Unlock Regulatory Compliance

With DORA, NIS2, and the EU AI Act

AUDITBOARD | Ascend2
RESEARCH-BASED MARKETING

Table of Contents

Introduction

The implementation of new regulatory measures that impact the UK, EU, and beyond are driving organisations to enhance vigilance in addressing evolving cybersecurity and operational risks. Compliance with regulations such as the **Digital Operational Resilience Act (DORA), the NIS2 Directive, and the EU AI Act** has become a critical priority for organisations, not just due to legal obligations, but as a strategic competitive advantage in today's high-risk, tech-driven world.

These regulations aim to improve cybersecurity resilience, ensure responsible AI use, and strengthen accountability amongst organisations they apply to. Non-compliance carries extensive consequences, from reputational damage to significant financial penalties, making it essential for organisations to understand where they stand, what risks they face, and what steps they need to take to achieve and maintain compliance.

AuditBoard, in partnership with Ascend2 Research, surveyed 272 risk, InfoSec, and IT compliance professionals throughout the UK and Germany to assess how organisations navigate compliance with these regulations. Our research uncovers both progress and promise in conformance, as well as pressing strategic and operational challenges.

A vast 91% of respondents report feeling concerned about cybersecurity threats to their organisation, and 86% are aware of incidents within their industry in the past year. However, disparity exists between awareness of these risks and the actions currently undertaken to mitigate them. We found that even amongst organisations that initially regarded themselves to be fully compliant, many are missing essential controls that could leave them vulnerable to non-conformance and related risks. This research also uncovers a critical disconnect between the strategic lens of the executive compared to the operational perspectives of those working within the compliance lines of defence.

For professionals navigating these demands, **this report provides actionable insights into the state of organisational readiness, highlighting industry-specific challenges and opportunities for improvement**. Regardless of where you are on your journey to conforming with the regulations relevant to your organisation, this report equips you with the information needed to drive efforts in the right direction.

UK vs. EU

UK professionals report more concern about cybersecurity risk with 35% saying they are extremely concerned vs. 28% of the EU. 49% of those in the UK report knowledge of a cybersecurity incident in their industry that had a significant impact, compared to just 37% in the EU.

DORA, NIS2, and the EU AI Act at a Glance

DORA (Digital Operational Resilience Act)

DORA, fully implemented by 2025, aims to strengthen the financial sector within the EU by establishing unified standards for cybersecurity and ICT resilience. It emphasises monitoring third-party service providers, incident reporting, and regular system testing to ensure a more secure and resilient financial system across member states.

NIS2 (Network and Information Security Directive 2)

NIS2 enhances cybersecurity across the EU by requiring member states to improve their network and information system security, emphasising incident reporting, risk management, and collaboration between the public and private sectors. It encourages information sharing and cooperation whilst imposing penalties for non-compliance.

EU AI Act

The EU AI Act, set to be fully implemented in 2025, is the first comprehensive regulatory framework for artificial intelligence, aimed at ensuring transparency, accountability, and ethical governance in AI systems. It applies to both EU-based organisations and those wishing to trade with the EU, establishing strict oversight and a European Artificial Intelligence Board for national cooperation.

Top Takeaways

Bracing for workload impact.

90% of professionals surveyed report that their workload will be impacted by conformance with DORA, the NIS2 Directive, and/or the EU AI Act. InfoSec professionals feel the weight of compliance efforts most, with 38% expecting to be impacted to a great extent, compared to 29% of risk management professionals and 28% of IT professionals.

Bridging the gap.

92% of executives say they have real-time insights into compliance posture compared to just 69% of management professionals, highlighting a disconnect we see throughout this report. Executives may view periodic updates as “real-time,” whilst practitioners often rely on manual processes and Excel-based reporting, which are often far from truly real-time.

Red flag.

To ensure compliance with DORA, monitoring third parties is essential. However, an alarming 14% of those who claim their organisation is already in compliance have not yet implemented this critical element.

Playing catchup.

Compliance with NIS2 is reported to be a high priority among organisations surveyed. However, despite the directive’s compliance deadline having passed, only 52% of organizations report being compliant, with another 44% planning to meet requirements by the end of next year. This progress is influenced by the varying timelines and implementations of NIS2 directives across EU member states, as compliance requirements depend on whether individual countries have published and enforced their own localized versions of the directive.

A long road ahead.

Many organisations have significant work ahead of them on their journey to compliance. Even those claiming to already be in compliance with the EU AI Act are missing essential elements of compliance that could leave them vulnerable. Less than two-thirds (63%) of those claiming compliance report having transparency measures in place, only 55% say they have implemented risk management frameworks, and just over half (51%) execute comprehensive risk assessments.

Third-party AI use.

83% of professionals are concerned about third-party AI use in regard to compliance with the EU AI Act. 91% of those surveyed feel that the EU AI Act will positively impact their organisation’s use and development of AI applications.

Special Segments

Executive Perspective

43% of professionals surveyed are in the executive or C-level leadership for their organisations. This group, specifically when compared to those in senior leadership and management positions, gives us insight into the perceived priorities and challenges of those at a strategic level and how that differs from those who are closer to the day-to-day operations of an organisation.

The Road to Compliance

Our research covers organisations across all stages and timelines on their road to compliance. Use this insight to determine the various steps that need to be taken to effectively conform and gauge where your organisation stacks up compared to the competition.

UK vs. EU

Insights from professionals working for organisations in both the United Kingdom (60%) as well as the EU (40%) provide a unique picture of how the evolving regulatory landscape has varying implications based on the regional market, and how these regions differ in their approach and sentiment toward each of these regulatory acts.

Take Action!

Look for this icon throughout this report for useful tips and actionable insights to help you navigate your organisation's regulatory journey.

Industry Insight

Different industries face unique regulatory challenges and opportunities. Throughout this report, you will find various industry segments that closely examine sector-specific sentiment.

TECHNOLOGY 49%
(*Communications equipment, IT services, software, hardware*)

INDUSTRIAL 26%
(*Manufacturing, utilities, mining/quarrying/oil and gas extraction, construction, transportation/warehousing, waste management/remediation services*)

FINANCE AND INSURANCE 11%
(*Financial institutions, insurance, asset management, broker-dealers*)

SERVICES 10%
(*Healthcare, retail trade, real estate, hospitality, wholesale trade, entertainment, information, professional, agriculture*)

PUBLIC SECTOR AND EDUCATION 4%
(*Public administration, educational services*)

The Use of Frameworks

Amongst all organisations surveyed, 83% rely on ISO frameworks such as ISO 27001/2, 69% use NIST frameworks, and 42% use the NIST AI Risk Management Framework (AI RMF). By providing a structured, repeatable approach to managing cybersecurity risks, **frameworks play a critical role as organisations work to align with complex regulatory requirements** brought on by directives like DORA, NIS2, and the EU AI Act.

Industrial and technology companies are more likely to use ISO frameworks. In the finance and insurance industry, 61% have adopted the NIST AI RMF framework, compared to 33–44% of other industries. Both technology and finance companies are more likely to use NIST frameworks than others.

Professionals using these frameworks report yielding significant value from them: **93% of those utilising frameworks report that their use has reduced cybersecurity risk, with 45% seeing significant reductions**.

Do you currently use any of the following frameworks as guidance, structure, or support in complying with cybersecurity risk-related regulations?

	Industrial	*Technology*	*Finance*	*Services*
ISO 27001/2	**89%**	**85%**	**77%**	**67%**
NIST (CSF, 800-51, 800-171, etc)	**69%**	**72%**	**77%**	**59%**
NIST AI RMF	**44%**	**40%**	**61%**	**33%**
Other	**0%**	**0%**	**0%**	**0%**
None of the above/We do not utilise frameworks	**0%**	**2%**	**3%**	**11%**

UK vs. EU

52% of those in the UK report that utilisation of frameworks like ISO and NIST lessened the risk of cybersecurity incidents in the last 12 months to a significant degree, compared to just 32% in the EU.

Overview of Key Frameworks

ISO 27001/2: These international standards provide a comprehensive framework for managing information security risks, emphasising processes and controls to protect data. ISO frameworks are particularly popular in the technology sector, where adherence is often seen as a baseline for operational excellence and global trust.

NIST (CSF, 800-53, 800-171, etc.): The National Institute of Standards and Technology's frameworks are widely used for their detailed guidelines on managing cybersecurity risks, especially in industries that require robust risk assessments and control implementations.

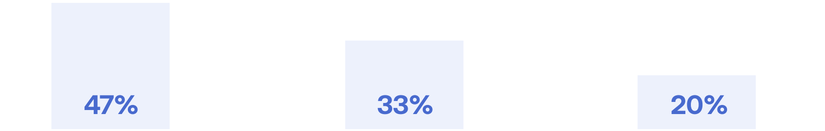
NIST AI RMF: This emerging framework addresses the unique risks associated with artificial intelligence systems, offering guidance on building trustworthy and secure AI solutions. This is a critical consideration given the EU AI Act's focus on ethical and secure AI development.

1.1

Adopting New Frameworks

The vast majority of organisations are navigating multiple and often overlapping regulations. Over 80% of the organisations we surveyed must comply with at least two of the three regulations we discuss in this report (DORA, NIS2, and the EU AI Act).

Percent of those required to comply with DORA, NIS2, and EU AI Act.



Required to comply with all three regulations

Required to comply with two of the three regulations

Required to comply with one of the three regulations

Adopting multiple frameworks to map to the requirements of each regulation can help ensure comprehensive coverage and minimise duplication of efforts as organisations work to comply. Frameworks like ISO 27001 and NIST CSF serve as foundational tools that address overlapping regulatory requirements, whilst specialised frameworks enable targeted compliance for more niche requirements.

However, whilst frameworks are undeniably valuable, adopting them is not always seamless. Only 25% of professionals surveyed find it extremely easy to adopt new frameworks using their current technology.

Executive Perspective

Executives are over 1.5x more likely than non-executives to perceive the adoption of new frameworks as extremely easy (32% vs 19%). This disconnect demonstrates how executives may not fully understand the undertaking of integrating new frameworks into existing systems. Those in senior leadership and management roles face the day-to-day operational challenges that this may present, allowing them to better quantify the required effort and resources.

Take Action

A streamlined approach to adopting new frameworks. When dealing with overlapping requirements, such as those found in DORA, NIS2, and the EU AI Act, organisations can benefit greatly from adopting new frameworks. By leveraging AuditBoard's compliance management solution, companies can efficiently navigate adoption and manage compliance across global operations. With AuditBoard, you can automatically map new frameworks to existing controls, simplifying the implementation of additional compliance requirements. This streamlined approach reduces redundancies, enhances visibility, and strengthens overall cybersecurity posture.

1.2

Leveraging AI

Professionals across industries agree that **the most valuable applications of AI in governance, risk, and compliance (GRC) are identifying and evaluating risks and detecting fraudulent activities**. These AI applications perform deep analysis and pattern recognition, which typically require significant amounts of time and human resources. By freeing up resource time, this allows professionals to focus on taking a proactive approach to their compliance posture, rather than a reactive approach.

The data highlights a clear trend in how professionals perceive the value of AI in GRC efforts. Organisations are beginning to see AI as a tool that can go beyond spotting trends or streamlining repetitive tasks. The interest in leveraging AI to test adherence to regulations (57%) and applying machine learning to uncover insights within data (54%) reflects this growing confidence.

UK vs. EU

UK companies place even greater emphasis on many of these applications, such as prioritising risk evaluation (74% vs. 63%) and identifying fraud (72% vs. 62%).

Which of the following applications of AI would be most useful in your governance, risk, and compliance (GRC) efforts?

70% *Identifying and evaluating risks*

68% *Identifying fraudulent activities*

64% *Automating responses to incidents and breaches*

57% *Tools for testing adherence to regulations*

54% *Applying ML to uncover relationships and insights within data*

47% *Drafting risk, control, and policy language*

AI offers powerful tools for automating processes, uncovering insights, and enhancing efficiency. However, it cannot replace the professional judgment or accountability required for high-stakes decisions, such as responding to cybersecurity incidents. **Effective GRC strategies rely on a human-in-the-loop approach, where AI supports, but does not replace, practitioner expertise.**

86% of those surveyed say they have access to real-time insights on their compliance posture.

Executive Perspective

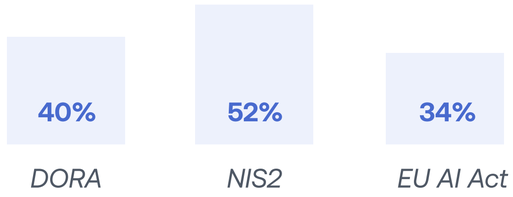
Executives, VPs/directors, and management professionals have varying perspectives on their access to real-time insights. **92% of executives say they have real-time insights into compliance posture compared to just 69% of management professionals.** This disparity could reflect differing definitions of “real-time.” Executives typically receive periodic updates that provide a high-level overview aligned with their strategic decision-making needs. Meanwhile, practitioners and management professionals are directly involved in the day-to-day work and would experience firsthand efforts and manual work, creating a disconnect between perceived and actual real-time insights. Whilst executives may feel informed, the operational reality often involves labour-intensive reporting, causing a natural delay in data timeliness.

2.0

Prioritisation of Regulations

Organisations are most likely to already be in compliance with NIS2, with 52% reporting adherence, compared to 40% for DORA and just 34% for the EU AI Act. This disparity demonstrates the relative maturity of organisations' cybersecurity measures compared to emerging requirements around AI governance.

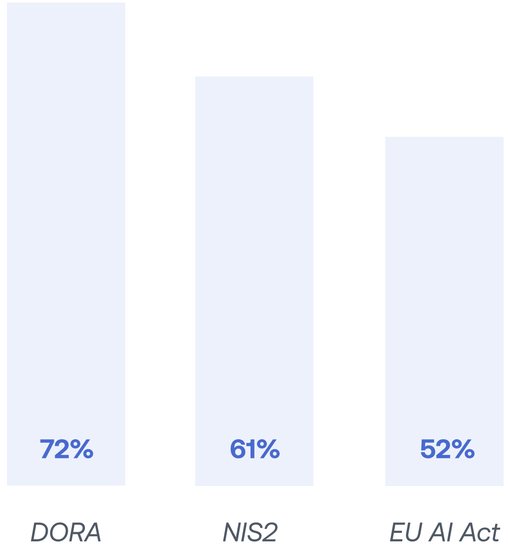
Percent of organisations reporting already in compliance.



Despite lower compliance rates, **72% of organisations list DORA as a high priority, requiring immediate attention**. Only 52% of organisations, however, see the EU AI Act as an urgent matter, which could be attributed in part to the transitional window of 24 months for most elements of the act to become applicable, whilst certain prohibited practices will take effect earlier. This phased implementation allows organisations time to align their AI systems with the new regulations. However, it's important to note that the grace period primarily applies to products already on the market. AI systems currently in the development phase are expected to comply upon launch.

Grace period or not, **organisations should move adherence to the EU AI Act to their list of high priorities and proactively work** towards compliance to ensure readiness by the deadlines.

High priority, requires immediate attention.



3.0

Challenges to Conformance

Despite the distinct requirements of each regulation, there are consistent challenges that organisations face as they work toward conformance with DORA, NIS2, and the EU AI Act. Whilst each brings its own complexities, there is notable overlap of key barriers such as resource constraints, continuous resilience testing, integrating multiple regulatory requirements, and maintaining ongoing compliance across the three. This indicates a critical need for compliance strategies to address shared challenges whilst also taking into account the unique demands of each regulation.

Top Four Challenges Across Regulations

DORA

- **47%** *Procuring resources (financial, human, technological)*
- **45%** *Continuous resilience testing/monitoring*
- **43%** *Complexity of integrating multiple regulatory requirements*
- **42%** *Establishing a comprehensive incident reporting system*

NIS2

- **45%** *Maintaining ongoing compliance*
- **40%** *Complexity of integrating multiple regulatory requirements*
- **39%** *Implementing disaster recovery/business continuity planning and testing*
- **38%** *Procuring resources (financial, human, technological)*

EU AI Act

- **39%** *High implementation costs*
- **37%** *Ensuring monitoring of resilience in third-party relationships*
- **37%** *Continuous resilience testing/monitoring*
- **35%** *Maintaining ongoing compliance*

3.1

Resources and Workload

90% of respondents feel that conformance will increase their workload. Increased workloads can strain resources, driving organisations to prioritise resource optimisation and workload management. The data demonstrates this, as 45% of organisations have already allocated significant resources toward compliance with these regulations. Another 45% plan to do so in the next six months, a timeline that is precariously close to regulatory deadlines.

Executive Perspective

Executives feel this pressure most acutely, with 37% expecting a “great extent” of impact, compared to 27% of senior leadership and 22% of management. This disparity suggests that executives have a more future-looking perspective on the operational and strategic challenges that maintaining compliance will impose as these regulations take effect.

UK vs. EU

40% of those in the UK feel that compliance with DORA, NIS2, and/or EU AI Act will impact their workload to a great extent, compared to just 17% of the EU professionals surveyed who feel their workload will be impacted greatly.

Take Action

The right tools and solutions can address compliance challenges, enabling organisations to effectively navigate the complexities of the ever-evolving regulatory landscape.

- Simplify the **ongoing management of compliance programs** by centralising common controls, automating workflows, and providing real-time visibility into compliance status to ensure continuous alignment with evolving regulatory requirements.
- Manage the **complexity of integrating multiple regulations** through enhanced framework crosswalk capabilities. AuditBoard’s compliance management solution allows you to map your controls across various frameworks and regulations, such as DORA, NIS2, and the EU AI Act, allowing you to take credit for existing controls and reduce implementation efforts for new controls.
- The right technology to support your compliance efforts can greatly increase efficiency, reducing the **resources required to manage these programs**. AuditBoard can automate manual tasks such as testing procedures and integrate compliance management into a single platform, enabling you to optimise existing resources.
- AuditBoard’s third-party risk management solution helps you **assess and monitor the resilience of third-party vendors**, a critical component of regulations like DORA and the EU AI Act.

Ensuring Compliance With DORA

At the time of this survey, **40% of organisations reported already being in compliance with DORA, and an additional 53% planned to meet the January 2025 deadline**. However, a closer examination reveals potential gaps between perceived and actual compliance. Amongst those claiming to be compliant, 77% have implemented critical controls such as regular ICT system testing and monitoring of third-party ICT service providers, but this leaves a notable portion who have not completed these foundational elements. Similarly, only 65% of those claiming compliance report having timely, standardised incident reporting, another key aspect of DORA.

In comparison, organisations not yet in compliance lag further behind, with only 61% conducting regular ICT system testing and 59% monitoring third-party ICT service providers. This suggests organisations should conduct a gap analysis on their current compliance posture against their future state target compliance, in order to understand, prioritise, and undertake the actions required for full regulatory compliance and avoidance of consequent penalties.

Which of the following elements of DORA has your organisation *completed*?

	Already in compliance with DORA	*All Others*
Regular ICT system testing	**77%**	**61%**
Monitoring third-party ICT service providers	**77%**	**59%**
Advanced threat-led penetration testing for critical systems	**73%**	**58%**
Timely, standardised incident reporting	**65%**	**55%**
Developing detailed risk management frameworks	**65%**	**65%**

Take Action

Identify and monitor service providers to ensure compliance with DORA. To ensure compliance with DORA, monitoring third-party ICT service providers is essential. However, an alarming 14% of those who claim their organisation is **already in compliance** have not yet implemented this critical element. Organisations without active monitoring in place are not yet compliant with DORA. Follow these best practices to protect your organisation:

- **Never rely solely on quarterly KPI or SLA meetings with service providers.** These meetings often provide reports influenced by the provider's bias to maintain the business relationship.
- **Tier vendors as soon as possible.** As a first step, classify your vendors by their criticality to your operations, particularly ICT vendors, then apply policies per tier.
- **Regularly monitor and resurvey.** DORA requires that critical ICT vendors be resurveyed and monitored at least annually. For high-risk or critical vendors, quarterly reviews are ideal to ensure alignment with evolving standards and identify emerging risks.
- **Maintain detailed documentation.** Ensure that your monitoring activities are well-documented. This documentation demonstrates proactive compliance and can protect your organisation in the event of third-party failures.

4.1

An Executive Disconnect

Executives are more likely than non-executives to rate implementation of disaster recovery, business continuity planning, ensuring monitoring of resilience in third-party relationships, and understanding the requirements as top challenges. Meanwhile, senior leadership and management professionals are more likely than executives to identify the complexity of integrating multiple regulatory requirements as a top challenge, and **nearly 70% of management professionals find procuring resources to be a top issue**.

Executive Perspective

Executives are often less involved in the day-to-day of regulatory compliance, which might explain why they are less likely to rank the complexity of integrating multiple regulatory requirements as a top concern. However, senior leadership and management are closer to the implementation process and more directly impacted by these challenges.

What are the top challenges to comply with DORA?

	Executive /C-Suite	*Senior Leadership*	*Management*
Implementing disaster recovery/business continuity planning and testing	47%	36%	38%
Continuous resilience testing/monitoring	47%	49%	34%
Establishing a comprehensive incident reporting system	45%	44%	31%
Ensuring monitoring of resilience in third-party relationships	43%	33%	16%
Procuring resources (financial, human, technological)	41%	44%	69%
Maintaining ongoing compliance	40%	36%	56%
Understanding the requirements	31%	17%	25%
Stakeholder accountability and engagement	29%	29%	22%
Complexity of integrating multiple regulatory requirements	29%	56%	53%
High implementation costs	27%	40%	59%

Take Action

Do more with less. Executives are less likely than senior leadership and management professionals to experience firsthand the ongoing effort required to maintain compliance, especially under resource constraints, which nearly 70% of management professionals listed as a top challenge. **Utilise technology to automate manual tasks**, such as the mapping and integration of multiple regulatory frameworks, and reduce the burden on existing resources whilst addressing the strategic objectives of executives, such as improving efficiency and scalability. Learn more.

Nuances of Essential vs. Important Entities

The NIS2 Directive enforces stricter cybersecurity requirements for organisations classified as either essential entities (39% of those surveyed) or important entities (58%). Both classifications must comply, with essential entities facing potentially harsher penalties for non-compliance.

Despite the directive's compliance deadline having passed, only 52% of organisations report being compliant, and another 44% plan to meet requirements by the end of next year. Compliance progress varies across organizations, partly due to the varying publication and enforcement of NIS2 legislation at the national level. **Organisations that are deemed essential are significantly more likely** than those deemed important entities **to have taken critical steps toward compliance**, such as developing an incident response plan, conducting digital resilience testing, and training and educating board members and employees on security procedures.

This disparity is likely due to the heightened risks and potential penalties that essential entities face. Providers of critical infrastructure and services may be under increased pressure to protect against cybersecurity risks. Important entities may also perceive these risks as less immediate or face resource constraints that delay compliance efforts.

Which of the following elements of NIS2 has your organisation *completed*?

	Essential	*Important*
Develop an incident response plan	**60%**	**40%**
Conduct digital resilience testing	**58%**	**41%**
Monitor and detect incidents	**58%**	**45%**
Train and educate board and employees on security procedures	**57%**	**38%**
Engage with cybersecurity professionals	**57%**	**55%**
Identify frameworks that align with compliance	**56%**	**37%**
Implement strong cybersecurity access controls	**52%**	**41%**
Adopt new technology	**52%**	**47%**
Conduct gap analysis/risk assessment	**45%**	**41%**
Ensure business continuity	**45%**	**37%**

Organisations that claim to be in compliance with NIS2 are significantly more likely than others to have already engaged with cybersecurity professionals (61% vs. 48%) and monitor and detect incidents (60% vs. 40%) on their NIS2 compliance journey.

5.1

Evolving Challenges of Compliance With NIS2

Those already in compliance with NIS2 are most challenged by establishing incident reporting systems, maintaining ongoing compliance, and complexities that come with managing multiple regulations. Interestingly, those not yet in compliance anticipate being most challenged by maintaining ongoing compliance, likely because they have not yet implemented the foundational systems and processes required for efficient and effective management. For these organizations, the prospect of meeting ongoing requirements can feel particularly daunting, as they are still in the early stages of addressing compliance demands.

What are the top challenges to comply with NIS2?

	Already in compliance with NIS2	*All others*
Establishing a comprehensive incident reporting system	**42%**	**32%**
Maintaining ongoing compliance	**41%**	**49%**
Complexity of integrating multiple regulatory requirements	**40%**	**39%**
High implementation costs	**38%**	**32%**
Procuring resources (financial, human, technological)	**38%**	**38%**
Continuous resilience testing/monitoring	**38%**	**25%**
Implementing disaster recovery/business continuity planning and testing	**35%**	**42%**
Understanding the requirements	**32%**	**26%**
Stakeholder accountability and engagement	**30%**	**34%**
Ensuring monitoring of resilience in third-party relationships	**29%**	**42%**

Executive Perspective

Managers and senior leadership find maintaining ongoing compliance and the complexity of integrating multiple regulatory requirements to be top challenges, a direct reflection of their close involvement in daily operations. Meanwhile, executives list implementing disaster recovery and business continuity planning and testing at the top of their list of challenges. **This disconnect suggests that those day-to-day managing compliance operations need more support to efficiently deliver.** Leverage technology to bridge this gap and build a multi-framework risk and compliance program by streamlining processes for managers whilst providing executives with actionable insights into goals from the top-down.

Navigating New Regulatory Waters

The EU AI Act is recognised as the world's first comprehensive regulatory framework for artificial intelligence, applying not only to EU member states but also to organisations wishing to trade with the EU bloc. Included in its measures are requirements for effective oversight, control, documentation, and transparency across AI systems. The regulation establishes a European Artificial Intelligence Board to foster national cooperation and ensure compliance.

The EU AI Act classifies businesses based on the potential harm an AI system could cause if it malfunctions, is misused, or fails to meet safeguards. **Nearly half (47%) of organisations surveyed report being categorised as high risk, or potentially causing significant harm if their data protection controls fail.** Another 36% are classified as limited-risk, and 12% report minimal risk classification. Unacceptable risk is prohibited under the Act.

What is the highest level of risk that the EU AI Act classifies your product(s) in?

Unacceptable	**3%**
High	**47%**
Limited	**36%**
Minimal	**12%**
Does not apply	**1%**
Unsure	**1%**

91% of those surveyed feel that the EU AI Act will have a positive impact on their organisation's use and development of AI applications.

6.1

Challenges Across Industries

As organisations navigate the uncharted territory of compliance with the EU AI Act, they face **significant challenges, including high implementation costs (39%), ensuring resilience in third-party relationships (37%), and continuous resilience testing and monitoring (37%)**.

The specific barriers vary by industry. Industrial organisations are significantly more likely to struggle with allocating adequate resources. The technology sector finds continuous resilience testing and monitoring particularly difficult. In the services industry, maintaining ongoing compliance poses a challenge for half (50%) of organisations. Meanwhile, financial institutions report heightened difficulties in establishing comprehensive incident reporting systems and interpreting regulatory requirements.

Executive Perspective

Executives are more likely to find third-party monitoring (40% vs. 34%), continuous resilience testing (40% vs. 34%) and disaster recovery planning (39% vs. 32%) challenging. Meanwhile, non-executives struggle more with establishing incident reporting systems (28% vs 36%) and understanding requirements (25% vs. 31%) as they face the complexity of applying regulatory standards without full control over resources. It is critical for organisations to acknowledge this gap between strategic, high-level risk management and operational implementation.

What are the top challenges to comply with the EU AI Act?

	Industrial	*Technology*	*Finance*	*Services*
Procuring resources (financial, human, technological)	**43%**	**36%**	**19%**	**35%**
Complexity of integrating multiple regulatory requirements	**43%**	**33%**	**30%**	**40%**
High implementation costs	**37%**	**41%**	**33%**	**45%**
Stakeholder accountability and engagement	**37%**	**38%**	**37%**	**10%**
Maintaining ongoing compliance	**35%**	**30%**	**33%**	**50%**
Continuous resilience testing/monitoring	**33%**	**40%**	**30%**	**35%**
Ensuring monitoring of resilience in third-party relationships	**32%**	**39%**	**44%**	**45%**
Implementing disaster recovery/business continuity planning and testing	**30%**	**37%**	**33%**	**40%**
Establishing a comprehensive incident reporting system	**25%**	**33%**	**41%**	**30%**
Understanding the requirements	**17%**	**29%**	**41%**	**35%**

Concerns about third-party accountability

Concerns about the role third parties play in compliance with the EU AI Act are widespread, with 83% of professionals expressing worry. The EU AI Act places obligations on buyers, employers, providers, and distributors, but end users such as retailers typically face less responsibility. With the rollout of the Act, organisations will likely benefit greatly from the transparency requirements that extend to third parties, making the vetting process easier. For now, however, thorough vetting and comprehensive third-party risk management processes are recommended to mitigate potential compliance risks.

UK vs. EU

UK professionals report significantly more concern than EU professionals about third-party use of AI, with 34% saying they are extremely concerned compared to just 17% who are extremely concerned from the EU.

6.2

Timelines for Compliance

At the time of the survey, one-third of organisations reported already being in compliance with the EU AI Act, whilst 38% expected to comply by February 2025. Another 24% plan to be in compliance by the end of 2025.

When do you expect to comply with the EU AI Act?

34% *We are already in compliance with the EU AI Act*

38% *By February 2025*

24% *By the end of 2025*

4% *In 2026 or after*

UK vs. EU

The UK is ahead of the curve in compliance efforts with the EU AI Act, with 76% who say their organisation is already in compliance or will be by February 2025, compared to 63% from the EU.

There seems to be less of an urgency to comply with the EU AI Act amongst those surveyed compared to other regulations with just over half (52%) indicating that compliance is a high priority requiring immediate attention. This could be due to the two-year grace period provided for AI products after they go to market. **It is critical that organisations are proactive about their compliance with the EU AI Act now, as this grace period applies only to launched products, not to those in development, and deadlines are fast approaching.**

Executive Perspective

Executives and senior leaders are more likely to view compliance as a high priority than managers (56% and 53% versus 43%, respectively). Leadership not only has a broader responsibility for organisational strategy and risk management, but they also may be more directly impacted by punishments for non-compliance that include significant fines, reputational damage, and barriers to market access within the EU. It is important for organisational leaders to communicate the critical nature of compliance with the EU AI Act to their employees.

Timeline for Compliance

- 12 July 2024: The AI Act was published in the Official Journal of the European Union.
- 1 August 2024: The Act entered into force, initiating the countdown to its application.
- 2 February 2025: Prohibitions on certain AI systems posing unacceptable risks become applicable.
- 2 August 2025: Obligations for providers of General Purpose AI (GPAI) models commence, along with governance rules and the designation of national competent authorities by Member States.
- 2 August 2026: The majority of the Act's provisions, including those for high-risk AI systems listed in Annex III, become applicable. Member States are also required to have established at least one operational AI regulatory sandbox by this date.
- 2 August 2027: Obligations for high-risk AI systems not specified in Annex III, particularly those integrated into regulated products, take effect.
- 31 December 2030: AI systems that are components of large-scale IT systems established by EU law must be brought into compliance by this date.

Source

6.3

Compliance Maturity

Overall, approximately half of organisations report having high-quality data governance (52%) and are actively implementing risk management frameworks (50%). Additionally, nearly half indicate they are conducting post-market monitoring for high-risk AI systems (47%) and adhering to specific transparency obligations (46%).

Whilst those who claim to be in compliance with the EU AI Act have taken significantly more action than others, there are gaps that suggest full compliance is still a work in progress. True compliance is a substantial undertaking for organisations and this data gives insight into a potential misunderstanding of what this entails. These misconceptions could leave businesses vulnerable to regulatory risks and potential penalties.

Which of the following elements of the EU AI Act has your organisation *completed*?

	Already in compliance with EU AI Act	*All others*
High-quality data governance	**64%**	**46%**
Transparency measures	**63%**	**32%**
Robust system design	**59%**	**35%**
Detailed technical documentation	**56%**	**33%**
Implement risk management frameworks	**55%**	**48%**
Human oversight mechanisms	**54%**	**35%**
Post-market monitoring for high-risk AI systems	**54%**	**43%**
Adhering to specific transparency obligations	**54%**	**42%**
Comprehensive risk assessments	**51%**	**42%**
None of the above	**0%**	**3%**

Take Action

Apply existing frameworks for stronger coverage. Whilst ISO 42001 offers a widely adopted framework to help businesses align with the regulation, compliance remains complex. Many organisations are piecemealing strategies by incorporating elements of the NIST AI RMF and GDPR. Innovative compliance solutions like AuditBoard can support businesses in integrating multiple frameworks, helping ensure sufficient coverage and readiness for this landmark regulatory shift. Learn how to secure your organisation and accelerate your business here.

Conclusion

Organisations across the UK, EU, and beyond are constantly under pressure to adopt more proactive and strategic approaches to compliance. Regulations and frameworks like DORA, NIS2, and the EU AI Act are not only obligations that must be prioritised in order to avoid penalties, they also serve as opportunities for organisations to strengthen their risk posture, improve operational workflows and processes, and use technology more responsibly. This journey to compliance does not come without challenges, however, and requires a high-functioning ecosystem to support success.

Our findings demonstrate that organisations are well on their way to conformance despite these challenges. There is a general awareness of the repercussions of non-compliance and there are valuable actions being implemented to ensure conformance. We discovered that when organisations can address and manage the gap between strategic perspectives and operational execution, they are better equipped to navigate these steps. We also found that by leveraging the right technology, professionals at all levels and functions can make more effective decisions and more efficiently execute efforts required to maintain compliance. Whether in early stages of compliance or actively working to maintain it, organisations can use the findings in this report to build a framework for their journey and help future-proof their strategies.

Methodology and Participants

Methodology

AuditBoard, in partnership with Ascend2 Research, developed a custom online questionnaire to survey 272 professionals in decision-making roles in risk management, information technology (IT), and information security (InfoSec). These individuals represent organisations in the United Kingdom and Germany with an annual recurring revenue of $25M or greater. The survey was fielded in November 2024.

Participants

N = 272 professionals

Applicable Regulations

DORA (Digital Operational Resilience Act)	68%
NIS2 (Network and Information Security 2 Directive)	72%
EU AI ACT (European Union Artificial Intelligence Act)	85%

Area of Focus/Department

INFORMATION TECHNOLOGY (IT)	56%
INFORMATION SECURITY (INFOSEC)	25%
RISK MANAGEMENT/OPERATIONS	16%
LEGAL	2%
INTERNAL AUDIT	1%

Job Level

EXECUTIVE/C-SUITE	43%
SENIOR LEADERSHIP	37%
MANAGEMENT	20%

Region

UNITED KINGDOM/IRELAND	60%
EMEA	40%

Industry

TECHNOLOGY **49%**
(e.g., *communications equipment, IT services, software, technology hardware*)

INDUSTRIAL **26%**
(e.g., *manufacturing, utilities, mining/quarrying/oil and gas extraction, construction, transportation/warehousing, waste management/remediation services*)

FINANCE AND INSURANCE **11%**
(e.g., *financial institutions, insurance, asset management, broker-dealers*)

SERVICES **10%**
(e.g., *healthcare, retail trade, real estate, hospitality, wholesale trade, entertainment, information, professional, agriculture*)

PUBLIC SECTOR AND EDUCATION **4%**
(e.g., *public administration, educational services*)

About the Authors

Jason Sechrist
Director of Product Solutions (EMEA)
AuditBoard

Jason Sechrist, CIA, CISA, is the EMEA Director of Product Solutions at AuditBoard where he works with various internal audit and compliance teams to help automate the administrative tasks of audit, risk, and compliance activities. He previously was the Global Head of Internal Audit at Rackspace Managed Cloud where his responsibilities included developing and executing on a risk-based audit plan for the company's global footprint of data centres and office locations across the Americas, Europe, and Asia. Jason started his auditing career with PwC in Silicon Valley, working primarily with software and cloud service providers where he advised CTOs, CISOs, compliance managers, and system engineers. Prior to becoming an auditor, he led user testing and development for global aviation weather visualisation software as a service whilst serving on active duty for the United States Air Force.

Saulo Consalter
Alliances and Partner Manager (EMEA)
AuditBoard

Saulo Consalter, CISA, CRISC, PMP, is an Alliances and Partner Manager for EMEA at AuditBoard, connecting clients and partners to get the most out of their AuditBoard platform. He brings over 18 years of experience in guiding organisations to implement leading GRC and internal audit practices to the role. He specialises in helping businesses across various industries meet critical regulatory standards, including IFRC, SOX, and the UK Corporate Governance Code. Previously, Saulo served as the Head of Security and Information Governance at National Grid.

Mai Tran
Product Solutions Manager (EMEA)
AuditBoard

Mai Tran is a Product Solutions Manager for EMEA at AuditBoard, working with various audit, risk, and compliance teams to meet regulatory standards and help automate their compliance programs. Mai started her career as an IT Risk Auditor at EY, before moving into consulting work for the firm and specialising in conducting SOC 2 readiness assessments and audits. She then joined a FTSE 250 company, Dunelm, as their Risk Business Partner, where she built their technology risk and TPRM programs from the ground up.

About the Research Partners

AUDITBOARD

AuditBoard is the leading cloud-based platform transforming audit, risk, compliance, and ESG management. More than 50% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the sixth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit AuditBoard.com.

Ascend2™
RESEARCH-BASED MARKETING

Ascend2 specializes in creating custom research studies that empower businesses to drive demand and elevate their marketing efforts. From survey design and conceptualization to comprehensive report creation and media outreach, Ascend2 delivers end-to-end research solutions tailored to your goals. Companies partner with Ascend2 to fuel impactful marketing content, generate high-quality leads, and engage prospects using original research and data. To learn more about Ascend2, visit ascend2.com.