Raconteur

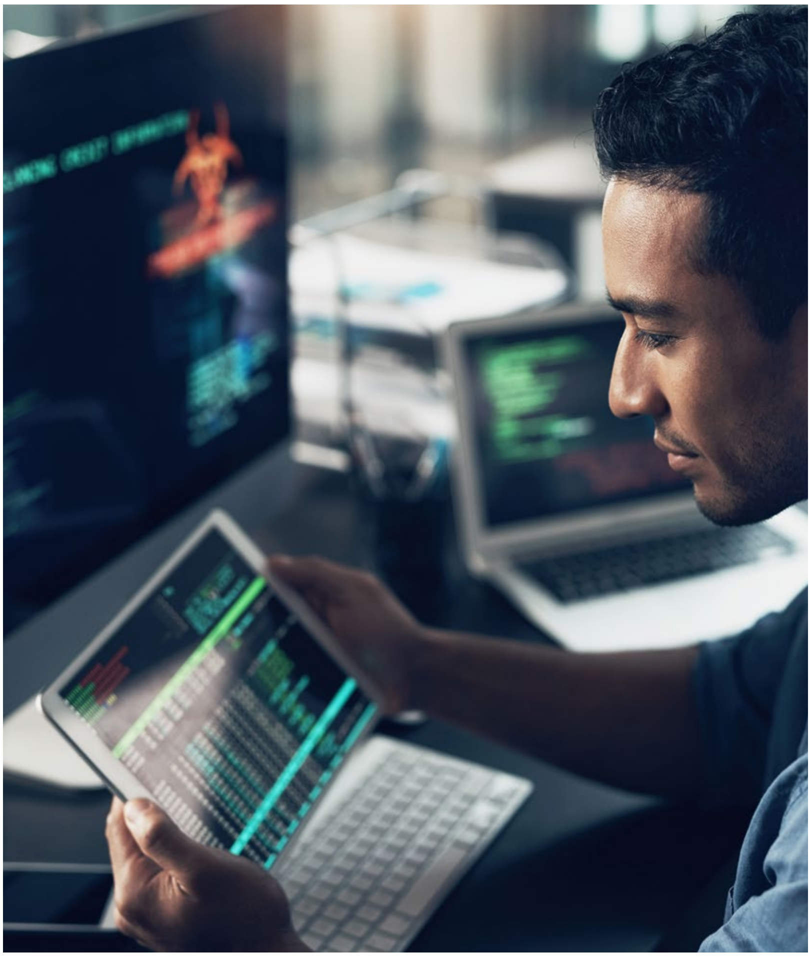
# Certified success: why leaders should master digital compliance

digicert®

# Contents

# The compliance transformation checklist: Five leadership moves to drive sustainable security excellence

As cyber regulations reshape business risk, how can leaders transform mounting security obligations into a market advantage? A five-step roadmap can help drive compliance excellence



With fresh cybersecurity regulations reshaping the global business landscape and new compliance frameworks gaining momentum, organisations face unprecedented pressure to transform their security posture from reactive defence to strategic advantage.

Leaders are grappling with a complex challenge - as cyber attacks grow more sophisticated, regulatory compliance has shifted from a back-office burden to a business-critical differentiator. The question is no longer whether to act, but how quickly businesses can adapt

Companies that proactively manage their digital security aren't just avoiding breaches and system outages – they're building resilient operations that can adapt quickly to new regulations like DORA. As digital threats increase, strong compliance has become inseparable from good business practice.

Seismic shifts in compliance requirements are around the corner. The Digital Operational Resilience Act (DORA) became law on 17 January 2025, reshaping the EU financial services sector and its ICT suppliers.

Meanwhile, the UK Cyber Security and Resilience (CS&R) Bill is set to progress through Parliament this year, aligning the UK with the EU's 2022 NIS2 Directive. Both initiatives establish clear responsibilities for executives to oversee cybersecurity risk management.

Patrick Beckman Lapré, director and digital trust specialist at DigiCert, says: "An important step in the move to security excellence is making the organisation as resilient as possible. We can't control everything, but we can be aware of how to minimise the disruption of a cyber attack to your customers, and also, to your organisation."

What global security and risk management leaders need is a structured approach to an evolving security landscape. But translating complex and overlapping requirements from various guidance into actionable strategies requires a clear roadmap and a different approach to doing digital business.

Here are the five essential steps leaders must take to transform regulatory requirements from burden to benefit while ensuring auditor-ready operations.

## 01 Understand your digital asset inventory

Getting to understand the digital asset landscape is crucial to effective cybersecurity. Leaders must understand their digital asset landscape for effective cybersecurity. The automated discovery of assets, continuous monitoring capabilities and clear visibility of third-party connections are all part of this puzzle.

"Examples of assets include PCs, servers, applications, digital certificates, firewall rules, staff or third parties. If you don't have a complete inventory of assets, then you cannot be sure that your cybersecurity controls are protecting everything they should be", Simon Lawrence, director and co-founder of cyber security and risk consultancy i-confidential, says.

"For example, if a server is missing from your Configuration Management Database (CMDB) then your vulnerability scanner will not know about it, and you may have undiscovered critical vulnerabilities," he explains.

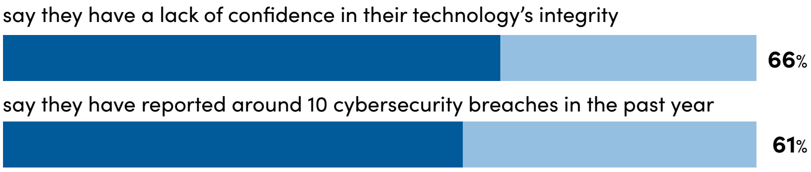
Mapping of the ICT ecosystem must include grouping assets to the information systems that use them so they can be prioritised for business criticality. This prioritisation considers the business impact if the information system is compromised – a risk to both organisational and personal reputation.

"Without a view of criticality, organisations will under-invest in controls for their most critical systems and over-invest in lower risk systems, leaving the critical systems exposed to significant cyber risks," adds Lawrence.

"This can also make operational security less effective. For example, when an organisation is under attack, incident response staff will not have the information they need to focus on the most critical systems."

**As cyber threats evolve alongside regulatory changes, businesses need robust strategies to defend themselves effectively**

Percentage of leaders expressing cybersecurity concerns



Deloitte 2024

## 02 Refine your access and permission control architecture

Access control architecture requires implementing granular permissions that precisely define what resources users can access and what actions they can perform. This can be achieved through role-based access management (RBAM), where permissions are assigned based on job functions rather than individual users, simplifying administration and reducing security risks.

Effective access control relies on strong identity verification, which leaders can achieve by using digital certificates for users, devices, and workloads. These certificates serve as trusted credentials that authenticate identities across the businesses' infrastructure.

Once an enterprise implements certificate-based identity verification, automated certificate lifecycle tracking becomes crucial to manage these digital identities from issuance through renewal and revocation. This automation ensures certificates don't expire unexpectedly and are promptly revoked when no longer needed.

The system maintains detailed audit trails of all system interactions, providing visibility into who accessed what resources and when. This is essential for security monitoring and compliance requirements.

The architecture must support dynamic updates to accommodate business changes while maintaining security integrity. This includes automated workflows for access requests, approvals and revocations, ensuring timely updates while preventing unauthorised access.

The key to success lies in continuous updating and a clear definition of team responsibilities. Without an effective process that automates tasks while accounting for the human element, access controls can become a business risk rather than a security asset.

Access control management is not a one-time action, but a process that must be monitored and controlled continuously, for example, factoring in new hires as well as people who leave the company and could take data with them.

## 03 Outline and develop clear incident frameworks

Leadership teams and security operations both play a critical role in cyber incident response.

"The efficiency and effectiveness of the initial response influence the severity of operational, reputational impact and financial losses following an attack," says Katherine Kearns, head of proactive services, EMEA at consultancy S-RM.

Mitigating these challenges requires mastering collaboration between strategic decision-makers and technical responders from the start.

She explains that regular response exercises provide an opportunity to practice critical skills and responsibilities in a consequence-free training environment and to improve cyber incident response plans based on the learnings from the exercise.

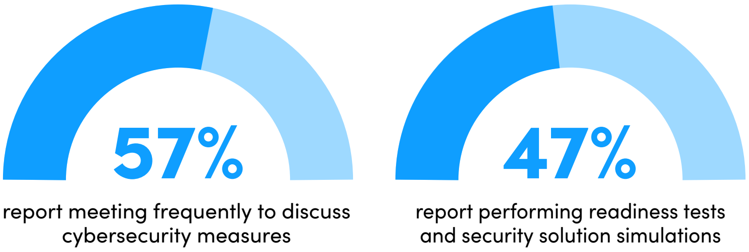
"An effective response exercise tests key capabilities including business continuity, resource management, system recovery, threat handling, communications, and regulatory compliance."

## 04 Implement automated compliance controls

Moving from manual oversight into automated assurance can ensure leaders are ready for when the auditors arrive and demonstrate to partners that your organisation is effectively managing risk at all times.

**Leaders must harness resilient security systems that stand up to scrutiny to sail through compliance audits**

Percentage of leaders citing proactive leadership engagement in cybersecurity measures



Deloitte 2024

Even more important is measuring the effectiveness of cybersecurity controls so that any gaps or weaknesses can be addressed in real time for continuously secure and compliant business operations.

While many organisations deploy security technologies, they often do little to make sure they remain effective, which can lead to successful cyber attacks breaching an organisation's defences.

"Controls are often measured using control testing. Typically, this activity will take a sample of assets and determine whether the required controls are being applied. This is usually carried out once or twice per year. While this approach will give a view of control effectiveness and compliance, it has limitations", Lawrence says.

## 05 Align your cyber strategy with global requirements

Organisations with global operations must navigate diverse and evolving cyber requirements across multiple jurisdictions. This requires a clear understanding of each region's complex reporting and regulatory obligations.

Implementing scalable frameworks, such as ISO 27001 or NIST CSF, can significantly streamline compliance activities across jurisdictions.

Assigning roles dedicated to tracking regulatory changes and emerging threats through ongoing assessments is crucial.

Because regional teams often face similar challenges, coordination across the teams is essential to avoid fragmentation or duplication in compliance efforts. ●

> "
> If you don't have a complete inventory of assets, then you cannot be sure that your cybersecurity controls are protecting everything they should be

# When one DORA opens: how leaders can harness security solutions

With manual compliance processes leaving companies exposed, business leaders must put harnessing automated security solutions high on the agenda

Commercial feature
in association with
digicert®

Despite rising digital risks, many organisations still cling to manual compliance processes instead of embracing automated security systems, leaving them exposed to costly errors, resource drain and compliance failures that threaten business continuity.

Tracking regulatory changes manually can increase the risk of non-compliance, resulting in fines, and ultimately a loss of digital trust and lasting damage to an organisation's reputation.

With the Digital Operational Resilience Act (DORA) and cybersecurity budgets expected to grow for 57% of leaders over the next 12-24 months according to Deloitte, knowing how to tackle compliance is an increasing priority on the executive agenda.

## Managing cost-effectiveness

Patrick Beckman Lapré, director and digital trust specialist at DigiCert, a global provider of enterprise PKI and certificate lifecycle management solutions explains that digital transformation can help slash manual effort and the costs that incur, allowing executives to focus on strategies which bolster competitive advantage.

"The costs associated with errors, inefficiencies and penalties can far outweigh the perceived savings of manual approaches. You are limited to reacting only at the moment – not being able to foresee what the damage will be or have any insight".

He explains that cryptographic agility - an organisation's ability to rapidly switch between different methods of data encryption and security - is imperative for businesses to maintain a competitive edge.

Cryptography protects information by converting it into secure, encoded formats. Today, businesses need to move from being reactive to being proactive, with a complete inventory of their cryptographic tools and the capability to quickly replace vulnerable solutions before they're exploited," he says.

"Leaders must have the capability to model scenarios before they happen. And if problems do occur, they need the controls and processes in place that will minimise the disruption", he says.

Security and compliance are not one-time actions, but an ongoing commitment. Automation platforms provide real-time monitoring, alerting companies to potential risks and enabling proactive responses much more quickly.

Digital certificate management systems respond rapidly to regulatory changes and updates like DORA, ensuring that nothing is missed and that organisations avoid fines and other consequences of non-compliance.

These systems automatically track and manage digital security certificates, helping leaders quickly spot and fix security issues before they cause disruption - a key requirement of DORA's new security rules.

### Top-down digital transformation

While the business case for digital compliance technology is clear, from enhanced efficiencies to more informed and quicker decision-making, success demands leadership commitment from the top.

"Many organisations see digitalisation as a purely technical thing," says Lapré. "Often, they will appoint a CISO without giving enough consideration to what cybersecurity really means. However, senior leadership and management must be involved and fully aware of what is happening."

"They make the decisions about where to spend money. When they are asked for investment in something that they don't know with any certainty when it might happen, they may be more inclined to put money into projects that they know will deliver in three months."

"Senior management needs to understand that failure to invest in digital cybersecurity compliance can impact the business very badly due to the loss of its digital trust," he adds.

### Redefining digital trust

Robust digital compliance can help deliver critical business advantages including early detection of data breaches, protection of valuable IP assets and enhanced customer trust.

Beyond safeguarding intellectual property and personal data, these measures transform security investments into customer loyalty and work to drive organisational value long-term.

> “
> A digital compliance strategy offers businesses better protection, and as a result, greater digital trust

"What the regulations force companies to do is to take care of their customers," says Lapré. "Whether you are a financial institute or a service provider, you need to mitigate the risks and make online business interactions safer and more trustworthy."

"These days we know with everything that is happening around AI it has become much more difficult to identify whether something is real or fake, and that has the potential for inflicting a huge amount of damage on a business," Lapré explains.

Selecting a strategic digital solutions partner ensures robust processes and controls while extending security capabilities without the need for leaders to expand headcount.

### Navigating evolving challenges

"Every audit is an opportunity for improvement. At DigiCert, we undergo over 26 annual audits spanning the full scope of our business and global footprint. That brings trust to the table because you know that the company you are partnering with has the processes in place to maximise risk mitigation," says Lapré.

While cybersecurity risks can't be entirely avoided, employing a robust cybersecurity strategy can ensure no money is left on the table and reputation is left intact.

Cyber threats are becoming more intelligent, and compliance regulations are increasingly complex and onerous. A digital compliance strategy offers businesses better protection, and as a result, greater digital trust."

Failure to make the transition from manual processes to a digital strategy is a huge risk that no organisation can afford to take," he says. ●

# Why your compliance strategy is only as strong as your team

Robust cyber strategies can help future-proof organisations – but success hinges on building compliance-ready teams who understand their role in digital trust

Despite substantial investments in digital compliance tools, human error remains a cause of security breaches worldwide with 68 percent of breaches involving a human element in 2024 according to Verizon.

This gap between technological capabilities and human performance highlights a crucial truth: effective cybersecurity depends not just on organisations implementing the right tools, but on building teams that fully understand how to use them.

Executives need to invest equally in their people's compliance knowledge and their technological defences. This balanced approach ensures teams can both implement security measures effectively and maintain them over time, creating a robust defence against evolving cyber threats.

To stay ahead and afloat of complex digital challenges, your cybersecurity strategy is only as strong as the people implementing it.

## Strengthening collective responsibility

Cybersecurity compliance is a collective responsibility that extends beyond the IT department to encompass the entire organisation. As regulatory requirements grow more complex, organisations must build diverse compliance teams with a range of skills.

Modern cybersecurity compliance requires input from every level of an organisation, no longer leaving digital responsibility to IT teams. Each team member can bring essential skills and perspectives to maintain effective compliance.

Dr Tommaso De Zan, senior manager for data governance at tech policy advisory Access Partnership, says "The often-overlooked role of team members at different levels is crucial in this era of increasing regulatory complexity. Leaders should develop entire teams so that they are ready and able to adopt robust security processes - proactive teams are an asset," he says.

Keeping up with regulatory changes is a constant challenge that tests even the most organised compliance teams and prioritising upskilling in tandem with the pace of evolving risks should be a key consideration for businesses.

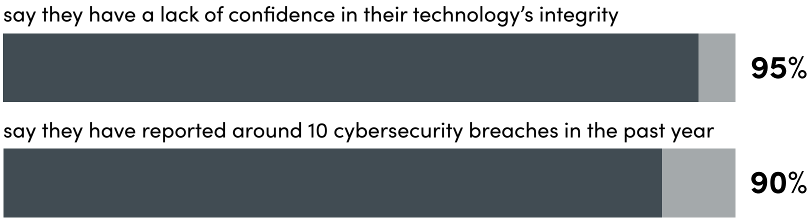
New requirements emerge continuously across industries and regions, creating a complex web of rules that teams must track, interpret and implement. Success requires not just vigilance from compliance teams but a genuine dedication from every department to maintain standards and adapt to new requirements.

## Fostering compliance-first cultures

No longer is compliance a one-time checkbox exercise, but an essential culture for teams to embed and continue developing. Success depends on making compliance a shared responsibility where security becomes integral to how teams work, not just an extra requirement to fulfil.

**For sustainable success, leaders must shift compliance from checkboxes to an adaptive, learning-driven culture**

Percentage of leaders expressing their approach to enterprise-wide compliance learning



Deloitte 2024

This can enable organisations to meet security requirements essential for reaping the benefits of digitalisation and building lasting security awareness.

Casey Ellis, who advises national security agencies in the US, UK and Australia, argues that good compliance should happen naturally and become second nature as part of robust business operations.

"If you're doing it right, it's effective and the business doesn't notice it. Ultimately, security compliance can be pivoted from an extrinsic force to an intrinsic drive by driving cross-functional security awareness, celebrating wins, and looking for ways to use security excellence as a market differentiator. These are all useful tools for creating a culture that has security compliance at its core," he says.

### Upskilling and reskilling

Shifting privacy concerns and digital threats add complexity to compliance efforts. Teams must understand how these new risks affect their regulatory obligations, requiring constant training and skill development.

Yet many organisations struggle to fund adequate compliance training and updates due to budget and staffing constraints.

"Securing adequate budget for high-quality compliance programs can produce conflicts with other business priorities, and creating compliance frameworks that are applicable across jurisdictions adds another layer of complexity," Dr De Zan says.

"However, perhaps the most daunting challenge is ensuring widespread adoption throughout the organisation, as it requires changing behaviours and fostering a culture of compliance that resonates with employees at all levels," he adds.

Beyond just training delivery, organisations must verify that staff actually retain and apply security knowledge through continuous assessment and reinforcement - a one-off win is not enough.

Compliance demands a holistic approach where employees can become digital guardians. The most effective approach integrates compliance into daily workflows, creating a shared understanding that goes beyond traditional training.

"You don't just see it in companies, but also in external auditors and supervisory bodies. In the Netherlands, for example, the size of the team responsible for supervising those regulations has doubled or even tripled in the last two or three years, and it is still growing because more regulations will come, and more standards will be set," Lapré says.

"You need people with the skills to check them, implement them and control them, so a huge growth in demand for talent is expected in all those areas," he adds.

### Reimagining best practices

Empowering teams to adapt quickly to regulatory changes without sacrificing operational efficiency or creativity is a constant challenge when teams can feel constrained by compliance requirements, leading to resistance or delays in implementing updates.

Ellis says: "Ultimately, organisations should apply security according to their threat and risk models but given that these are dynamic and often poorly understood within an organisation, compliance plays a vital role in reducing human error, guiding best practice and otherwise picking up the slack.

"Thoughtful vendor selection, prioritisation based on existing organisational strengths, and striving for alignment with revenue and product-generating business units is both a challenge and an opportunity for excellence and differentiation if it is done well," he says. ●

> Leaders should develop entire teams so that they are ready and able to adopt robust security processes - proactive teams are an asset

# Regulatory reboot: the future of cyber compliance

From compliance mandates to cybersecurity imperatives: how can leaders navigate stricter regulations, transform risk frameworks and win the race for robust governance?

**Prioritising effective responses to changing frameworks and cyber regulation can help executives maintain their organisation's competitive edge**

Percentage of leaders expressing how effective compliance offers a competitive advantage

**57%** say it enhances customer trust

**49%** say it enhances brand integrity and loyalty

**46%** say it aids business growth

**43%** say it helps maintain leadership position in the market

**As organisational compliance demands increase, cybersecurity has moved from an IT concern into a critical boardroom imperative**

Percentage of large businesses citing cybersecurity as an executive priority

**78%** provide cybersecurity updates to senior leaders quarterly

**75%** consider cybersecurity a high priority for senior leaders

**63%** have board members and senior leaders explicitly responsible for cyber security as part of their job role

**Leaders seeking to future-proof operations must understand how to balance security tool adoption with workforce compliance awareness**

Percentage of leaders expressing their security priorities over the next two years

**58%** improving employee cybersecurity awareness

**54%** improving information protection

**45%** consolidation and simplification of security solutions and tools digicert®

DigiCert is a leading global provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs its award-winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world.

For more information please visit **digicert.com**

Raconteur

**Editor:** Larnie Hur
**Design:** James Lampard, Samuele Motta
**Contributors:** Alison Coleman

Although this publication is funded through advertising and sponsorship,all editorial is without bias and sponsored features are clearly labelled.
For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3428 5230 or e-mail info@raconteur.net