polled. A quarter have experienced AI data poisoning over the past year while a fifth claim to have suffered attacks using deepfake clones. Some 38 percent are concerned about AI-powered phishing over the coming year. The truth is that point-in-time compliance is no longer fit for purpose in this new age. It encourages reactive security rather than proactive resilience.

More suppliers, more endpoints and more AI mean more risk. It's trends like these that continuous compliance is designed to help organisations manage. But it's not just about the threat landscape. Regulators may move slowly, but they do get there in the end. The burden continues to grow for GRC teams. But by building compliance programmes that support multiple frameworks and evolve over time, new requirements can be more easily absorbed without exerting undue stress on the organisation.

So, what should GRC teams be aiming for in order to achieve ongoing governance and monitoring? The honest answer is that best practice looks less like a set of tools and more like a set of habits. The organisations doing this well have stopped treating governance as something that gets activated before an audit and de-prioritised after it. Controls are reviewed on a rolling basis, not assembled under pressure. Evidence is generated as a byproduct of how the business operates, not produced on demand for inspection.

REGULATORY MANDATES REPRESENT THE FLOOR, NOT THE CEILING, FOR CYBER RESILIENCE

In practical terms, this means three things running in parallel. Active monitoring of the controls that matter most. A regular cadence of review that catches drift before it becomes a gap. And human oversight applied at the points where automated tools reach their limits. The latter is particularly important. Human expertise helps by interpreting what a finding means in context, assessing whether a control is genuinely working or just technically documented and making judgement calls that no platform can make responsibly. The bottom line: this is not about technology. It is about design. Technology is an enabler, but the discipline is what makes it real.

Organisations keen to turn this theory into reality should start with prioritisation. Not every control needs the same level of attention. Monitor the most business-critical assets and highest-consequence risks most actively. Define what good looks like for each, set the metrics and automate the evidence collection where possible. This will free up human experts for when they're really needed.

Next, build the review cadence into the business rhythm rather than treating it as a separate compliance activity. A monthly review of access controls sits naturally alongside an HR process. A quarterly supplier review can run alongside contract management. When governance is embedded in how the business already runs, it stops feeling like an overhead.

Third, assign clear ownership. The single most common reason ongoing governance falls apart is that nobody is responsible for it between audit cycles. Named accountability at all levels, including senior leadership, is what keeps it real. Finally, test the plan. Incident response processes that have never been exercised are of little value. Running a tabletop scenario once a year costs very little and surfaces gaps that no automated tool will find.

We found that nearly half (45 percent) of UK security leaders believe human expertise is essential when evaluating whether suggested automated

compliance processes and actions are relevant or accurate. A third say it's required to interpret complex regulations, and a similar percentage agree that it can challenge the credibility or completeness of automated compliance evidence. They're right on all counts.

THE PAST FEW YEARS HAS DEMONSTRATED JUST HOW FAST THINGS CAN CHANGE IN CYBERSECURITY

Consider a business that acquires a smaller competitor with ISO 27001 certification. After acquisition, the combined entity is running new systems and has new supplier relationships that the original control set wasn't designed for. Automated tools will show the controls as documented, but not that they no longer reflect the actual risk environment.

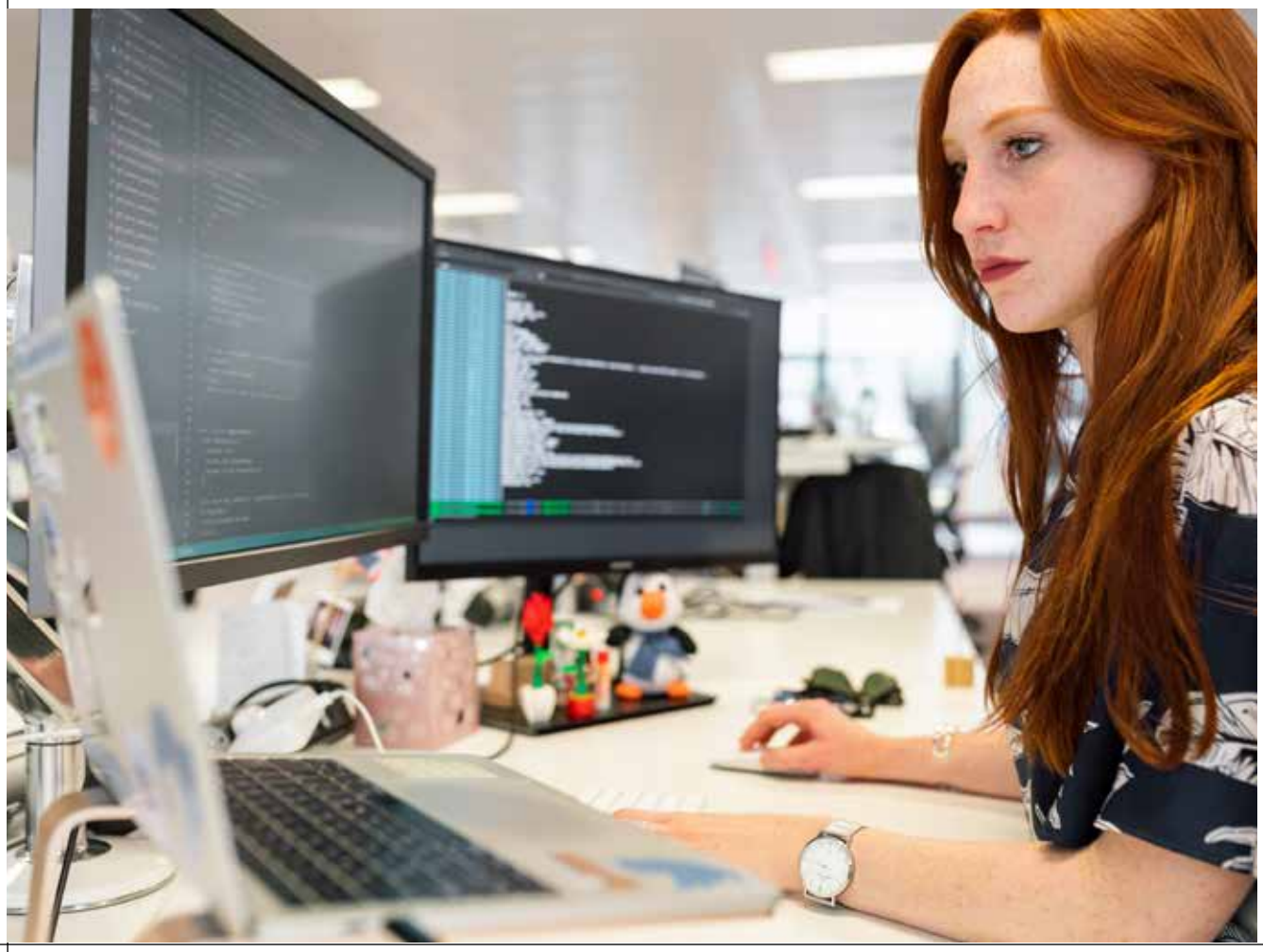
In another example, a company subject to NIS2 needs to work out whether its existing ISO 27001 controls satisfy the regulation's requirements. This is no easy feat, especially given that NIS2 obligations vary by sector and entity type. Automation can highlight where existing controls map to NIS2 articles and where gaps exist. But it can't determine what is proportionate for a given organisation operating in a given sector under the supervision of a specific national competent authority. In both cases, automation is part of the answer, it moves faster, covers more ground, and removes the most routine work. But it is not the whole answer. Humans sit above the technology, validate what it produces and make the calls that no automated system can make responsibly.

There's no time like the present to start these efforts. The Cyber Security and Resilience Bill will soon become law, enacting some of the most significant updates to UK cyber legislation since the NIS Regulations of 2018. It won't apply to all businesses, but there are lessons for every organisation.

For organisations already holding ISO 27001 or ISO 27701, the foundations are strong. These standards provide many of the governance structures, risk management disciplines and documented controls the bill is expected to require. Active governance will be particularly useful in helping organisations meet the requirements around incident reporting, supply chain risk management and board accountability.

But it's important to bear one last thing in mind. Both regulatory mandates and industry standards represent the floor, not the ceiling, for cyber resilience. The only way to keep customers, regulators and boards happy is with a relentless focus on ongoing monitoring and improvement. Embed it into the fabric of business processes and it starts to become culture. That's when you know you're on the right path. And the organisation is ready for anything that comes its way ●

Chris Newton-Smith
is CEO at IO.



Human expertise helps by interpreting what a finding means in context