DORA360
A Gieom Solution

7 MYTHS ABOUT DORA COMPLIANCE

DORA360.AI

gieom

DORA myths explained

Despite growing regulatory fatigue within the financial services sector new operational resilience regulations keep coming, thick and fast.

Operational resilience is a major focus of regulators, globally through the Basel Committee on Banking Supervision (BCBS), in Australia through the APRA Prudential Standard CPS 230, in the UK through new rules from the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA), and in the European Union (EU) through DORA.

DORA, the Digital Operational Resilience Act, raises the bar on digital resilience while the BCBS principles, APRA standard and the new post-Brexit, post-COVID UK regime seek to improve resilience more generally across organisations.

The crux of the regulatory focus on resilience is that disruption is inevitable.

Operational resilience equips firms to manage operational disruptions effectively, through adaptions and contingency plans, thereby avoiding negative impacts on consumers, firms and markets.

We speak with firms falling within scope of DORA every day. We are alarmed to hear many commonly shared views that in reality are dangerous myths, perpetuated through misunderstanding or misinformation. Not only are these myths jeopardising the likelihood of these firms hitting the January 2025 DORA compliance deadline, they also have the potential to cause long-lasting harm. Only with the passing of time are mistakes realised – by then it is too late.

In this eBook Gieom's regulatory subject matter experts and Advisory Board members highlight the myths, the risks of believing them and the reality.

THE TRUTH BEHIND THE MYTHS

Contents

03 | MYTH 1
We coped with COVID, so job done on resilience

05 | MYTH 2
DORA is a cybersecurity regulation, so IT and Info Security have it covered

07 | MYTH 3
The DORA deadline may change and, even then, we're under the regulator's radar

09 | MYTH 4
We can run our operational resilience controls off a spreadsheet

11 | MYTH 5
We have all the data we need to conduct DORA scenario testing

13 | MYTH 6
We are ISO 27001 certified, so we are DORA compliant

15 | MYTH 7
ICT Service providers not named on the DORA critical suppliers list don't have to comply

Jimi Hinchliffe
Gieom Advisory Board Member
Follow on LinkedIn

MYTH 1

We coped with COVID, so job done on resilience

One disturbing trend in recent years, which regulators have been aware of, is the belief of some organisations that their relatively smooth handling of the COVID 19 pandemic crisis means they can draw confidence in their resilience. This is a misguided myth that is leading firms down a path of complacency and inaction.

These firms question the need to do any more in response to UK regulations and the EU DORA (Digital Operational Resilience Act). As such, some have adopted a tick-box approach to new regulations rather than using them as an opportunity to improve resilience. Others have done even less.

THE RISKS OF BELIEVING THE MYTH

There are 2 reasons why this is a dangerous myth.

First, COVID was a **slow-burn event.** Firms in the UK and Europe had several months to observe the spread of COVID and observe the measures taken by governments in Asia. When COVID and the measures taken by western governments in response (e.g. lockdowns, travel bans etc.) were implemented, firms had plenty of time to prepare for the disruption and most were able to smoothly shift to remote working, for example. Most types of operational disruptions don't offer this kind of advance notice; they occur suddenly and without warning, not providing the luxury of time to plan and adjust.

Organisations failing to bolster their resilience run the risk of suffering damaging disruption in service and/or compliance that will take time to resolve, thereby increasing both financial and reputational losses, and requiring higher capital allocation.

Second, COVID was a **systemic event**. In other words, all firms were impacted, and as such firms received a much greater degree of tolerance for the inconvenience and harm caused than would normally be the case. However, a typical disruption will be idiosyncratic or impact a small number of firms. In such circumstances there is likely to be much less tolerance – from regulators and consumers – for disruption and poor service.

A typical example of this forbearance was the impact of COVID and the resultant remote working on call centre wait times. These lengthened significantly across the industry during COVID as firms coped with lockdowns, yet because this was a market-wide impact, there was a general acceptance that it was inevitable so couldn't be helped.

Disruption of service and poor service occurring under less extreme circumstances, in more 'normal' times, will undoubtedly impact client experience, increase attrition and in many cases lead to damaged reputation and punitive enforcement actions.

THE REALITY

It is critical that firms **take the new regulations seriously** and don't rely on the relatively smooth experience of COVID to draw a false comfort that everything is fine and there is nothing more to do on improving resilience. Regulators in the EU and UK have provided long implementation windows for their new rules, not out of their generosity, but because they expect firms to take the new rules seriously. Firms are expected to take actions to improve resilience, which may include implementing new systems or replacing critical third parties.

Regulators have emphasised repeatedly the importance of the new rules and we can expect them to take a robust approach to non-compliance – especially given the long implementation windows. Any firm that is not materially compliant with the new rules by the deadlines in 2025 (January for DORA, end March for the new UK rules) and that fails to manage operational disruptions and digital resilience after the deadline, can expect short shrift from regulators. We can expect to see fines and other action against accountable individuals on Boards and in senior management.

Bhavana Mallesh
Chief Technology Officer, Gieom
Follow on LinkedIn

MYTH 2

DORA is a cybersecurity regulation, so IT and Info Security have it covered

The EU Digital Operational Resilience Act (DORA) is designed to enhance the digital resilience of the financial sector. While cybersecurity is a critical component, DORA extends far beyond merely addressing IT security issues. Firms believing the myth that DORA is a cybersecurity regulation risk late and incomplete compliance.

DORA mandates the implementation of comprehensive measures to prevent, detect and respond to a wide array of operational disruptions, encompassing not only cybersecurity threats but also risks related to system downtime, software vulnerabilities, human error and third-party dependencies.

The myth that DORA is solely an IT problem arises from the historical context of cybersecurity regulations, often triggered by high-profile breaches. When the default is to interpret new regulations through a narrow cybersecurity lens, firms are overlooking the broader operational resilience objectives that DORA encompasses. This misunderstanding is compounded by a cultural tendency within many organisations to silo responsibilities, where IT departments focus on security while other departments manage operational resilience.

DORA's focus on ensuring financial institutions can withstand various operational disruptions necessitates collaboration across multiple departments, beyond IT. Effective governance, risk management and operational resilience require business-wide input. The regulation's broader goals also include establishing a unified framework for managing ICT risks, which is essential for maintaining operational continuity in the face of diverse threats, not just cyber incidents.

Information security also relies heavily on frameworks and standards such as ITIL and ISO 27001, which are optional not regulatory requirements, therefore accentuating the need for a unified and thorough approach in order to meet all DORA obligations.

The view that DORA is simply an extension of cybersecurity regulation that must be dealt with by IT and Info Security is clearly a myth.

THE RISKS OF BELIEVING THE MYTH

The recent CrowdStrike incident involving a routine software update caused significant disruptions to around 8.5 million Microsoft Windows devices, illustrating the fragility of IT infrastructure. It was a software patch not a cyberattack. It resulted in an estimated $10 billion in financial damage across various sectors, highlighting the need to prepare for operational resilience in a comprehensive manner, addressing both IT and non-IT related risks.

Viewing DORA solely as an IT issue can lead to lack of accountability across different departments. Operational resilience requires a coordinated effort from IT, risk management, compliance and business operations. If IT is deemed solely responsible, other critical areas may neglect their roles in ensuring resilience – and by the time they realise their responsibilities they will have wasted valuable time needed to prepare for the January 2025 compliance deadline.

Organisations underestimating the range of risks DORA addresses are likely to formulate strategies that are inadequate for managing not just cyber threats, but also other operational risks such as human error, third-party dependencies and system failures.

When focusing compliance efforts narrowly on cybersecurity measures and overlooking broader DORA requirements firms run the risk of non-compliance, leading to significant penalties and even suspension of licence to operate.

A narrow view of DORA can also foster a culture that resists change and collaboration. Employees may feel disconnected from the importance of operational resilience, leading to complacency and a lack of engagement in resilience-building initiatives.

THE REALITY

DORA is a multi-faceted regulation, extending beyond cybersecurity and designed to enhance operational resilience across the entire financial ecosystem. While it addresses information and communication technology (ICT) risks, it aims to ensure financial institutions can withstand, respond to and recover from various operational disruptions.

Key aspects of DORA

- **ICT Risk management:** Frameworks must be established to identify, mitigate and monitor risks associated with information systems and processes.
- **Incident reporting:** Standardised EU-wide incident reporting obligations enhance the ability of financial institutions to respond and cooperate during incidents.
- **Resilience testing:** Regular testing of critical ICT systems is required to detect and address potential disruptions, including conducting penetration tests on live systems.
- **Third-party risk management:** Firms are required to monitor risks posed by the third-party ICT providers their business relies upon.
- **Governance responsibilities:** Accountable senior managers are responsible for ensuring digital operational resilience and implementing adequate protections against ICT disruptions, including cyber threats.

Implementation challenges

- **Categorising contracts:** Existing contracts with third-party ICT providers must be analysed and categorised to establish compliance status and requirements.
- **Standardised procedures:** Monitoring and reporting ICT incidents in a uniform way is essential.
- **Risk-based testing:** Conducting risk-based testing to identify and address potential ICT disruptions is a significant undertaking.
- **Threat detection:** Ensuring that ICT systems can promptly detect and defend against threats is crucial for compliance.

In summary, DORA is a holistic regulation requiring a comprehensive, cross-functional approach to ensure compliance and the effective management of the broad range of risks that DORA encompasses. Those who continue to believe the myth that DORA is a cybersecurity regulation will fall far short of the regulator's expectations.

Andrew Sheen
Gieom Advisory Board Member
Follow on LinkedIn

MYTH 3

The DORA deadline may change and, even then, we're under the regulator's radar

The Digital Operational Resilience Act (DORA) has been a long time coming. DORA proposals were published in September 2020 by the European Union (EU) Commission and the regulation came into force in January 2023. Since then we have seen several public consultations and the delivery of final regulatory technical standards. The compliance deadline is 17th January 2025. The common view that DORA has been sprung upon firms, with little time to comply, is a myth.

Having worked for both regulatory authorities and financial institutions, I am always amazed when firms genuinely believe regulatory deadlines will either be delayed or (more bizarrely) cancelled at the last minute. Is this to hide the fact they have failed to prepare adequately, or do they honestly feel there are grounds for a deadline extension? I am never sure.

Firms have had at least four years to prepare and the vast majority have devoted significant resources and effort to ensuring they are DORA compliant. Extending the deadline would be an affront to those who are working hard to comply on time. It is inconceivable that the EU Commission, EU Parliament and three European Supervisory Authorities will conspire to reward those who have failed to prepare and ensure their DORA compliance.

Some firms are claiming they are too small to be captured by DORA and will therefore fly low under the regulator's radar. This is clearly nonsense. DORA Article 2 (Scope) lists the entities captured by DORA – a list that includes many small firms. The only exemptions are for "very small" enterprises (fewer than 10 employees with annual turnover and/or balance sheet under €2 million) and intermediaries (less than 250 employees and a turnover under €50 million or balance sheet under €43 million).

If you are a captured firm you must be compliant by 17th January 2025, no exceptions. Also, what happens when your business grows and you appear on the regulator's radar? You will suddenly find yourselves in a very difficult (non-compliant) position.

THE RISKS OF BELIEVING THE MYTH

'Deadline deniers' and 'low fliers' cannot argue they had insufficient time to prepare, as the EU has provided a long implementation period for the new requirements, not out of generosity, but because they expect firms to take the new rules seriously. They expect firms to take decisive action to improve their resilience, which may include implementing new systems or replacing critical third parties.

So, what risks are these firms exposing themselves to?

Regulators will respond firmly to all institutions that fail to comply within the deadline. Firms will not wish to be on the receiving end of the regulators if they experience operational disruptions after 17th January that highlight their failure to comply with DORA.

While EU Member States can impose criminal penalties, they have conferred on the competent authorities the power to apply fines and penalties, including:

- **Requiring the cessation of conduct** that is in breach of DORA and ensuring it is not repeated.
- **Requiring the temporary or permanent cessation of any practice or conduct** considered to be contrary to DORA's provisions and preventing its repetition.
- **Imposing any type of sanction, including financial penalties,** to ensure that financial entities continue to comply with DORA.
- **Identifying the perpetrator publicly** and revealing the nature of their breach.
- **Imposing enforcement fines** on critical ICT third-party service providers up to 1% of their average daily worldwide turnover in the preceding business year (considering the gravity and duration of non-compliance, whether it is intentional or negligent, and the level of cooperation of the ICT third-party service provider).

THE REALITY

DORA will apply from 17th January 2025. The oversight activities undertaken by the three European Supervisory Authorities (ESAs) – the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) – will commence on that day.

Laggards in scope must ensure they are compliant by 17th January 2025, or face the wrath of the regulator. The sooner these firms accept that the DORA deadline will not move, they are in scope and they have to comply, the sooner they can get started! It is still possible for firms to achieve DORA compliance and avoid penalties within just four to five months.

The reality is, most laggards will fail to achieve compliance in time without a technology-enabled approach designed to address the nuances of DORA, combined with the specialist knowledge of regulatory experts who can help interpret DORA requirements, formulate effective strategies and implement according to best practices.

The sheer volume of work, heavy lifting and expertise needed to conduct the preparatory steps of conducting gap analysis against the new rules, identifying policies and procedures that need updating and analysing ICT service provider contracts is too vast to contemplate using traditional manual approaches or outdated GRC platforms. And the skill sets needed to accelerate implementation are rarely present in-house.

The good news is that technology, and especially Generative AI, is enabling firms to conduct these analyses much faster, cheaper and more completely, granting you (just) enough time to work with the experts to evidence DORA compliance on time.

Gary Penolver
Chief Technology Officer, Quod Orbis
Follow on LinkedIn

MYTH 4

We can run our operational resilience controls off a spreadsheet

There's nothing wrong with spreadsheets. They have underpinned regulatory compliance since the dawn of time. And they've worked, right? Countless financial institutions have no intention of moving away from this practice. However, the myth that operational resilience controls can be established and monitored effectively using spreadsheets is deep-rooted, dangerous and is putting many financial institutions and their stakeholders at risk.

Compliance and risk professionals have always used spreadsheets to monitor controls and many see no reason to change. Regulators have been satisfied with spreadsheets and, as audits and report collation have become periodic, why should the Digital Operational Resilience Act (DORA) be the catalyst for change?

Here's why. Business is no longer linear and organisations' ecosystems have become increasingly complex. Exponential growth in digitisation has escalated exploitation by cyber criminals and other bad actors whose activity has become increasingly sophisticated.

Not only that, but a multi-faceted approach to managing regulatory compliance is now needed. After the 2008 financial crisis, strict guidelines requiring stringent (often real-time) monitoring were imposed on financial institutions. From 2025, DORA will also require them to ensure they are operating securely for strengthened resilience. Throw into the mix the need to comply with global as well as European regulations, and without doubt the practice of using spreadsheets to monitor compliance and controls has become unsustainable.
DORA spans this increasingly complex business and regulatory environment. Having proactive operational resilience is no longer a case of point-in-time information, gathered over a period of time and inputted onto a spreadsheet.

This is a round peg in a square hole scenario, from both an operational and compliance viewpoint – fitting a linear process into a multi-faceted, complex environment.

Those who continue to believe the myth that spreadsheets are an effective means of monitoring not only DORA, but any other regulatory framework they have to comply with, are blinkered to the complexity of capturing the required information from multiple sources and maintaining it on a spreadsheet.

THE RISKS OF BELIEVING THE MYTH

Without change, many financial institutions cannot comply with DORA. How will they monitor controls and compliance continually if spreadsheets are their only monitoring tool?

Hazards include:

- **Resource burden of manual processes.** Multiple compliance professionals are required simply to monitor DORA on a spreadsheet, because as soon as information is gathered manually it is out of date!
- **Error-prone.** Whether in data entry, formula creation or manual updates, even small mistakes can lead to significant inaccuracies in compliance tracking and reporting completeness.
- **Lack of scalability.** As financial institutions grow and their operations become more complex, the volume of data that needs to be managed for DORA compliance increases. Spreadsheets cannot scale to handle large datasets effectively, leading to inefficiencies and potential monitoring gaps.
- **Weak security.** Spreadsheets are inherently less secure than dedicated compliance monitoring systems. Without adequate security controls the risk of unauthorised access or data breaches rises. Spreadsheet data is easily shared, copied or altered, which is especially concerning given the sensitivity of financial data.
- **Static not dynamic.** Spreadsheets typically require manual updates and do not support real-time data processing or monitoring. DORA compliance requires continuous oversight of various risk factors, which is virtually impossible to achieve with static, manually administered spreadsheets.
- **Inefficiency.** Manual spreadsheet processing consumes valuable time and resources that could be better spent on strategic risk management activities and ensuring critical compliance deadlines are met.
- **Data languishing in silos.** Spreadsheets do not integrate well into IT infrastructure, leading to data silos that make it harder to get a holistic view of operational risks and compliance status.
- **Inadequate reporting.** Generating comprehensive, compliant reporting and defensible audit trails is notoriously difficult when utilising spreadsheets to track changes over time.

THE REALITY

DORA has Articles spanning most of its 5 pillars, which stipulate the requirement for "Continual Monitoring" to ensure resilience:

Sources:

Official Journal of the European Union Regulations
European Commission Supplementing Regulation

For financial institutions to gain a holistic view of operational resilience, monitor controls continually and be alerted to changes in their compliance status they must utilise smart technology and intelligent automations that connect their entire infrastructure. Only then can they provide assurance to key stakeholders that the quality and accuracy of the data they are receiving and reporting on is adequate.

DORA is enforcing much-needed proactivity within financial institutions operational resilience that is simply not possible with ageing spreadsheet processes. Those who continue to believe the myth that it is, and fail to evolve now, will fail to meet DORA compliance obligations.

Antony Bream
DORA Lead, Gieom
Follow on LinkedIn

MYTH 5

We have all the data we need for DORA scenario testing

There is nothing new about financial institutions needing to conduct scenario testing to evidence operational resilience and regulatory compliance – typically utilising synthetic and anonymised data, because live client data can't be shared externally. However, the notion that synthetic data can be used to scenario test across all 5 Pillars of DORA is a myth because the data needed to test third-party risk in a meaningful, realistic way has to be live.

Pillar 1 of the Digital Operational Resilience Act (DORA) is ICT Risk Management. Firms must diligently test the operational resilience, compliance status, financial health, business processes and money laundering/cyber-attack readiness of third-party providers, on an ongoing basis. They need to know how a breach or significant weakness could impact their clients, their business or the financial sector as a whole.

More than 50% of EU financial institutions rely on US-based cloud service providers for business continuity – and we've seen outages. We've also seen the "CrowdStrike effect" – the universal operational resilience impact of a seemingly innocuous, routine software update. And numerous instances of wholesale cybersecurity failures that have been costly and reputationally damaging.

DORA regulators expect firms to be able to resolve operational resilience failures quickly and appropriately, off-board existing service providers if they pose a risk and on-board replacement providers in a controlled and timely manner, without threatening business continuity.

Today, restoring service after a digital operational resilience failure can take days; the monetary impact and disruption caused can be catastrophic. And when a critical supplier fails it can take several years to replace them. Realistic scenario testing is vital because these timescales are unlikely to pacify DORA regulators.

Data changes daily, meaning that only live, dynamic data will suffice. Those who continue to believe the myth that synthetic data will enable realistic DORA scenario testing cannot meet regulators' expectations.

THE RISKS OF BELIEVING THE MYTH

Firms denying the need to source live data to test the digital operational resilience of third-party ICT service providers cannot be accountable for their supply chain.

Their scenario testing is likely to be incomplete and/or inaccurate, putting their business and its stakeholders at risk.

Failure to use the "right" (aka live) data for supply chain scenario testing can result in a raft of damaging outcomes that firms will be keen to avoid:

Regulatory enforcement fines and other harmful sanctions

Punitive personal penalties for accountable senior managers

Reputational damage causing loss of trust, client attrition and a decline in new business

Threats to the welfare of key stakeholders

Concerns over the viability of the business in the future

THE REALITY

Never before have financial institutions had to conduct such extensive third-party risk scenario testing or evidence such tight control over the supply chain. They are poorly equipped to do so.

And never before have ICT service providers had to evidence to financial services clients and regulators that they have operational resilience built in, and processes to act appropriately when incidents arise.

One option is to source the required live data manually. However, this would take a great deal of time, be very costly and seem counterproductive given that specialist data firms can provide instant access to billions of live data points.

The kinds of live, real-time third-party data that is readily available include:

- **Financial health:** Is there any insolvency risk? Have they been involved in a merger or acquisition – or are they likely to be?
- **Operational resilience infrastructure:** Have they (or their onward supply chain) been involved in an operational resilience incident previously? Are they certified for other frameworks and standards, such as NIST, ITIL and ISO?
- **Senior manager risk:** Has there been CEO churn? Are there any Directors with conflicts of interest? What is their background and track record? Has anyone been subject to conduct risk sanctions?
- **Cyber risk:** Have they (or their onward supply chain) experienced a cyber attack in the past? How was that managed? What was the impact? Did this open a back door for bad actors to access client data? Did the CTO resign?
- **Employee retention:** What is the staff turnover rate? Is there excessive retirement or flight risk? Does the firm have robust succession plans?

Only by integrating live data seamlessly with your governance, risk and compliance (GRC) or DORA compliance platform will financial institutions be able to evidence comprehensive DORA coverage and complete oversight of suppliers.

Live, real-time data enables real-world scenario testing that generates meaningful, realistic and assured results. Many firms will undoubtedly discover risks they were previously unaware of, enabling a more proactive approach to safeguarding your business, its senior managers and key stakeholders.

Nicola Cowburn
DORA Strategic Marketing Lead
Follow on LinkedIn

MYTH 6

We are ISO 27001 certified, so we are DORA compliant

Financial institutions and their ICT service providers have gone to great lengths to secure ISO 27001 certification, which validates their commitment to information security. Many also believe the myth that ISO 27001 certification makes you DORA compliant. It does not.

ISO 27001 certification is much prized among financial institutions and their ICT service providers, not least because it was once considered a competitive advantage. Still considered to be a high value accolade, ISO 27001 has become a check box that many firms must tick to be able to win new business or retain existing clients. DORA compliance is likely to follow in the same vein, in coming years.

While ISO 27001 is an optional information security standard, the Digital Operational Resilience Act (DORA) has operational resilience at its core and compliance is mandatory. Therein lies the fundamental difference between the two.

No doubt, firms that have secured ISO 27001 certification will have a head start on DORA compliance versus those that have not. However, ISO 27001 is narrower in scope; different processes, controls and practices are required to address the unique nuances of DORA.

Believers of the myth that ISO 27001 certification is akin to DORA compliance are jeopardising the welfare, reputation and continuity of their business.

THE RISKS OF BELIEVING THE MYTH

Firms harbouring the misguided belief that ISO 27001 makes them DORA compliant will fail to meet regulators' expectations and will be prone to significant financial and operational sanctions.

DORA emphasises the role of accountable senior managers in overseeing operational resilience, requiring them to monitor, approve, review and set the direction for initiatives needed to ensure compliance. DORA has much broader reach than ISO 27001; failure to ensure that DORA compliance measures are complete, robust and defensible could render senior managers personally liable, facing sanctions for non-compliance.

Ultimately, it will be customers who suffer most due to the DORA compliance gaps caused by firms relying on ISO 27001 to solve operational resilience challenges.

THE REALITY

ISO 27001 certified firms have a bedrock of systems and processes in place to evidence information security and compliance, so are better positioned to augment them as new regulations emerge.

They already have a strong focus on risk management, with a raft of controls already in place, which bodes well for DORA compliance. The task of identifying gaps between current and target states will be quicker, easier and less costly for these firms than their non-certified peers.

Also worth a mention is ISO 27002, a set of best practices and control objectives that encompasses "key cybersecurity aspects" like human resource security, incident response, user access controls and crypto. ISO 27002 addresses some areas of DORA not covered by ISO 27001 – but by no means all – and currently no certification is available.

Firms relying on ISO 27001 for DORA compliance are exposed in 4 key areas:

- **Continuous compliance and monitoring –** DORA compliance is not a one and done effort. Its requirement for ongoing Business Continuity Management (BCM), as a matter of course as well as during an incident, is not addressed by ISO 27001. Although the standard does touch on some elements of BCM, ISO 27001 has no requirement for the implementation and ongoing maintenance of BCM processes and there is no provision for real-time, continuous business continuity. Firms must implement robust systems to continuously track compliance and performance, which goes beyond the periodic review requirements of ISO 27001.

- **Regular testing and updates –** Unlike ISO 27001, which requires vulnerability management only, DORA imposes an unprecedented level of security and threat-led penetration testing. Resilience testing of ICT tools and systems must be performed at least annually, and threat-led penetration at least every 3 years. As a result, the current routines, processes and controls used by most financial institutions are likely to fall short of DORA standards.

- **Third party risk management (TPRM) –** DORA's requirement to analyse and evidence the compliance status of all critical third-party ICT service providers has created a jaw-dropping supply chain risk management (SCRM) challenge. Financial entities must be prepared with exit strategies if required, and ICT service providers must be ready to come under financial services regulatory scrutiny. ISO 27001 and 27002 have an internal information security management focus and do not define any process for assessing or monitoring third party risk, so this is uncharted territory for most firms.

- **Incident management and reporting –** The scale and timescales of DORA incident reporting necessitate a wholesale overhaul of incident management processes for many firms. Incidents classified as "major ICT-related incidents" must be reported to competent authorities without delay: initial notifications must be submitted within 4 hours of classification (maximum 24 hours of discovery), the intermediate report (and tracking updates) within 72 hours and a final report within one month of the cause being identified. ISO 27001 defines notification procedures that are inadequate from a DORA perspective. The challenge is to facilitate seamless incident handling and reporting for DORA without compromising the security protocols established by ISO 27001.

While ISO 27001 offers a sound start-point and clear headwind for firms required to meet the DORA compliance deadline, there is no truth in the myth that ISO standards can be relied upon to deliver DORA compliance in entirety.

Vinod Menon
Chief Product Officer, Gieom
Follow on LinkedIn

MYTH 7

ICT Service providers not named on the regulator's DORA critical suppliers list don't have to comply

The EU's Digital Operational Resilience Act (DORA) has a number of unique characteristics, not least it's scope, which is Europe-wide and includes the resilience of ICT service providers as well as the financial institutions they serve. Many firms believe the myth that ICT service providers not cited as 'critical' on the regulator's list don't have to comply. Nothing could be further from the truth.

DORA will take effect on January 17th, 2025. The Act's aims include ensuring the financial soundness of firms as well as guaranteeing they can maintain resilient operations during severe disruptions caused by cybersecurity threats and information and communication technology (ICT) issues.

Although DORA was primarily designed for financial institutions, its impact also extends to ICT service providers supporting the financial sector. DORA regulations apply directly to ICT providers under regulatory supervision when they are classified as critical ICT third-party service providers.

A 'Critical ICT Third Party Service Provider (TPSP)' is defined according to criteria laid out within DORA Article 31, paragraph 2. These criteria include the extent and nature of the financial sector's reliance on the ICT TPSP, the importance of the services provided, the potential impact of any disruption and the interconnectedness of these services with other critical operations.

The designation of 'critical' status is issued by the European Supervisory Authorities (ESAs) – specifically, the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA), through a joint committee based on recommendations from the Oversight Forum.

Many ICT providers believe the myth that the direct impact of the regulation affects only firms officially designated as critical ICT TPSPs, typically the largest ICT service providers, and does not extend to those not named on this official designated list.

Many also hold the misguided belief that only ICT TPSPs based in Europe have to comply with DORA, when it is the location of their financial services client that determines their regulatory obligations.

THE RISKS OF BELIEVING THE MYTH

This narrow view overlooks the broader indirect implications of DORA, which also impose significant obligations on ICT providers through the financial entities they support. As a result, some providers may not fully appreciate the extent of their responsibilities under the regulation and could face high-impact consequences, including:

- **Losing contracts** with financial entities
- **Falling out of compliance** with regulatory requirements and incurring financial penalties
- **Being replaced by competitors** who meet the new DORA standards, when others don't
- **Experiencing a reduction in market share** due to diminished business opportunities

Each of these outcomes can have significant implications for an ICT provider's reputation, revenue and long-term viability.

THE REALITY

Whether an ICT service provider is on the officially designated critical list or not, any third party (or onward supplier) that is critical to a financial entity's operational resilience must be assessed and monitored to ensure operational resilience.

DORA regulates the obligations of ICT providers in two ways: directly and indirectly.

The Act holds financial entities directly responsible for managing activities related to ICT TPSPs, including onboarding, due diligence, auditing, monitoring and regulatory reporting. It also requires financial entities to incorporate mandatory contractual provisions with each provider to ensure compliance with these requirements.

The extent of their obligations is defined by the financial entity's internal policies for enforcing DORA and the terms of the agreement between them. ICT providers are required to implement various checks and balances and assist the financial entity according to the contractual arrangements made.

DORA's Regulatory Technical Standards (RTS) provide a detailed set of guidelines for financial entities to manage risks associated with ICT third-party service providers, including:

Under DORA, financial entities may only contract with ICT TPSPs that adhere to specified standards. Existing contracts may need to be amended or supplemented with the clauses required by DORA. These additional obligations could lead to increased costs for ICT services, depending on how they are regulated in the agreement.

ICT service providers should evaluate how DORA will affect their operations without delay and prepare accordingly. This involves understanding the specific requirements of DORA, such as adherence to stringent information security standards, assessing the compliance status of critical third parties and potentially making changes to contractual agreements.

Providers should expect to face heightened scrutiny and more frequent audits from financial entities, which will be assessing compliance with DORA's regulations. Preparing in advance will help mitigate risks, adapt to new compliance requirements and manage any potential increase in operational costs or administrative burdens associated with these heightened scrutiny measures. It will also help to create competitive advantage.

Why choose DORA 360 from Gieom?

Gieom specialises in financial services operational resilience and risk management.

We partner with more than 120 global financial services organisations to help manage their operational resilience, risk management and compliance – faster, smarter and more cost-effectively.

Underpinned by Gieom's award-winning Operational Risk & Resilience Platform, DORA 360 is a purpose-built RegTech solution that leverages the power of AI to address the nuances of the EU Digital Operational Resilience Act (DORA).

We have colleagues and customers in three continents, proven implementations, stand-out technology, unrivalled functionality and world-class support services.

Download our brochure.

5 BIG REASONS TO CHOOSE DORA 360

About Gieom

Founded 2012 | 100% focus on operational resilience | 120+ financial services clients
Global reach, local presence | Specialist partner ecosystem | ISO 27001 & ISO 9001 certified

Europe
Aislinn McKibbin
aislinn.mckibbin@gieom.com
+44 (0)7785 770 354
+31 6 332 59602

UK & Europe
Antony Bream
antony.bream@gieom.com
+44 (0)7880 796 403

CONTACT@DORA360.AI
WWW.DORA360.AI

© 2024 Gieom Business Solutions Pvt. Ltd. All rights reserved. Version 2.0.

gieom