The Readiness Report:

Financial Sub-sectors Most Prepared for the DORA Regulation

Contents

The DORA regulation..... 3

DORA readiness index..... 4

The cost of non-compliance..... 9

Steps to achieving DORA compliance..... 10

This report has analysed nine financially regulated sub-sectors against key regulatory compliance factors to assess the readiness of UK financial institutions for DORA. The findings highlight the key areas leading in compliance and which sub-sectors remain vulnerable to severe financial penalties and operational risks.

The DORA regulation

Last year, more than half of global financial institutions (54%) reported cyber-attacks that resulted in stolen and destroyed data, representing a 12.5% increase from 2023.

With cyberattacks costing British businesses close to £44 billion in lost revenue over the past five years, the case for stronger diligence has never been greater as digital threats grow more sophisticated.

Already, 66% of organisations view AI and machine learning as the biggest cybersecurity threat they expect to see in 2025, with generative AI fuelling increasingly advanced social engineering and ransomware attacks.

This comes after UK engineering firm Arup lost $25 million to fraudsters in 2024 after AI was used to digitally clone a senior manager in what is now the world's biggest known deepfake scam.

However, a critical gap in cybersecurity persists, particularly among SME businesses, after research found that many firms were operating under the misconception that they were 'too small' to be targeted by cybercriminals.

This is despite 58% of UK small businesses and 70% of medium businesses identifying breaches or attacks in the last 12 months, while 21% of businesses overall reported that breaches happen once a month.

The impact of data breaches, system failures, and cyber intrusions is widespread, detrimentally affecting consumers, markets, and the broader economy, especially as IBM revealed that it can take a company over 250 days to contain a breach.

Where previously firms relied on inconsistent guidelines, which varied by country, the implementation of DORA marks a concentrated stand by the EU to create a resilient financial sector in Europe.

By providing a universal framework, it eliminates regulatory discrepancies and conflicts and ensures all financially regulated businesses operating in the EU comply with the same standards - levying significant financial and reputational penalties for any non-compliance.

DORA readiness index

To assess readiness for DORA, our team analysed data from over 270 leading UK companies across nine financially regulated business sub-sectors.

By examining information from the Financial Conduct Authority (FCA), the Information Commissioner's Office (ICO), and other verified sources, we created an index that measures each sub-sector's current operational resilience to determine its ability to comply with new DORA requirements.

Which financial sub-sectors are most prepared for DORA?

DORA Readiness Index		
Rank	Sub-Sector	Index Score
1	Corporate and Specialist Services	100
2	Property and Real Estate Finance	99
3	Capital Markets and Trading	89
4	Pensions and Retirement Planning	79
5	Fintech and Technology	75
6	Insurance and Risk Management	66
7	Investments and Wealth Management	63
8	Financial Transaction Processing	55
9	Banking and Lending	37

The ‘DORA Readiness Report’ has revealed a far more resilient picture for the UK overall, with most financially regulated sub-sectors scoring highly on key indicators of digital resilience, such as low cybersecurity incident rates and minimal regulatory breaches.

Corporate and specialist services is the sub-sector most prepared for DORA, earning the maximum index score of 105. Notably, it scored highest for compliance with the FCA, with no fines reported in 2023 or 2024 and zero complaints raised.

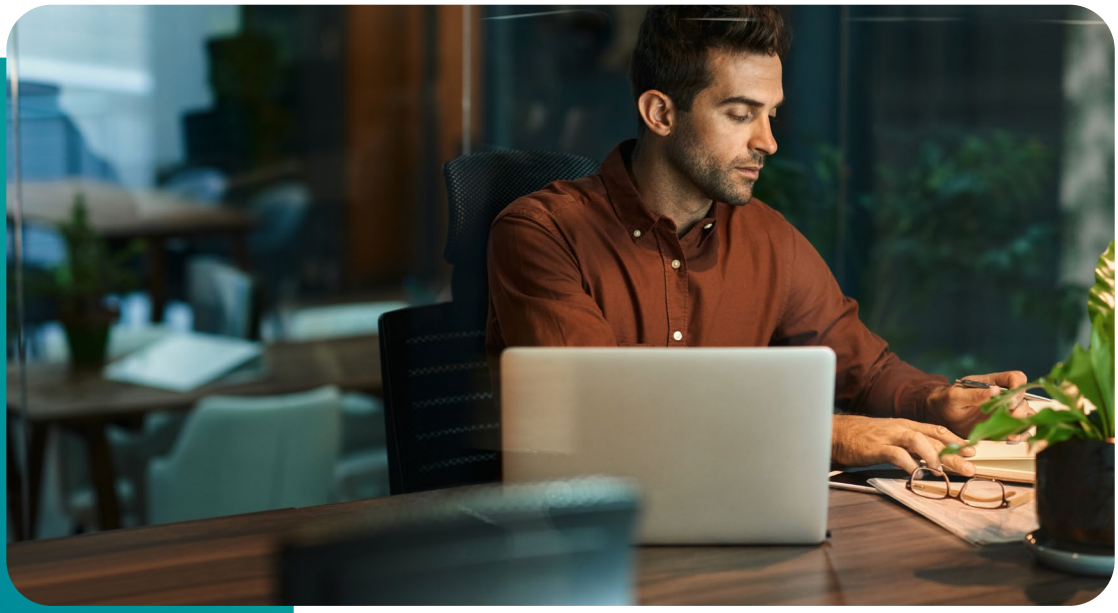
While it recorded four complaints to the ICO, including two cybersecurity incidents, it also had the highest number of firms registered to Cyber Essentials Plus - a government-backed certification that directly aligns with DORA's objectives of strengthening operational resilience.

Following close behind is the property and real estate finance sub-sector, and the capital markets and trading sub-sector, with scores of 99 and 89 respectively.

While the property and real estate finance sub-sector also reported zero fines or complaints with the FCA, the capital markets and trading sub-sector faces an estimated 1.3% overdue complaints, with only 29.6% of complaints closed within three working days and 68.9% within eight weeks.

These delays suggest that the sub-sector may be struggling to effectively manage and respond to risks, highlighting a potential gap in risk management practices across businesses.

Both sub-sectors also had a higher number of complaints reported with the ICO - with 14 in total for the property and real estate finance sub-sector - two of which were cybersecurity-related.



This comes as they were found to have a far lower cybersecurity certification uptake, particularly in the capital markets and trading sub-sector which had no firms registered for Cyber Essentials Plus.

This indicates a concerning vulnerability in their cybersecurity readiness which could increase their susceptibility to cyber threats.

All three sub-sectors were found to have a high concentration of businesses with operations in the EU, which could expose them to financial consequences for failing to adhere to DORA standards.

Elsewhere, the pensions and retirement planning and fintech and technology sub-sectors ranked in the mid-range, with overall scores of 79 and 75 respectively suggesting a moderate level of preparedness for DORA compliance.

Both sub-sectors had significantly higher levels of ICO complaints, with the pensions and retirement planning sub-sector reporting 26 incidents in total, six of which were cybersecurity-related.

As a key priority for cyber theft, improving cybersecurity has been a priority target in recent years, with The Pension Regulator releasing new guidance for pension scheme trustees and managers after the General Code of Practice shifted obligations from best practices to mandatory measures.

The sub-sectors most vulnerable to cyber threats

The insurance and risk management (66), investments and wealth management (63), and financial transaction processing (55) sub-sectors all ranked at the lower end of the scale for DORA readiness.

With notable gaps in operational resilience, the existing vulnerabilities may create greater challenges in meeting DORA standards and remaining resilient against emerging threats and challenges.

The research found the financial transaction processing sub-sector had the highest percentage of estimated overdue complaints with the FCA by far, at 10.6%, with only 15.7% of complaints closed or resolved within three days.

This underlines a slow or ineffective response rate to disruptions and risks, which may hinder the sub-sector's ability to adequately manage and comply with incident reporting.

However, the banking and lending sub-sector earned a DORA readiness score of just 37, marking it as the least prepared for compliance with the act.

The sub-sector's vulnerability is evident in the number of FCA fines it received, with seven fines totalling a cost of over £96 million between 2023 and 2024 - reflecting a serious pattern of non-compliance.

FCA Compliance			
Sub-Sector	**FCA Fines (2023-2024)**	**FCA - Amount Fined (Total)**	**FCA - Estimate Overdue Complaints (%)**
Insurance and Risk Management	0	£0	8.5%
Investments and Wealth Management	1	£27,766,200	6%
Financial Transaction Processing	0	£0	10.5%
Banking and Lending	7	£96,799,400	2.17%

Cybersecurity issues are also prevalent across all four sub-sectors, indicating a direct failure in operational resilience.

While the index ranked banking and lending as the least prepared sub-sector for DORA overall, the financial transaction processing sub-sector is revealed as the most vulnerable to cyber threats, with 30 reported cybersecurity incidents to the ICO - the highest out of all sub-sectors analysed.

The sub-sector also had the fewest firms registered for Cyber Essentials Plus, underscoring a severe lack of proactive cybersecurity measures and clear weaknesses in the existing digital infrastructure.

While reporting fewer cybersecurity incidents in comparison, the other sub-sectors also reported a low cybersecurity certification uptake despite firms having a large footprint in the EU.

This suggests that while financially regulated businesses in the UK are meeting basic operational compliance and resilience standards, many are failing to adequately safeguard systems against threats.

This gap in preparedness could leave them vulnerable to emerging risks, and for firms with operations in the EU, it undermines their ability to comply with DORA regulations.

The Sub-Sectors Most Vulnerable to Cyber Threats

Sub-Sector	ICO - Number of cybersecurity incidents reported	Number of firms registered to Cyber Essentials Plus
Insurance and Risk Management	16	4
Investments and Wealth Management	13	3
Financial Transaction Processing	30	3
Banking and Lending	13	4

The cost of non-compliance

The comprehensive framework set out in the Digital Operational Resilience Act will mean UK-based businesses interacting with the EU must adhere to it by January 2025, ensuring effective incident management, third-party oversight, and resilience testing.

However, challenges in managing complaints and adhering to current regulations, evident in the data, alongside the low adoption of resilience measures like the Cyber Essentials Plus certification, are key indicators of vulnerabilities in the financial sub-sector's preparedness for DORA.

With nearly two in five ICO complaints reported as cybersecurity incidents on average across all sub-sectors, the research highlights critical gaps in both compliance and cybersecurity controls - reinforcing the urgent need for robust risk management and resilience measures.

DORA compliance also extends beyond financially regulated businesses, particularly affecting any company providing technology or outsourcing services to financial institutions.

As a result, these firms may be classed as "critical third-party providers", or CTPPs, under DORA, subjecting them to the same level of regulatory scrutiny and standards.

Failing to comply with DORA will result in severe consequences for businesses, with financial penalties reaching up to 1% of a company's worldwide daily turnover for six months - posing a significant threat to businesses' bottom lines.

Beyond the financial severity, non-compliance can also damage a company's reputation and erode trust among clients and investors. This is particularly harmful, as cybersecurity incidents and operational disruptions can lead to long-lasting negative perceptions that also result in a financial hit.

DORA's regulatory framework also aligns with a broader trend in the UK's cybersecurity landscape, particularly with the government's forthcoming Cybersecurity and Resilience Bill.

This aims to address rising cyber threats by empowering regulators and enforcing stricter incident reporting requirements - emphasising the necessity for enhanced cybersecurity protocols and testing across all sub-sectors.

Steps to achieving DORA compliance

Employee awareness and role-specific training

Employee awareness and compliance training are fundamental to DORA compliance, yet only 30% of small businesses report having training or awareness sessions on cybersecurity in the last 12 months, rising to 52% for medium-sized businesses.

All employees will need to participate in regular ICT training and security awareness to effectively comply with the risk management framework, which will improve their ability to identify risks, protect ICT assets, and follow cybersecurity best practices.

Investing in training which is tailored to staff members' specific responsibilities can also bridge any resilience gaps by ensuring that employees are better equipped to handle critical functions, and effectively carry out recovery measures for improved business continuity.

Incident reporting and monitoring

Businesses must be prepared to promptly classify and report on significant ICT incidents to regulatory authorities to ensure effective and timely responses to any potentially disruptive events while allowing authorities to monitor resilience.

Establishing clear reporting channels, with defined incident classifications and employees trained to identify and report on incidents, will be an essential part of this.

Continuous monitoring will also need to be implemented to evaluate the effectiveness of incident response procedures and assess how well staff are applying ICT security measures in day-to-day operations.

Regular compliance testing and assessments

Regular compliance testing and assessments are vital for ensuring the business is consistently aligned with DORA and safeguarded against rising threats.

This includes conducting annual resilience tests to pinpoint existing vulnerabilities, as well as undergoing advanced threat-led penetration testing (TLPT) every three years to validate the effectiveness of implemented security controls.

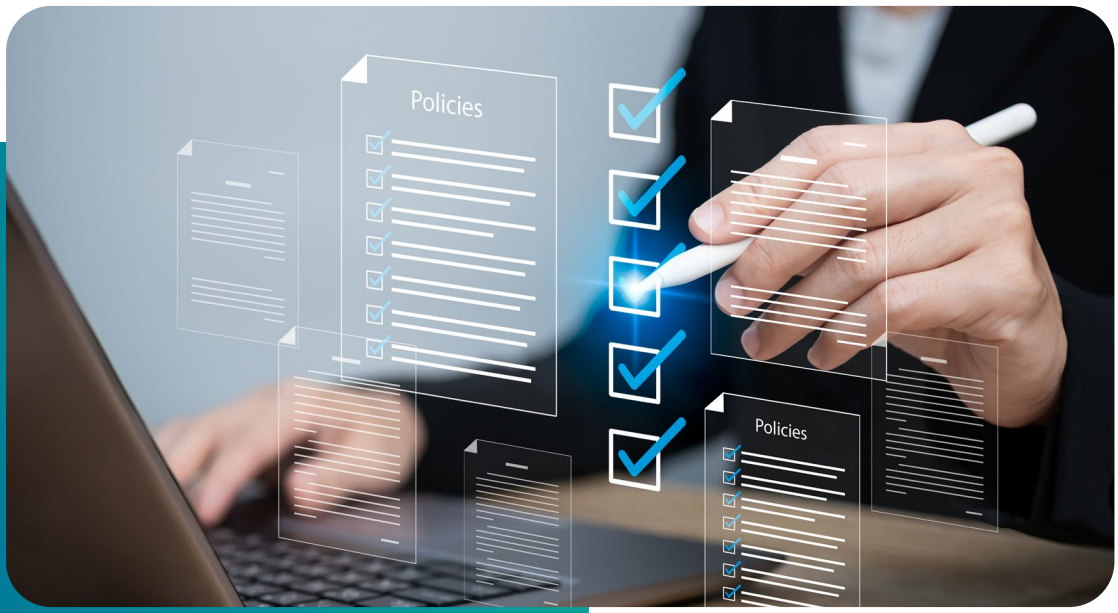
These periodic compliance testing and assessments will aid in long-term security and regulatory adherence while ensuring effective governance with all ICT risk management activities.

Methodology

To determine the readiness of financial product lines for compliance with the EU Digital Operational Resilience Act (DORA), Skillcast analysed over 270 leading UK companies across nine financially regulated sub-sectors using verified third-party data.

Key factors analysed included FCA fines and complaints, ICO complaints and the number of cybersecurity incidents reported, the number of firms registered to Cyber Essentials Plus, and whether the firms had operations in the EU.

Each factor was then assigned a weighted score depending on its direct impact on operational resilience, with the scores normalised to create an overall readiness index score out of 105. This enabled Skillcast to identify the industries most prepared for DORA and which ones are at significant risk of non-compliance.



skillcast

About Skillcast

Skillcast helps companies to create compliance awareness and inspire their employees to act with integrity. We offer bespoke e-learning content development, libraries of ready-made courses and a digital platform specifically built for compliance training. Over 1,400 companies use our digital products to deliver millions of learning interventions each year.

To start your free trial

Call us on +44 20 7929 5000

Visit www.skillcast.com/free-trial

Or scan the QR code below