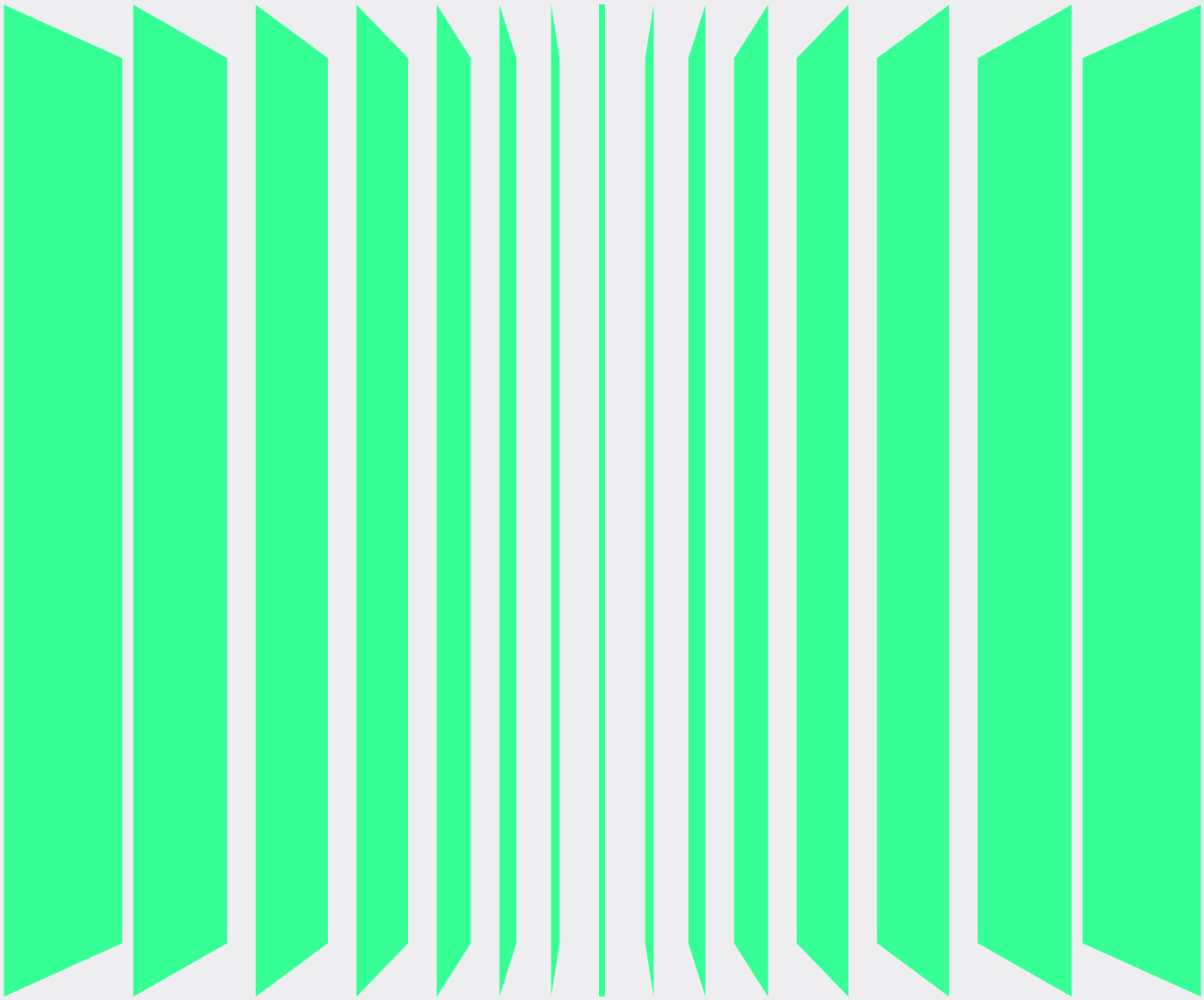


The compliance confidence gap

Certification, automation and regulatory readiness: what 251 senior UK cybersecurity professionals say

Public V1.0

Executive Summary

Four findings. One direction of travel.

The data suggests practitioners increasingly associate confidence with observable, ongoing governance rather than periodic attestation alone.

The challenge is no longer about achieving compliance. It's about sustaining it.

This report presents findings from independent research conducted among 251 UK cybersecurity managers, directors and executives in April 2026. The research examines how senior practitioners view third-party certification, where they see the limits of automated compliance, what they consider the strongest indicators of genuine resilience, and how they assess their organisations' readiness for upcoming regulatory change.

Four significant tensions emerge from the data. Each point to the same underlying shift: the questions that matter in compliance are no longer solely about achieving certification, but about sustaining the governance capability it is designed to represent.

1. Confidence does not equal scalability

99% of respondents describe their organisation as prepared for upcoming regulatory requirements. Yet only 35% believe their compliance model could absorb new requirements without significant adjustment. The gap between those two figures reflects a distinction practitioners draw between current readiness and structural adaptability.

2. Certification is valued, and implementation is scrutinised

97% of respondents view certification positively. 87% say the speed at which certification is achieved affects its credibility. These findings are consistent. They indicate that practitioners regard the standards themselves as sound and have become more attentive to the rigour of the implementation process behind the certificate.

3. Automation is valued, within defined boundaries

Respondents consistently identified human expertise as essential at the points where judgement carries the highest stakes: assessing whether automated outputs are relevant and accurate, interpreting complex regulatory requirements, and challenging the quality of automated evidence. The data does not indicate resistance to automation. It identifies where automation alone is considered insufficient.

4. Resilience is assessed operationally

Asked what best indicates genuine compliance resilience, respondents ranked continuous monitoring, executive accountability and independent oversight ahead of point-in-time assessment.
The data suggests practitioners increasingly associate confidence with observable, ongoing governance rather than periodic attestation alone.

The challenge is no longer about achieving compliance. It is about sustaining it.

01

The confidence paradox

Why organisations feel prepared today but uncertain about tomorrow

Asked about preparedness for upcoming regulatory requirements, 99% of respondents described their organisation as prepared to some degree. Asked whether their current compliance model could scale to meet those requirements without significant adjustment, only 35% said it could. Half said their model would need at least some changes. A further group anticipated substantial ones.

These figures are not contradictory. They measure different things. Preparedness, as most organisations experience it, describes the present: frameworks are in place, certifications are up to date, and the last audit was completed. Scalability describes the capacity for change, what happens when the next regulation arrives, and whether it can be absorbed into an existing system or requires a new programme built from scratch.

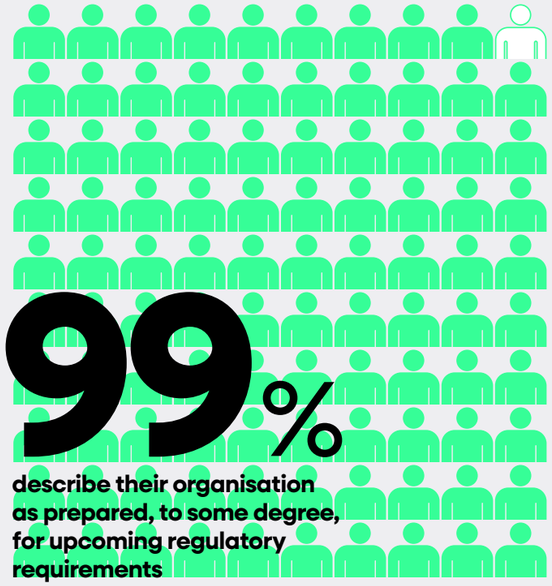
The gap is best read as the distance between those two definitions. Organisations have become effective at meeting the compliance requirements they face. Fewer have built the structural capacity to absorb requirements that have yet to arrive.

Organisations have become effective at meeting the compliance requirements they face. Fewer have built the structural capacity to absorb requirements that have yet to arrive.

Three factors are compressing that gap. Regulatory scope is expanding: the compliance perimeter now spans information security, data privacy and AI governance, with NIS2, DORA and the EU AI Act operating on overlapping timelines. Regulatory convergence is increasing: the same underlying controls appear across multiple frameworks, which rewards organisations able to map once and reuse evidence, and creates duplication costs for those treating each framework as a standalone project. And governance complexity is rising: more systems, more suppliers, more data flows, all changing faster than annual assessment cycles were designed to track.

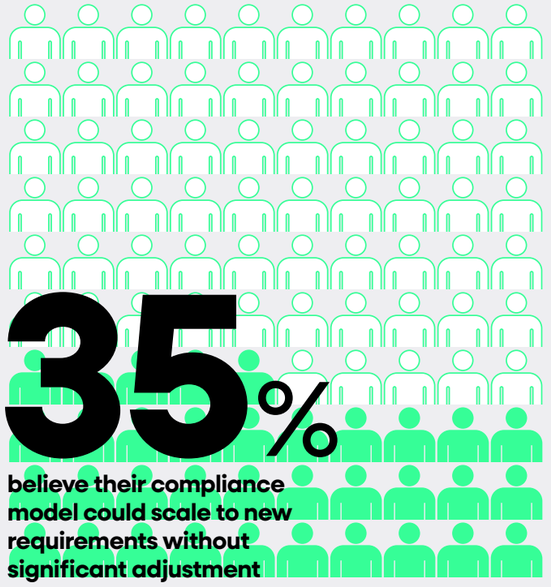
The central finding of this chapter: the gap between ‘prepared’ and ‘scalable’ is the clearest single measure of how much compliance adaptability now matters.

When you consider upcoming regulatory requirements (e.g. expanding cyber and data regulations), how prepared is your company’s current compliance model to adapt to these requirements?



99%

describe their organisation as prepared, to some degree, for upcoming regulatory requirements



35%

believe their compliance model could scale to new requirements without significant adjustment

The gap between ‘prepared’ and ‘scalable’ is the clearest single measure of how much compliance adaptability now matters.

02

Why speed influences trust

The changing relationship between certification credibility and implementation

Over 87% of respondents say the speed at which certification is achieved influences its credibility. In a field where certifications function as a common signal of security governance maturity, that level of consensus is significant and merits careful reading.

The first point the data makes clear is what this finding does not represent. It is not a loss of confidence in certification. 97% of the same respondents view certification positively, a near-total endorsement of the standards themselves and of what they represent. Certification remains the established mechanism for independent, standardised verification of security governance, and the data reflects that status.

What has changed is the level of scrutiny applied to the process by which a certification was achieved. Practitioners understand, from direct experience, what the relevant standards require. A management system in the ISO 27001 sense is not a document set. It is an operating capability: risks identified and treated, controls embedded in how work is actually done, a cycle of review and improvement that continues after the assessment. Practitioners can broadly estimate what it takes to build that capability.

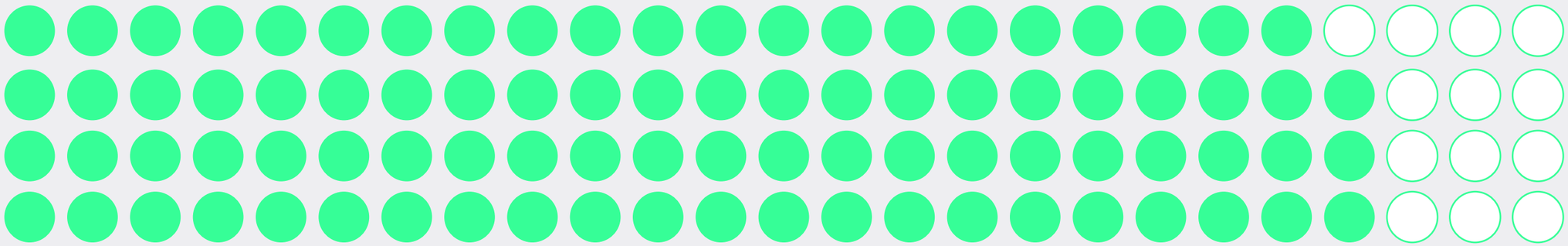
Certification remains the established mechanism for verification of security governance, and the data reflects that status. What has changed is the level of scrutiny applied to the process by which a certification was achieved.

When a certification is achieved at a pace that implies the underlying capability could not have been fully established, the inference many draw is that the documentation was assembled rather than the management system built.

The practical implication runs in both directions. A certification earned through rigorous implementation carries increasing weight among discerning counterparties, procurement teams, enterprise customers, and regulators, who are asking follow-up questions about how controls are maintained between audits. A certification acquired primarily as an artefact, through a compressed or heavily automated process that did not allow the management system to be genuinely established, provides less assurance than its holders may assume.

The standards themselves are not in question. What practitioners are assessing more carefully is the implementation process behind the certificate, and whether it was sufficient to establish the governance capability that the standard is designed to verify.

In your view, does the speed at which a third-party certification, such as ISO 27001, is achieved affect its credibility?



87%

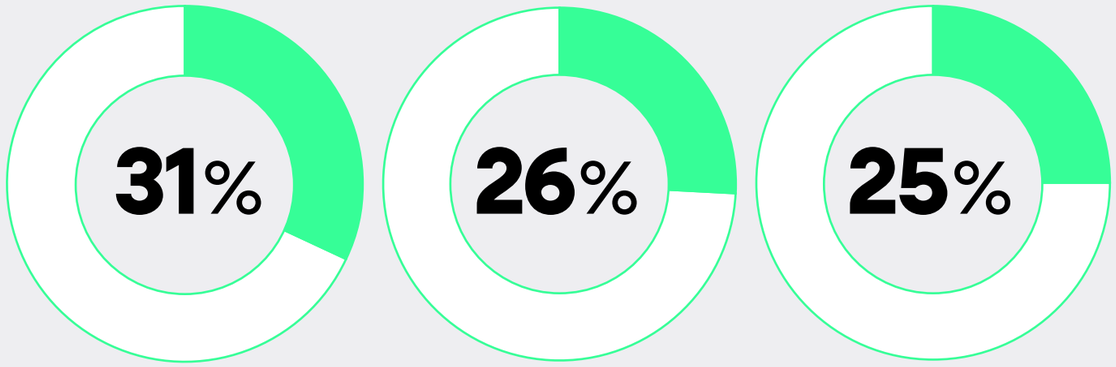
say the speed at which certification is achieved influences its credibility

03

What security leaders actually trust

The indicators practitioners associate with genuine compliance resilience

Which main actions or processes give an accurate picture of an organisation's security compliance resilience?



Continuous monitoring of controls

Clear executive accountability for compliance

Experienced human oversight from auditors

This study asked respondents to identify what they consider the strongest indicators that an organisation's compliance genuinely reflects operational resilience. The responses reveal a clear preference for ongoing, observable governance over point-in-time assessment.

31% continuous monitoring of controls

26% clear executive accountability for security outcomes

25% independent auditor oversight

24% automated and verifiable evidence collection

The most-cited indicator, continuous monitoring, describes an activity rather than an artefact. The second, executive accountability, describes a standing organisational arrangement. Independent auditor oversight, ranked third, reflects the continued value practitioners place on external, standardised verification. Automated evidence collection, fourth, serves as the infrastructure that enables the other three to operate at scale.

Read together, these choices reflect a coherent view of what assurance should rest on. Respondents were not designing an assurance model, but the data describes one: confidence grounded in continuous operation, visible ownership, independent verification and efficient evidencing, rather than in the fact of an assessment on a given date.

Practitioners increasingly look for evidence of what sits between the assessments, the controls that should still be operating, and the governance that should still be running, on every day that is not audit day.

This does not diminish the role of certification. Independent, standardised verification remains the anchor: no amount of internal monitoring substitutes for it, and respondents continued weighting of auditor oversight confirms that. What the data indicates is that practitioners increasingly look for evidence of what sits between the assessments, the controls that should still be operating, and the governance that should still be running, on every day that is not audit day.

Continuous monitoring ranks first because it provides that evidence. Executive accountability ranks second because it indicates that what is reported is also owned. The pattern across all four leading indicators is consistent: assurance is increasingly associated with ongoing operational behaviour rather than documents of compliance.

Practitioners associate genuine compliance resilience with continuous, observable governance, not with the frequency or speed of certification.

Practitioners associate genuine compliance resilience with continuous, observable governance, not with the frequency or speed of certification.

04

The limits of automation

Where human judgement remains essential to compliance integrity

Where do you believe human expertise is still most important to ensure the integrity of information security compliance processes?

Compliance automation is one of the fastest-growing areas of security tooling. Evidence collection, control mapping and monitoring at current scale are not feasible manually. This study did not find a profession resisting that development. It found one defining the boundary between what automation handles well and the judgements it cannot make.

Asked where human expertise remains most essential in an increasingly automated compliance process, respondents identified three consistent points:

44% evaluating whether automated outputs and recommendations are relevant and accurate

33% interpreting how complex regulatory requirements apply to their specific organisation

32% challenging the quality and completeness of automated compliance evidence

Each of these is a judgement about meaning rather than a task of collection. Whether an automated output is relevant depends on context the tool does not hold: how this organisation actually operates, where its data flows, and which third-party dependencies exist. Whether a regulation applies, and how, requires interpretation against a specific business and its operating environment. Whether a body of evidence is complete can only be assessed by someone who understands what should be present, not only what the system found.

The data does not frame automation and human expertise as competing approaches. Respondents appear to assign them different functions: Automation handles volume, human expertise handles the substantive questions.

The data does not frame automation and human expertise as competing approaches.

Respondents appear to assign them different functions. Automation handles volume: gathering evidence continuously, mapping controls across frameworks, flagging exceptions. Human expertise handles the substantive questions: is this evidence meaningful, is this interpretation correct, is this picture of compliance complete? Each depends on the other.

The specific finding that 44% of respondents identify validating automated outputs as the most critical use of human expertise carries a particular implication. A compliance programme that has reduced or removed human oversight at the point where automated outputs are assessed has removed the check on whether the automation is producing accurate and relevant results. The evidence it generates is then untested against operational reality.

Automation scales compliance evidence gathering. Human expertise validates whether that evidence is accurate, complete and meaningful. The organisations getting this right have positioned human judgement at these three points deliberately, and let automation do everything else.

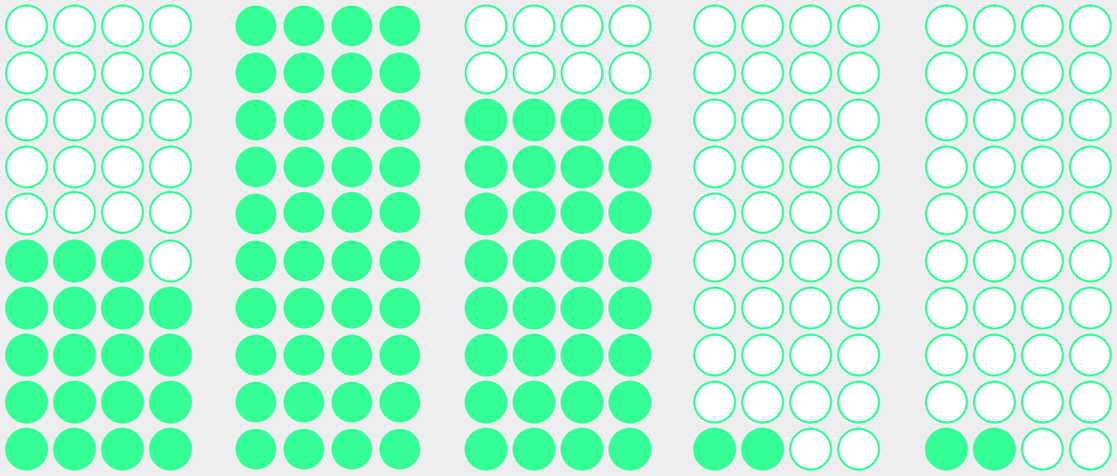
Automation scales compliance evidence gathering. Human expertise validates whether that evidence is accurate, complete and meaningful.

05

The economics of compliance at scale

From framework projects to governance architecture

To what extent do third-party certifications (e.g. SOC 2, ISO 27001) accurately reflect the real-world effectiveness of an organisation's security controls?



Completely accurately reflects | **Mostly accurately reflects** | **Somewhat accurately reflects** | **Partially accurately reflects** | **Does not accurately reflect**

The preceding chapters describe how practitioners assess compliance credibility, resilience and automation. This chapter examines what those findings mean for how compliance is structured and resourced, because the way most organisations currently operate compliance carries costs that the data suggests are becoming difficult to sustain.

Consider the compliance landscape a typical mid-sized organisation now navigates. Regulatory obligations: NIS2, DORA, GDPR and the EU AI Act set legal requirements. Frameworks such as ISO 27001, ISO 27701 and ISO 42001 provide the structured means to meet and evidence them. Across both, the same access management, risk assessment, and incident response requirements appear in different languages within multiple regulations and frameworks. These are not unrelated demands. Each is an expression of the same underlying expectation: know your risks, control them, document them, and keep them current.

The dominant operating pattern, however, treats each framework as a separate project: its own documentation, evidence collection, policies, tooling and, often, its own external advisers. The costs of that pattern compound incrementally. Evidence for the same control is assembled multiple times in different formats for different audits. Risk registers for security and privacy operate in parallel, describing the same systems, but cannot be reconciled. Cross-cutting risks that span multiple frameworks sit in the gaps between programmes. And, as Chapter 1 establishes, each new framework built as a standalone project means the next one arrives as a standalone project too, which is precisely why only 35% of organisations believe they could absorb new requirements without significant adjustment.

These are not unrelated demands. Each is an expression of the same underlying expectation: know your risks, control them, document them, and keep them current.

The alternative pattern, common controls, shared evidence, a single risk and governance architecture mapped to multiple frameworks, changes those economics. New regulatory requirements arrive as incremental obligations against an existing system rather than as new programmes. The marginal cost of each additional framework declines as the architecture absorbs it. The duplication costs that accumulate under the project model are largely eliminated.

In the project model, compliance investment produces a certificate and stops there. In the architecture model, the certificate is the foundation, and the governance capability built around it is what compounds over time.

In the project model, compliance investment produces a certificate and stops there.

In the architecture model, the certificate is the foundation, and the governance capability built around it is what compounds over time.

06

What the data says about maturity

Respondents who express the highest confidence in their organisation's adaptability consistently describe their approach differently from those who are least confident.

Five observable signals that distinguish compliance approaches

Read as a whole, the findings in this research describe a spectrum of compliance maturity. Respondents who express the highest confidence in their organisation's adaptability consistently describe their approach differently from those who are least confident. Five signals emerge from the data as consistent differentiators.

What triggers compliance activity

At one end of the spectrum, compliance activity is triggered externally, such as a customer questionnaire, a regulatory deadline, or an approaching audit, and evidence is assembled each time. At the other end, compliance activity is the continuous operation of a management system, and evidence accumulates as a by-product of how the organisation works. Chapter 3's data shows that practitioners associate confidence with the second condition.

What happens between audits

Some organisations demobilise after certification and remobilise before the next assessment; the compliance picture is accurate at two points in the year. Others monitor continuously and address drift as it occurs; the picture is accurate by default. The 87% finding in Chapter 2 reflects practitioners' ability to distinguish these two conditions when evaluating certifications from outside.

How many systems describe one risk

Where information security, privacy and AI obligations are governed as separate programmes, a risk that spans all three; an AI system processing personal data, for example, may be identified by multiple teams or by none. Where programmes share an architecture, that risk is visible and owned in one place. The economic argument in Chapter 5 follows directly from which of these conditions applies.

Where judgement sits

Chapter 4 identifies three areas where human expertise is considered non-negotiable: validating automated outputs, interpreting regulatory requirements, and challenging the quality of evidence. Organisations with named individuals accountable at these points produce compliance evidence that is tested against operational reality. Organisations that have removed human oversight at these points do not.

What a new regulation costs

For some organisations, a new regulatory requirement, NIS2, DORA, the EU AI Act, arrives as a new programme: new documentation, new evidence collection, new spend. For others, it arrives as a mapping exercise against an existing governance architecture. The 35% scalability figure in Chapter 1 is a direct measure of how few organisations currently sit in the second group.

Conclusion

What the findings point to

The future of compliance is continuous, evidenced and operational

The six chapters of this report address different aspects of how senior UK cybersecurity professionals think about compliance. Taken together, the findings point in a consistent direction.

Certification remains the established foundation of compliance assurance, the independent, standardised verification that organisations have implemented appropriate controls. 97% of respondents affirm that. What has changed is the scrutiny applied to the implementation behind the certificate, and the degree to which a certificate alone is treated as sufficient evidence of ongoing security posture. 87% of practitioners say the pace of certification affects its credibility. The standards are not in question; the rigour of the process behind them is.

Automation is a necessary component of compliance at the current scale. The data does not challenge that. It identifies three specific points: validating outputs, interpreting regulation, and challenging evidence, where human judgement remains essential and where removing it creates gaps between documented and operational compliance.

Business resilience, the capacity to sustain and adapt compliant operations as requirements, technologies and risks change, is becoming a strategic business capability, not solely a governance objective.

The indicators that practitioners associate with genuine compliance resilience are operational: continuous monitoring, named accountability, independent oversight, and verifiable evidence. These describe a management system that is running, not one that ran successfully at a point in time.

And the economics of compliance increasingly favour a governance architecture, common controls, shared evidence, a single system mapped to multiple frameworks, over the project model that treats each certification as a standalone exercise.

Business resilience, the capacity to sustain and adapt compliant operations as requirements, technologies and risks change, is becoming a strategic business capability, not solely a governance objective.

The organisations best positioned for the regulatory environment ahead are those whose compliance is a continuously operating management system, independently verified by certification, governed at the right level of the organisation, and evidenced in a way that holds up between assessments as well as during them.

The organisations best positioned for the regulatory environment ahead are those whose compliance is a continuously operating management system, that holds up between assessments as well as during them.

That is not a description of compliance done quickly. It is a description of compliance done properly.

That is not a description of compliance done quickly. It is a description of compliance done properly.

Research Methodology

The research was conducted by Censuswide among a sample of 251 UK cybersecurity managers and above. Data was collected between 8 and 13 April 2026. Respondents spanned junior managers through to C-level executives, including CISOs, CSOs and CROs, across organisations of varying sizes and sectors.

Censuswide is a member of the Market Research Society (MRS) and the British Polling Council (BPC), and a signatory of the Global Data Quality Pledge. All research adheres to the MRS Code of Conduct and ESOMAR principles.

About IO

IO is the business resilience platform helping organisations move beyond compliance to build information security, data privacy and AI governance that holds up in the real world.

Most compliance tools are built to help you pass an audit. IO is built for what comes after. That requires governance with the operational depth to back the certificate up; controls that are embedded, understood and actively maintained. Our platform gives organisations the structure, workflows and evidence management to run compliance properly, backed by a team that works directly with customers every day to make sure the right judgement is applied at every point where it matters. We have been doing this for over a decade.

IO brings Information Security, Data Privacy and AI Governance together in one joined-up SaaS platform, supporting over 100 global frameworks including ISO 27001, ISO 27701, ISO 42001, SOC 2, GDPR, NIS2 and DORA. Trusted by over 1,000 organisations worldwide, including ScottishPower, Siemens, Rightmove and Panasonic. Rated G2 Leader 9 quarters in a row.

IO. Setting the standard for business resilience.

Explore more at **isms.online**