QUADRANT
LAW GROUP

BRIEFING

May 12, 2025

Stress-Testing Cyber Resilience under DORA

Preparing Global Financial Firms for Ransomware and Data Breach Regulations

EXECUTIVE SUMMARY

- Resilience—the ability to recover and restore operations after a disruption—is the emerging cybersecurity standard for the financial system.
- U.S. and EU regulators are implementing new frameworks that prioritize resilience over prescriptive technical requirements.
- Under DORA, ICT vendors who provide critical services to European financial entities are now held to a new set of cybersecurity standards.
- Stress-testing critical ICT services and rehearsing incident response plans are likely to become key indicators in regulatory examinations.

203 N. La Salle St. Suite 2100, Chicago, IL 60601

Stress-Testing Cyber Resilience under DORA

Preparing Global Financial Firms for Ransomware and Data Breach Regulations

Jake Vollebregt
Partner, Quadrant Law Group, LLP

Banks, broker-dealers, investment advisers, and asset managers face a relentless barrage of cyberattacks and sensitive data breaches. To protect the financial system from these threats, U.S. and EU regulators have steadily introduced new rules for managing sensitive data and third-party ICT services, the latter of which currently represent weak links in the financial system. These rules are aimed at promoting resilience, the new and critical benchmark for cybersecurity. Resilience standards require financial entities to not only prevent and respond to cyber threats, but also to ensure rapid recovery of critical operations through scenario-based testing and adaptive risk management frameworks.

The Shifting Cybersecurity Landscape

"Resilience standards require financial entities to not only prevent and respond to cyber threats, but also to ensure rapid recovery of critical operations through scenario-based testing and adaptive risk management frameworks."

Once solely the concern of IT departments and management teams, cyberattacks have escalated to the point of becoming standing boardroom priorities and persistent risks to the banking and finance industries. In 2024, the FBI's Internet Crime Complaint Center (IC3) registered 67 new ransomware variants, including FOG, Lynx, Cicada 3301, DragonForce, and Frag, and reported $16.6 billion in losses occurred due to internet crime, a 33% increase from 2023.[1] Among the major targets of recent ransomware attacks are banking and finance firms such as loanDepot, Patelco Credit Union, Prudential, Bank of America, EquiLend, and Evolve Bank & Trust.[2] The following are a few examples of other recent cyber incidents:

- In November 2023, Bank of America's ICT vendor InfoSys McCamish Systems experienced a ransomware attack, resulting in the breach of 57,000 customers' sensitive personal data and account information.[3]
- In July 2024, CrowdStrike rolled out a software update containing a serious flaw that disrupted critical operations across multiple economic sectors, causing an estimated $1.29 billion in losses to Fortune 500 companies in the banking and finance industry (approximately $71.84 million per company).[4]
- In January 2025, a threat actor exploited a vulnerability affecting Oracle Fusion Middleware and Oracle Access Manager,[5] accessed the production environments of Oracle's Cloud Classic (Gen1), and subsequently exfiltrated 6 million records containing sensitive data affecting 140,000 tenants.[6]
- In April 2025, the Office of the Comptroller of the Currency (OCC) notified Congress that it identified a major incident involving a breach of the OCC's Microsoft e-mail system.[7]

These incidents jeopardize the sensitive data of millions of customers and employees, create legal risks; prompt regulatory action; and cause reputational fallout. Regulators are responding to the growing frequency and complexity of disruptions by adopting new standards for ICT services and stepping up enforcement actions.

Prioritizing Resilience for Global Financial Entities

Until recently, technical tools, defense measures, and risk management frameworks were prescribed as the first line in defending against cyberattacks and preventing data breaches. For example, firewalls, encryption, multifactor authentication, and rapid patch updates are all essential defenses. As cloud services and innovative technologies become standard in the rapidly evolving technology and finance sectors, regulators have determined that traditional cybersecurity approaches are no longer sufficient.

Instead of prescribing an ever-evolving set of technical tools and defensive measures in response to ICT incidents, regulators in both Europe and the United States have adopted resilience—the ability to restore operations quickly after a disruption—as the new cybersecurity standard. As a result, financial entities are now expected to prioritize resilience to avoid crippling losses, maintain customer trust, and meet the expectations of auditors and regulators.

EU Resilience Standards under DORA

To shift to a resilience-focused approach the European Council adopted the Digital Operational Resilience Act (Regulation (EU) 2022/2554) (DORA), which became enforceable on January 17, 2025. The Act provides European financial entities with a roadmap for resilience-focused contract provisions with their ICT vendors. It also requires European financial entities, including the European affiliates of non-EU entities, to establish and maintain comprehensive risk management, periodic stress testing, rapid incident reporting, and oversight of their ICT vendors.

"A Lead Overseer can even take action against ICT vendors located outside the EU by auditing and inspecting facilities and property used to deliver the ICT vendor's services within the EU's jurisdiction."

Enforcement of DORA

DORA's enforcement is delegated to the European Supervisory Authorities (ESAs*), which include each financial sector's respective regulator. These are the* European Banking Authority (EBA)*, the* European Insurance and Occupational Pensions Authority *(*EIOPA*), and the* European Securities and Markets Authority (ESMA).[8] DORA grants broad enforcement powers to ESAs and National Competent Authorities (NCAs). NCAs include BaFin, ACPR, and Banc D'Italia. DORA authorizes competent authorities to investigate, audit, prescribe remediation, and impose penalties on regulated financial entities and critical ICT vendors. For example, ESAs can audit a financial entity's ICT service agreements for information security requirements, service levels, use of subcontractors, service locations, security training, and penetration testing.

Among other things, financial entities have begun assembling and submitting registers of information to ESAs and NCAs to support monitoring and supervision and incorporating DORA into their internal and external audits in preparation for the close of the fiscal year. ESAs will review financial entities' registers of information to identify systemic dependencies and assess the impact a service outage would have on Europe's financial system. ESAs will then use these assessments to designate critical ICT vendors and establish oversight programs.

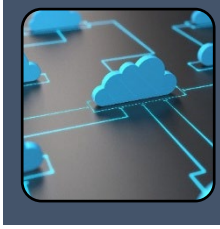
Regulation of Critical ICT Vendors

An ESA can be designated as "Lead Overseer" over a critical ICT vendor. As Lead Overseer, the ESA has additional powers to investigate, inspect, and require cooperation from a critical ICT vendor directly.[9] A Lead Overseer can even take action against ICT vendors located outside the EU by auditing and inspecting facilities and property used to deliver the ICT vendor's services within the EU's jurisdiction.[10] Non-compliant ICT vendors are subject to periodic penalty payments of up to 1% of the average daily worldwide turnover calculated based on the ICT vendor's prior fiscal year.[11] These fines can be imposed on a daily basis for up to six months until compliance is achieved.[12]

When does DORA apply?

Since DORA's enactment, financial entities and their ICT vendors have been creating business processes for ongoing compliance. Financial entities are required to submit registers of information (a prescribed format) with information about their use of ICT services. Financial entities that operate in the European Union can use the following screening questions to assist the business, contracting and procurement staff, and legal reviewers in determining whether DORA applies and which clauses are needed:

1. Is this an ICT service?



"Does this engagement include any information or communication technology services?"

To identify in-scope ICT services, the business, with support from the financial entity's contracting and legal teams, can evaluate the service with the following questions:

- Does the service involve the transmission, hosting, or processing of data?
- Does it rely on computer software or hardware?
- Is the service accessed by the financial entity's users via the cloud or other electronic networks?
- Could an outage or breach of servers or other digital components impact the financial entity's affiliates, customers, or operations?

2. Is this ICT Service subject to DORA?

"Will the ICT service support the financial entity's business activities in Europe?"

The financial entity's subject matter experts (SMEs) can use the following questions to evaluate whether the ICT service is subject to the EU's jurisdiction and regulatory supervision:

- Does the data relate to the financial entity's European customers?
- Would a breach or outage affect the firm's European operations or the EU's financial system?
- Do employees of a European financial entity or an affiliate use the service?

If the ICT service is subject to DORA, the financial entity will need to incorporate clauses under Article 30(2). As other jurisdictions continue adopt similar resilience standards, establishing a nexus to the EU will become less relevant.

3. Does this ICT service support CIF?

"Does the ICT service materially underpin one of the financial entity's critical or important functions (CIF)?"

The financial entity can use the following questions to evaluate the ICT service's materiality and whether it is CIF-supportive:

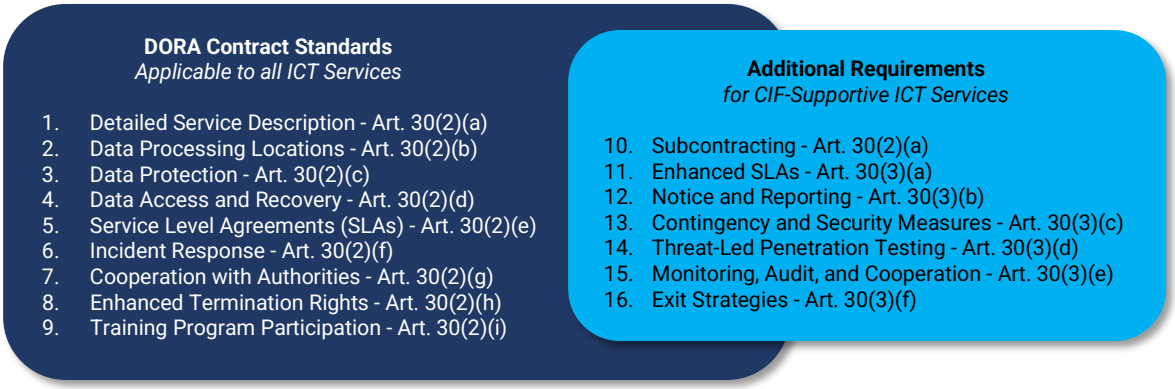
- Is the service essential to day-to-day operations of the firm or one of its core businesses?
- Do the financial entity's customers directly interact with the service?
- Does the service process sensitive information, such as confidential information belonging to the financial entity or sensitive personal information of its customers?
- Could a breach or outage of electronic/information components disrupt the financial entity's business operations?
- Could the financial entity continue normal operations if the service faced a breach or outage?

CIF-supportive ICT services need to be reported in the financial entities register of information and brought into compliance with DORA Article 30(3).

The questions above can elicit dialogue and leverage cross-functional expertise (business, security, privacy, legal, etc.) to evaluate and categorize services. Over time, this will help develop internal processes and controls for the ICT services and the types of data they process. This practice also supports reporting obligations, such as the financial entity's register of information, audits, and examinations. ESAs will use this information to identify critical ICT services.[13]

DORA Remediation and Contract Uplift

DORA prescribes contract provisions with ICT vendors and specific administrative and technical standards for resilience against cyber incidents. Consequently, financial entities are engaging in a two-pronged effort to comply with DORA. First, they are reviewing their ICT service agreements and negotiating amendments with the ICT vendors where necessary. Second, they are establishing new processes and controls to ensure their ICT services comply with DORA. Proactive vendor outreach, market-standard contract templates, and a structured screening process will help achieve compliance and minimize operational friction. The Act requires Europe's financial entities and their ICT vendors to include specified topics in their service agreements:



For CIF-supportive ICT services, DORA prescribes additional protections, such as subcontractor risk management, penetration testing, audit rights, and transition planning. Financial entities can balance thoroughness and efficiency by embedding resilience standards into their vendor agreement templates, onboarding questionnaires, and service evaluations. If a vendor's standard service agreements lack resilience clauses required by DORA, financial entities will be expected to incorporate standard contractual clauses developed by public authorities[14] or otherwise approved by legal counsel. Sample inventory checklists are available on pages 12 and 13.

U.S. Resilience Standards

"Like DORA, these standards emphasize proactive testing and recovery to prepare financial entities and their ICT vendors to respond to and recover from ransomware attacks, data breaches, and service outages."

Similar to their European counterparts, U.S. authorities like the OCC, the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC), the Federal Financial Institutions Examination Council (FFIEC), the Securities and Exchange Commission (SEC), and Financial Industry National Regulatory Authority (FINRA) have gradually transitioned from a risk-based approach to resilience-focused guidance and enforcement standards for the U.S. financial system. The FFIEC is a U.S. interagency body representing the FRB, FDIC, OCC, National Credit Union Administration (NCUA), Consumer Financial Protection Bureau (CFPB), and other regulators in maintaining examination standards and guidance for banks and depository institutions.

The FFIEC has adopted several cyber resilience measures for supply chain management into its examination handbooks. For depository institutions, this is outlined in the FFIEC's 2020 interagency paper, "Sound Practices to Strengthen Operational Resilience."[15] Like DORA, these standards emphasize proactive testing and recovery to prepare financial entities and their ICT vendors to respond to and recover from ransomware attacks, data breaches, and service outages.

Here are some examples of how U.S. regulators are prioritizing digital resilience:

Operational Resilience

- In 2020, the OCC, FRB, and FDIC issued an interagency paper on standards for operational resilience for U.S. banks, including effective governance, information security, and reporting obligations.[16] The paper reflects on disruptive technology failures arising from third-party ICT vendors. Rather than prescribing specific measures to minimize disruptions altogether, the paper prioritizes operational resilience as an approach to manage cyber risks by mitigating the adverse effects of disruptions and recovering as quickly as possible.

- In 2023, the SEC reopened comments for proposed new rules requiring investment firms to implement policies and procedures for mitigating and disclosing cyber risks.[17]

- The Cybersecurity and Infrastructure Security Agency (CISA) is preparing sector-specific goals for the financial services industry and expects to publish in late 2025.[18]

ICT Vendor Management

- In 2015, FINRA noted the rising prevalence among financial service providers of relying on ICT vendors to process sensitive information and highlighted the importance of exercising strong due diligence across the lifecycle of vendor relationships.[19]

"This data enables FINRA to identify systemic interdependencies among critical ICT vendors and evaluate whether these dependencies impede its ability to effectively supervise its members."

- In 2023, FINRA issued a questionnaire regarding its members' use of ICT vendors, generative artificial intelligence (AI), and large language models.[20] This data enables FINRA to identify systemic interdependencies among critical ICT vendors and evaluate whether these dependencies impede its ability to effectively supervise its members.

- In 2023, the SEC proposed a set of updates to Regulation Systems Compliance and Integrity (Reg SCI).[21] Reg SCI originally took effect in 2015 to strengthen the technology infrastructure of exchanges, clearing agencies, and alternative trading platforms (SCI entities).[22] The proposed changes—which large broker-dealers and cloud service providers generally oppose—expand Reg SCI's scope to include large broker-dealers, require SCI entities to manage and oversee ICT vendors, and to maintain business continuity and disaster recovery testing requirements.[23] While Reg SCI focuses on SCI entities, it also affects banks, fintechs, and ICT vendors who rely on these systems for trading and settlement.

- In 2024, the SEC published updates to Reg S-P, which require financial entities to ensure their ICT vendors have adequate controls to protect customer information, an incident response plan for breaches or vulnerabilities, and audit rights to ensure compliance. Depending on their size, financial entities have a compliance period of 18 to 24 months following August 2024 in order to implement the new requirements.

Information Security

- In 2021, the SEC imposed fines on several broker-dealers and advisers for violating Safeguards Rule 30(a) of Reg S-P and issuing misleading breach notifications to their clients.[24] Reg S-P was adopted in 2000 as an implementation of the Gramm-Leach-Bliley Act, which requires financial entities to safeguard customers' nonpublic information. The SEC found that the financial entities failed to implement adequate policies and security measures, including multifactor

authentication for e-mail accounts, between 2017 and 2021. As a result of these failures, more than 10,000 customers' sensitive personal information was compromised.

Incident Response

- In 2021, the OCC, FRB, and FDIC published the Computer-Security Incident Notification Final Rule.[25] The rule took effect in 2022 and requires banks to notify their regulators no later than 36 hours after determining that a computer-security incident has disrupted or degraded—or is likely to materially disrupt or degrade—banking operations or services.[26]

- In 2023, the SEC promulgated various rule changes requiring the boards and management of public companies to disclose their processes for assessing, identifying, and managing cybersecurity risks (17 CFR Parts 229, 232, 239, 240, and 249). The requirements for ongoing incident reporting and cybersecurity disclosures in annual reports have been in effect since December 2023.

Inspection and Audit

"Therefore, contracts should describe the types and frequency of audit reports the financial entity is entitled to receive from the ICT vendor (for example, SOC reports, Payment Card Industry (PCI) compliance reports, or other financial and operational reviews)."

- In 2022, the SEC updated Rule 17a-4 to permit audit-trail systems on modern cloud-based databases. The longstanding Rule 17a-4 requires broker-dealers to preserve all records for a period of 6 years, and to make them easily accessible for review and regulatory audit.[27] Subsection (f)(3)(vii) allows broker-dealers to maintain records electronically with banks and ICT vendors, and requires regulators to have direct access to records upon request. If the bank or ICT vendor fails to either preserve or produce records during an audit, the broker-dealer could face penalties. This rule indirectly causes other entities to align with SEC standards, especially when a ransomware attacks compromise security and the ICT vendor agreement accounts for these obligations, which promotes third-party resilience.

- In 2023, the FRB, OCC, and FDIC issued new guidance on managing third-party vendor risks.[28] This guidance requires financial entities to incorporate contract provisions—where appropriate according to the risk and complexity of the ICT service—entitling them to periodic, independent audits of the ICT vendor and its relevant subcontractors. Therefore, contracts should describe the types and frequency of audit reports the financial entity is entitled to receive from the ICT vendor (for example, SOC reports, Payment Card Industry [PCI] compliance reports, or other financial and operational reviews). Such contract provisions may also reserve the banking organization's right to conduct its own audits of the ICT vendor's systems, subcontractors, and processes.

Business Continuity

- In 2022, FINRA issued a Regulatory Notice acknowledging the proliferation of increasingly complex and sophisticated ransomware incidents.[29] The notice urged financial entities to evaluate and test their ICT vendors' cybersecurity controls and ability to protect sensitive data. Regulatory Notice 22-29 noted that disruptions and outages caused by ransomware are subject to FINRA Rule 4370's requirements for Business Continuity Plans, and that ransomware payments could implicate sanctions and anti-money laundering (AML) violations.

- In its 2025 FINRA Annual Regulatory Oversight Report, FINRA noted the increase in ransomware attacks and outages affecting ICT vendors and reiterated financial entities' obligations to monitor and supervise their ICT vendors. [30] The report offered best practices for developing third-party

risk management programs and processes for ICT vendors and acknowledged emerging AI risks and trends. To illustrate, the report cites FINRA Rules 3110 and 4370, which require broker-dealers to establish supervisory compliance and risk management systems, maintain business continuity plans to account for disruptions to operations, and monitor critical third-party dependencies.

> *"U.S. regulators are following a third-party oversight model similar to DORA by holding financial entities accountable for their ICT vulnerabilities and failures."*

The initial examples of recent cyberattacks given above, particularly the Bank of America ICT vendor breach in 2023 and SEC enforcement for e-mail breaches in 2021, affect financial entities and ICT vendors who would not ordinarily be subject to direct regulatory oversight. By implementing rules like the Computer-Security Incident Notification Rule, Rule 17a-4, Reg SCI, Reg S-P, and FINRA Rules 3310, 4370, and 4511, U.S. regulators follow a third-party oversight model similar to DORA by holding financial entities accountable for their ICT vulnerabilities and failures.

Below are some additional theoretical scenarios where an ICT vendor's failures can have detrimental effects on financial entities and their compliance with a variety of regulatory standards, which—again—demonstrate the need for systemic resilience:

- A data breach that corrupts customer data or a ransomware attack that freezes transaction records at a bank could hinder a broker-dealer's AML monitoring, leading to scrutiny under FINRA Rule 3310.

- A data breach or ransomware attack that disrupts a bank's interface with an SCI entity and has market-wide implications could prompt SEC scrutiny of the bank's cybersecurity practices under broader fiduciary or operational risk management principles.

- If a ransomware attack on a bank disrupts a broker-dealer's ability to process transactions, then the broker-dealer could be investigated under FINRA Rule 4370 and may face legal or contractual fallout for failing to support continuity. This, in turn, could indirectly call upon other financial entities and their ICT vendors to bolster resilience for FINRA members.

- If a bank, fintech, or ICT vendor processes customer data for a financial entity, then a breach could trigger notification and remediation obligations for the financial entity. For example, if the broker-dealer fails to comply with Reg S-P, then a ransomware attack on a bank's systems hosting broker-dealer data could lead to both SEC enforcement and FINRA penalties. Other financial entities could be implicated by cybersecurity, recordkeeping, and AML rules intended to manage ransomware and data breach risks. ICT vendors could face legal and reputational risk if their contracts do not account for responding to ransomware attacks, outages, and regulatory inquiries.

- FINRA Rule 4511 (Books and Records) requires broker-dealers to maintain and preserve records as an application of SEC rules (e.g., Rule 17a-3 and 17a-4). If an ICT vendor stores books and records for a financial entity subject to FINRA Rule 4511 and suffers a ransomware attack or breach, then the broker-dealer could be considered non-compliant. This creates a ripple effect, pressuring other institutions to adopt cybersecurity measures compatible with FINRA regulations. A bank's failure to protect records could lead to fines and other legal and regulatory risks for the broker-dealer.

These examples highlight the cascading effects of third-party vulnerabilities, reinforcing the need for robust ICT vendor oversight and proactive resilience testing. Ransomware and data breaches can trigger compliance failures downstream and affect the broader financial system. This may prompt U.S. policymakers to copy a page from DORA by regulating critical ICT vendors directly.

"This may prompt U.S. policymakers to copy a page from DORA by regulating critical ICT vendors directly."

Evolving Regulatory Standards

Moving forward in parallel with the advent of DORA's enforcement, the OCC, FDIC, FRB, FFIEC, SEC, and FINRA are likely to implement several of their own regulatory updates soon and will likely include the following:[31]

- **Mandatory Resilience Stress testing**: Financial entities will be expected to perform resilience stress testing to evaluate their readiness for ransomware attacks and data breaches. DORA requires scenario-based testing, such as ransomware lockdowns or data exfiltration simulations.[32] The FFIEC is likely to require banks to use similar exercises for testing recovery from encrypted systems or breached databases. These tests would assess backup integrity, response times, and continuity plans, thereby shifting focus from static audits to dynamic resilience.[33] The outcomes of these rehearsals will inform financial entities when they negotiate their agreements with ICT vendors and will affect how ICT vendors compete for their business.

- **Enhanced Third-Party Risk Management**: The EU's oversight of financial entities' use of ICT services is necessary because they are prime targets for cyberattacks and data breaches. U.S. regulators will likely expand existing guidance, mandating ransomware-specific due diligence, malicious code warranties, and contractual recovery guarantees from cloud providers and payment processors.

- **Prompt Incident Reporting and Recovery Standards**: Building on the FDIC's 36-hour rule, regulators may adopt DORA's detailed incident classification, requiring banks to report ransomware or breach impacts on critical operations within hours and to adhere to phased notice and recovery timelines in their SLAs (e.g., immediate notification upon discovery, data restoration within 48 hours, and root cause analysis within 30 days).

- **Sector-Wide Threat Intelligence Sharing**: DORA encourages voluntary data sharing to boost collective resilience. The OCC and FDIC are likely to examine current practices for monitoring, reporting, and sharing anonymized ransomware tactics or breach patterns to strengthen industry-wide defenses. Industry groups like Financial Services Information Sharing Analysis Center (FS-ISAC) can serve as clearinghouses for this information.[34]

Getting Ahead of the Curve

Financial entities that can resolve disruptions resiliently can avoid crippling losses and retain their customers' trust. To adapt to a resilience framework, financial entities and ICT vendors can incorporate the following practices into their risk management programs and contract negotiation standards:

"The FFIEC recognizes tabletop exercises, limited-scale exercises, and full-scale exercises as valid methods for testing continuity and resilience. CISA and FS-ISAC provide tabletop exercise packages with plausible financial industry scenarios."

- **Include Resilience Clauses in ICT Agreements**:
  New ICT services and renewals may require specific provisions. This requires working proactively with ICT vendors to incorporate DORA-compliant clauses and other applicable regulatory

obligations. Critical ICT services will need additional protections, such as CIF-supportive provisions under DORA Article 30(3).

- **Conduct Stress Tests**: Engage cross-functional teams to simulate a ransomware attack that is encrypting core systems or a breach that gains access to customer data to test recovery using offline backups. Coordinate tabletop exercises and rehearsals with crisis management teams. The FFIEC recognizes tabletop exercises, limited-scale exercises, and full-scale exercises as valid methods for testing continuity and resilience.[35] The Cybersecurity and Infrastructure Security Agency (CISA)[36] and FS-ISAC provide tabletop exercise packages with plausible financial industry scenarios.[37]

- **Update Recovery Plans**: Use stress test findings to revise standard procedures and checklists. Define and update ransomware-specific contingencies (e.g., alternative workflows) during outages and breach response protocols, checklists, and notification timelines for customers, data subjects, and government authorities.

- **Assess Third Parties**: Audit vendors for resilience capabilities based on the criticality of the supported operations and the volume and sensitivity of the data they process. This will ensure that the appropriate scrutiny is applied and that contracts do not impose excessive obligations on ICT vendors.

These efforts will aim to deliver advantages by reducing the impact of ransomware attacks and disruptions, as well as fulfilling the expectations of regulators and customers.

Conclusion

Cyberattacks and data breaches along with gaps and failures in ICT vendor systems can disrupt financial entities and undermine consumer trust in the financial system. As a result, financial entities and ICT vendors face growing pressure to comply with OCC, FDIC, FRB, FFIEC, SEC, and FINRA regulations and guidelines, which—much like the EU's DORA—seek to make stress testing the cornerstone of cybersecurity vigilance in the United States. Technology, legal, compliance, and risk management leaders who prioritize resilience as a competitive edge beyond meeting a minimum standard will empower their firms to succeed in a digital world.

For additional information, please contact:

Jake Vollebregt | Partner
Quadrant Law Group, LLP
T +1-949-954-6349
jvollebregt@quadrantlaw.com

Key Terms

Key Term	Definition/Reference
Critical or Important Function (CIF)	A function within a financial entity that is essential to—and "materially underpins"—its core operations or services, such that a disruption could significantly impact its business or customers, as defined under DORA Article 30(3).
Digital Operational Resilience Act (DORA)	A European Union regulation (Regulation (EU) 2022/2554) effective January 17, 2025, mandating financial entities to enhance ICT risk management, stress testing, and oversight of ICT vendors to protect the financial system.
European Supervisory Authorities (ESAs)	Regulatory bodies (EBA, ESMA, EIOPA) responsible for overseeing DORA compliance, including auditing financial entities and critical ICT vendors, with powers to impose penalties and remedial measures.
Information and Communication Technology (ICT) Service	Technology services involving data processing, software, hardware, or cloud-based systems that support financial entities' operations.
ICT Vendor	A third-party provider of ICT services to financial entities, such as cloud service providers or software vendors.
Periodic penalty payments	Daily fines imposed by Lead Overseers on critical ICT vendors for non-compliance with DORA, up to 1% of average daily worldwide turnover for up to six months.
Ransomware	A type of cyberattack where malicious software encrypts a target's systems or data, demanding payment for restoration, posing significant risks to financial entities, ICT vendors, customer data, and financial systems.
Register of Information	A mandatory record maintained by financial entities under DORA, detailing their use of ICT services. Information in the Register is used to identify interdependencies and designate critical third-party ICT vendors.
Resilience	The ability of a financial entity or ICT vendor to anticipate, withstand, recover from, and adapt to cyberattacks, data breaches, or other ICT-related disruptions, as emphasized in DORA and U.S. regulatory frameworks.
Stress Testing	Scenario-based exercises to simulate disruptions like ransomware attacks or data breaches that assess a financial entity's recovery capabilities.
Third-Party Risk Management	The process of assessing and overseeing ICT vendors to ensure their services meet cybersecurity and resilience standards, as required by DORA and U.S. regulations like FFIEC guidance, FINRA rules, Reg SCI, and Reg S-P.

DORA Checklists

Contract Standards for all ICT Services
DORA Article 30(2)

- ☐ **Detailed Service Description** - Article 30(2)(a): Does the contract include a comprehensive description of all ICT services and their functions?
- ☐ **Data Processing Locations** - Article 30(2)(b): Does the contract specify the countries or regions where services are provided and data is processed/stored, with a requirement for the provider to notify the financial entity in advance of a change?
- ☐ **Data Protection** - Article 30(2)(c): Does the contract include provisions to ensure availability, authenticity, integrity, and confidentiality of data, including personal data, in compliance with GDPR and other applicable data protection laws?
- ☐ **Data Access and Recovery** - Article 30(2)(d): Does the contract guarantees access, recovery, and return of personal and non-personal data in an easily accessible format in cases of insolvency, resolution, business discontinuation, or contract termination?
- ☐ **Service Level Agreements (SLAs)** - Article 30(2)(e): Does the contract include detailed SLAs with expected performance and quality of services, and provisions for updates and revisions?
- ☐ **Incident Response** - Article 30(2)(f): Does the contract obligate the ICT vendor to assist during ICT-related incidents at no additional cost (or at a pre-agreed cost) to address disruptions, incidents, or other issues arising from the services?
- ☐ **Cooperation with Authorities** - Article 30(2)(g): Does the contract require the ICT vendor to fully cooperate with the financial entity's regulators?
- ☐ **Enhanced Termination Rights** - Article 30(2)(h): Does the contract define clear termination rights and minimum notice periods for ending the agreement, aligned with expectations of the financial entity's regulators?
- ☐ **Training Program Participation** - Article 30(2)(i): Does the contract include conditions for the ICT vendor's participation in the financial entity's ICT security awareness programs and digital operational resilience training under DORA Article 13(6)?

Other Considerations for Legal Reviewers

- **Proportionality** - Article 4: Apply requirements proportionately based on the nature, scale, complexity, and risk profile of the ICT services and the financial entity.
- **Written Contracts** - Article 30(1): Document all obligations in a single written contract, including SLAs, available in print or electronic format that can be downloaded and retained.
- **Effective Date**: Ensure DORA-related contractual clauses take effect January 17, 2025.

Additional Requirements for CIF-Supportive ICT Services
DORA Article 30(3)

- ☐ **Subcontracting** - Article 30(2)(a): Does the contract indicate whether subcontracting of CIF-supportive ICT services, or material parts thereof, is permitted and under what conditions? Ensure subcontracting conditions comply with regulatory technical standards (RTS) promulgated by the ESAs under Article 30(5).
- ☐ **Enhanced Service Level Agreements** - Article 30(3)(a): Does the contract include comprehensive SLAs with precise quantitative and qualitative performance targets to enable effective monitoring and prompt corrective actions if service levels are not met?
- ☐ **Notice and Reporting** - Article 30(3)(b): Does the contract require the ICT vendor to notify the financial entity of developments that could materially impact service delivery in line with agreed service levels, with specified notice periods?
- ☐ **Contingency and Security Measures** - Article 30(3)(c): Does the contract require the ICT vendor to implement and test business contingency plans and maintain industry standard security measures, tools, and policies to ensure an appropriate level of security consistent with the financial entity's regulatory obligations?
- ☐ **Threat-Led Penetration Testing (TLPT)** - Article 30(3)(d): Does the contract require the provider to participate and fully cooperate in the financial entity's TLPT exercises to assess and strengthen service security pursuant to DORA Articles 26 and 27?
- ☐ **Monitoring, Audit, and Cooperation** - Article 30(3)(e): Does the contract grant ongoing audit, inspection, and monitoring rights?
    - Unrestricted access, audit, and inspection rights by the financial entity, its appointed third parties, and regulatory authorities, with the right to review and retain copies of relevant documentation
    - Full cooperation by the ICT vendor during inspections and audits by competent authorities, the Lead Overseer, or appointed third parties

  Note: If the rights of access would impact the ICT vendor's other customers, include the option to agree on reasonable alternatives, such as certifications and third-party audit reports.
- ☐ **Exit Strategies** - Article 30(3)(f): Does the contract require an adequate transition period during which the ICT vendor will continue providing the services? These provisions should reduce the risk of disruption by supporting seamless resolution and restructuring, and allowing the financial entity to migrate to another ICT vendor or in-house solutions.

Endnotes

[1] Federal Bureau of Investigation. (2025). 2024 internet crime report. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf.

[2] The biggest data breaches of 2024 in financial services. (2024, December 16). American Banker. https://www.americanbanker.com/list/the-biggest-data-breaches-of-2024-in-financial-services.

[3] Adams, A. (2024, February 14). Data breach affects 57,000 Bank of America accounts. American Banker. https://www.americanbanker.com/news/data-breach-affects-57-000-bank-of-america-accounts.

[4] Parametrix. (2024, July 24). CrowdStrike's impact on the Fortune 500. Parametrix Insurance Services. https://www.parametrixinsurance.com/crowdstrike-outage-impact-on-the-fortune-500.

[5] National Institute of Standards and Technology. (n.d.). CVE-2021-35587 detail. National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2021-35587.

[6] CloudSEK. (2025, January). The biggest supply chain hack of 2025: 6M records for sale exfiltrated from Oracle Cloud, affecting over 140K tenants. CloudSEK Blog. https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants.

[7] Office of the Comptroller of the Currency. (2025, April 24). OCC releases bank supervision operating plan for fiscal year 2026 [News release]. https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-32a.pdf.

[8] European Union. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector. Official Journal of the European Union, L 333, 1–79. Recital (7). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.

[9] *Ibid*., Article 35(1).

[10] *Ibid*., Article 36.

[11] *Ibid*., Article 35(8).

[12] *Ibid*., Article 35(7).

[13] *Ibid*., Article 31(2).

[14] *Ibid*., Article 30(4).

[15] Office of the Comptroller of the Currency. (2020, October 30). Sound practices to strengthen operational resilience (OCC Bulletin 2020-94). https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-94.html.

[16] Federal Reserve Board. (2020, October 30). Interagency paper on sound practices to strengthen operational resilience (SR Letter 20-24). https://www.federalreserve.gov/supervisionreg/srletters/sr2024.htm.

[17] Securities and Exchange Commission. (2022, March 9). Cybersecurity risk management for investment advisers, registered investment companies, and business development companies. Federal Register, 87, 13524–13639. https://www.federalregister.gov/documents/2022/03/09/2022-03145/cybersecurity-risk-management-for-investment-advisers-registered-investment-companies-and-business.

[18] Cybersecurity and Infrastructure Security Agency. (n.d.). Cross-sector cybersecurity performance goals. U.S. Department of Homeland Security. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

[19] Financial Industry Regulatory Authority. (2015, February 3). Report on cybersecurity practices. https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

[20] Financial Industry Regulatory Authority. (2025, January 27). 2025 FINRA annual regulatory oversight report: Third-party risk. https://www.finra.org/rules-guidance/guidance/reports/2025-finra-annual-regulatory-oversight-report.

[21] Securities and Exchange Commission. (2023, April 14). Regulation systems compliance and integrity: Proposed rule. Federal Register, 88, 23146–23240. https://www.federalregister.gov/documents/2023/04/14/2023-05775/regulation-systems-compliance-and-integrity.

[22] Securities and Exchange Commission. (2014). Regulation systems compliance and integrity (17 C.F.R. §§ 242.1000–1007). https://www.ecfr.gov/current/title-17/chapter-II/part-242.

[23] Securities and Exchange Commission. (2023, March 15). SEC proposes to expand and update Regulation SCI [News release]. https://www.sec.gov/news/press-release/2023-53.

[24] Securities and Exchange Commission. (2021, August 30). SEC announces three actions charging deficient cybersecurity procedures [News release]. https://www.sec.gov/news/press-release/2021-169.

[25] Office of the Comptroller of the Currency. (2021, November 18). Computer-security incident notification: Final rule [News release]. https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-119.html.

[26] Office of the Comptroller of the Currency. (2021, November 18). Computer-security incident notification: Final rule (OCC Bulletin 2021-55). https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-55.html.

[27] Securities and Exchange Commission. (n.d.). Records to be preserved by certain exchange members, brokers, and dealers (17 C.F.R. § 240.17a-4). https://www.ecfr.gov/current/title-17/chapter-II/part-240/subpart-A/subject-group-ECFR9a3b1ee5e7a78f3/section-240.17a-4.

[28] Office of the Comptroller of the Currency, Federal Reserve Board, & Federal Deposit Insurance Corporation. (2023, June 9). Third-party relationships: Risk management guidance. Federal Register, 88, 37920–37934. https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf.

[29] Financial Industry Regulatory Authority. (2022, December 6). Regulatory Notice 22-29: FINRA reminds firms of their obligations regarding ransomware payments. https://www.finra.org/sites/default/files/2022-12/Regulatory-Notice-22-29.pdf.

[30] Financial Industry Regulatory Authority. (2025, January 27). 2025 FINRA annual regulatory oversight report. https://www.finra.org/sites/default/files/2025-01/2025-annual-regulatory-oversight-report.pdf.

[31] Office of the Comptroller of the Currency. (2024, October 1). Bank supervision operating plan: Fiscal year 2025 [News release]. https://www.occ.gov/news-issuances/news-releases/2024/nr-occ-2024-111.html.

[32] European Union. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector. Official Journal of the European Union, L 333, 1–79. Article 26. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554.

[33] Federal Financial Institutions Examination Council. (2024, August). Development, acquisition, and maintenance. In Information technology examination handbook. https://ithandbook.ffiec.gov/media/m21ni0b3/ffiec_itbooklet_developmentacquisitionmaintenance.pdf.

[34] Office of the Comptroller of the Currency. (2022, July 12). FFIEC cybersecurity resource guide for financial institutions (Bulletin 2022-22). https://www.occ.gov/news-issuances/bulletins/2022/bulletin-2022-22.html.

[35] Federal Financial Institutions Examination Council. (n.d.). Business continuity management: Exercise and test methods. In Information technology examination handbook. https://ithandbook.ffiec.gov/it-booklets/business-continuity-management/vii-exercises-and-tests/viig-exercise-and-test-methods/.

[36] Cybersecurity and Infrastructure Security Agency. (n.d.). Cybersecurity scenarios. U.S. Department of Homeland Security. https://www.cisa.gov/resources-tools/resources/cybersecurity-scenarios.

[37] Financial Services Information Sharing and Analysis Center. (n.d.). Resilience. https://www.fsisac.com/resilience.