PROTEGO
TRUST BANK

Either OR Frameworks

Operational Resilience Frameworks in the EU and US

October 21, 2023

Weiyee In, Chief Information Officer, Protego Trust Bank

Executive Summary

This white paper examines some of the key differences between the European Union's Digital Operational Resilience Act (DORA) and the operational resilience frameworks in the United States, particularly those from the Federal Financial Institutions Examination Council (FFIEC) and other regulatory bodies. It highlights the inconsistencies in approach, scope, and requirements, with a focus on the treatment of Information and Communication Technology (ICT) third-party service providers. This white paper highlights several of the challenges financial institutions will face beginning in January 2025 and the dire need to carefully map the requirements of each framework, develop thoroughly comprehensive and adaptable compliance, security, and data strategies to address the demands of multi-jurisdictional regimes.

- Divergent Approaches and Scope: EU's DORA takes a more prescriptive and focused approach specifically on digital operational resilience, while the US FFIEC guidelines are and have been far broader and more high level principles-based. This divergence creates complexity for institutions operating in both jurisdictions, as they need to navigate and reconcile these different approaches.
- Geographic Scope and Extraterritorial Impact: DORA has potentially significant extraterritorial impact, affecting non-EU entities serving EU financial firms or having a presence in the EU, while US frameworks are generally limited to US-regulated institutions. This creates far greater challenges for global institutions that need to comply with both regimes than many realize.
- Balancing Prescriptive vs. Flexible Approaches: Financial Institutions must balance DORA's more prescriptive requirements with the FFIEC's more flexible, risk-based approach, potentially leading to challenges in creating unified policies and procedures as well the implementations needed in today's digital economy.
- Third-Party Oversight: DORA introduces direct oversight of critical ICT third-party providers by EU regulators, while US frameworks have historically relied more on financial institutions to manage third-party risk through contractual arrangements. This difference in approach requires institutions to maintain different processes for vendor and third-party management in EU and US operations with potentially deep control level granularity into use cases.
- Incident Reporting Requirements: DORA establishes harmonized incident reporting requirements across the EU, while US incident reporting requirements have historically

varied by regulator, type of incident and jurisdictions. These inconsistencies complicate security and compliance efforts for institutions operating in multiple jurisdictions.

- Resource and Expertise Constraints: As highlighted in the FFIEC compliance guide, institutions may face "*resource and expertise constraints, especially for small and medium-sized financial institutions, that may limit their ability to achieve and maintain FFIEC compliance*.[1]" This new challenge is likely exacerbated when trying to comply with both DORA and FFIEC guidelines simultaneously.
- Continuous Adaptation to Evolving Regulations: Both frameworks are evolving, with potential new US regulations indicated by the OCC for the end of 2024 and potential changes due to increases or decreases in regulations after the election this year. Institutions must stay informed about regulatory changes and continuously adapt their compliance strategies.
- Implementation of Technology-Driven Solutions: Both frameworks emphasize the need for robust, technology-driven solutions for security, data governance, risk management, testing, and monitoring. However, beyond best practices across jurisdictions varying, implementation of these solutions across different regulatory regimes becomes complex and resource-intensive.
- Harmonizing Contractual Requirements: DORA specifies mandatory elements for contracts with ICT providers, while FFIEC guidelines are far less prescriptive. Financial Institutions must navigate these differences with vendors and service providers when drafting contracts that comply with one or both regimes.
- Cost and Resource Allocation: Complying with both regimes likely increases costs and requires careful resource allocation to meet divergent standards while maintaining efficient global operations.

Introduction

As financial institutions increasingly rely on digital technologies and third-party services, regulators worldwide are developing frameworks to ensure operational resilience. The EU's DORA and the US frameworks, while sharing common goals and principles, differ significantly in their approaches, creating complexity and deep challenges for global financial institutions. While both DORA and US frameworks aim to enhance operational resilience in the financial sector, their approaches differ significantly, particularly in the treatment of ICT third-party providers. At a very high level, EU's DORA introduces a much more comprehensive and direct regulatory approach, while the US frameworks and standards focus on guiding financial institutions in managing their third-party relationships.

Financial institutions operating globally, therefore, shall need to carefully navigate these differences, developing very involved integrated risk and compliance strategies to meet both EU and US expectations while maintaining efficient operations and resilience. As the regulatory landscape continues to evolve, ongoing monitoring and adaptation will be crucial for ensuring compliance and operational resilience. While the US approach is currently less prescriptive

[1] https://www.ffiec.gov

than those in the UK or EU, financial institutions need to now stay informed about potential regulatory changes and continue to strengthen their operational resilience capabilities in line with existing guidance and industry best practices.

Scope and Approach

The European Union's DORA and the United States' Federal Financial Institutions Examination Council (FFIEC) guidelines represent very distinct approaches to operational resilience in the financial sector. Tailored specifically for financial institutions, including banks, insurance companies, investment firms, and their third-party service providers, both DORA and FFIEC frameworks aim to enhance the industry's ability to withstand and recover from disruptions. However, their scope, focus, and implementation strategies differ significantly, presenting unique challenges for global financial institutions. Beyond The cross over of the Network and Information Systems Directive 2 (NIS2) and the sunsetting of FFIEC CAT further complicate the regulatory landscape.

The focus of regulatory efforts started with the harmonizations of standards and over-arching taxonomies. By pushing forward a unified set of rules across the EU member states, EU DORA aims to standardize cybersecurity practices across the financial sector, facilitating compliance and enhancing overall security measures. However it is important to bear in mind that EU DORA is considered a *lex specialis*[2] for financial entities, meaning its requirements take precedence over overlapping regulations like NIS2 and even US regulations and standards when conflicts arise. EU DORA explicitly states that its provisions concerning information and communication technology (ICT) risk management, incident reporting, and operational resilience testing supersede those outlined in NIS2 for financial entities.

EU Digital Operational Resilience Act (DORA)

This *lex specialis* position obligates financial institutions to adhere to the most stringent standards applicable to their operations and legal provisions tailored to particular circumstances are prioritized, leading to more precise and effective governance. EU DORA takes a targeted approach, focusing specifically on digital operational resilience. As stated in the EU DORA framework, it "*establishes uniform requirements for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics services*"[3]. This includes comprehensive requirements for ICT risk management, incident reporting, operational resilience testing, and oversight of critical ICT third-party service providers. EU DORA focuses specifically on digital operational resilience for the financial sector. It establishes a comprehensive framework with uniform requirements across the EU for:

[2] a legal doctrine that establishes the principle that a law governing a specific subject matter (*lex specialis*) takes precedence over a more general law (*lex generalis*) when both laws apply to the same situation.

[3] European Securities and Markets Authority.. Digital Operational Resilience Act (DORA) Article 1(1

- ICT risk management: DORA mandates that financial entities "shall have in place a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system"[4]. This framework must include strategies for ICT risk identification, protection and prevention, detection, response and recovery, learning and evolution, and communication[5].
- Incident reporting: The regulation requires financial entities to "*establish and implement a management process to monitor and log ICT-related incidents*"[6]. It also stipulates that "*financial entities shall report major ICT-related incidents to the relevant competent authority*"[7], ensuring a standardized approach to incident reporting across the EU.
- Operational resilience testing: DORA mandates that financial entities "*shall maintain a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk management framework*"[8]. This includes various types of tests, such as vulnerability assessments, open-source analyses, network security assessments, and advanced threat-led penetration testing for certain entities[9].
- Oversight of critical ICT third-party service providers: The regulation introduces a novel oversight framework for critical ICT third-party service providers (CTPPs). It states that "*critical ICT third-party service providers shall be subject to an oversight framework*"[10], granting European Supervisory Authorities the power to directly oversee these providers.

For US financial institutions operating in Europe or dealing with EU clients, EU DORA's position as *lex specialis* means they must align their operational resilience strategies with DORA's requirements rather than relying solely on their existing compliance frameworks under NIS or even US regulations, FFIEC or standards such as NIST. This requires significant adjustments in more than their cybersecurity practices and governance structures to ensure compliance with DORA's stringent prescriptive standards. EU DORA effectively requires US financial institutions to comprehensively reassess and potentially overhaul all of their existing policies, procedures, processes and operational frameworks, including risk management and incident response protocols, not to mention TPRM and integrations.

US Frameworks for Financial Institutions

In contrast, the US approach historically, as exemplified by FFIEC guidelines, takes a much broader and philosophically risk based “principled view” of operational resilience. The FFIEC Architecture, Infrastructure, and Operations (AIO) booklet states that it "*focuses on enterprise-wide, process-oriented approaches that relate to the design of technology within the overall enterprise and business structure, implementation of information technology (IT)*

[4] Digital Operational Resilience Act (DORA) Regulation (EU) 2022/2554, Article 5(1)
[5] Digital Operational Resilience Act (DORA) Regulation (EU) 2022/2554, Article 6(1)
[6] Digital Operational Resilience Act (DORA) Regulation (EU) 2022/2554, Article 17(1)
[7] Digital Operational Resilience Act (DORA) Regulation (EU) 2022/2554, Article 19(1)
[8] Digital Operational Resilience Act (DORA) Regulation (EU) 2022/2554, Article 26(1)
[9] Digital Operational Resilience Act (DORA) Regulation (EU) 2022/2554, Article 26(3)
[10] Digital Operational Resilience Act (DORA) Regulation (EU) 2022/2554, Article 31(1)

infrastructure components, and delivery of services and value for customers"[11] The US approach allows for far more flexible implementation based on an institution's size, complexity, industry and risk profile. The FFIEC Cybersecurity Assessment Tool (CAT) further emphasizes this flexible approach, stating that it is "*intended to help institutions identify their risks and determine their cybersecurity preparedness*" [FFIEC CAT].

Another key difference between the US versus the EU approaches is the treatment of third-party oversight. DORA introduces direct regulatory oversight of critical ICT third-party providers, while the FFIEC Third-Party Risk Management (TPRM) guidance places the responsibility on financial institutions, stating that "*a financial institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships*"[12].

For data, DORA also provides a more prescriptive framework. It outlines specific requirements for data governance, data quality, and data protection. The US approach, as outlined in the FFIEC AIO booklet, provides a much higher level and more general guidance on data management, stating that "*management should implement a data governance program to ensure data accuracy, integrity, and availability*"[13]]. EU DORA directly requires financial entities to establish a comprehensive data governance framework. EU DORA Article 9 (1) specifically states: "*Financial entities shall have in place an ICT risk management framework which includes strategies, policies, procedures, ICT protocols and tools that are necessary to effectively protect all relevant physical components and infrastructures, including computer hardware, servers, as well as all relevant premises, data centres and sensitive designated areas, to ensure that all those physical components and infrastructures are adequately protected from risks including damage and unauthorised access or usage*."

Despite these differences, both frameworks maintain common goals of enhancing operational resilience in the financial sector. As the financial landscape continues to evolve, institutions operating globally will need to navigate these different regulatory approaches to ensure comprehensive operational resilience. Again, adding to the quagmire is the emergence and rampant growth of generativeAI and the horde of AI based solutions focused on governance risk and compliance with EU DORA. The key differences between the approaches and regulatory direction will not only create significant challenges for financial institutions in the US, but a number of structural or systemic issues.

Key Differences

[11] Federal Financial Institutions Examination Council. (2021, June 30). Architecture, Infrastructure, and Operations Booklet. FFIEC IT Examination Handbook

[12] FFIEC: Guidance for Managing Third-Party Risk. as published from FDIC https://www.fdic.gov/sites/default/files/2024-03/fil08044a.pdf

[13] Federal Financial Institutions Examination Council, "*Architecture, Infrastructure, and Operations (AIO) Booklet"*, 2021

The key differences between EU DORA and US frameworks revolve around the former's heavier prescriptive approach. These differences shall have significant implications for business operations, security practices, regulatory compliance, and data governance in financial institutions. EU DORA's prescriptive approach requires financial entities to implement specific ICT risk management frameworks and testing procedures. For US financial institutions this will likely necessitate significant and substantial changes (both broad and deep) in policies, procedures, business processes, resource allocation (infrastructure and people), and strategic planning. For instance, because DORA mandates that "*financial entities shall have in place a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system*"[14]. Not suggesting that financial institutions would be lacking these, but most financial institutions have grown or come to the fore through decades of mergers and acquisitions.

While financial institutions work towards a combination of integration and modernization efforts as a result of mergers and acquisitions, often running fundamental or core digital transformation in parallel, these institutions now face additional challenges in achieving EU DORA compliance due to their convoluted, heterogeneous IT environments that today are most likely both hybrid and multi-cloud.

During a merger or acquisition most financial institutions do track and document all information assets and ICT assets, as well as all ICT-supported business functions, but the levels of inventories of ICT assets, including hardware, software, data, and services is rarely consistent and generally far less "well-documented" and down to a level that includes "*policies, procedures and protocols to protect all information and ICT assets*". Merged institutions aside from having heterogeneous infrastructure also have a number of different IT risk frameworks because even the FFIEC CAT is a voluntary assessment tool to help financial institutions identify risks for an inherent risk profile and and determine cybersecurity maturity and preparedness. Moreover with FFIEC CAT being sunsetted and most of the industry first going towards NIST CSF 2.0 (which is less domain specific than FFIEC CAT and applies broadly to organizations of all sizes and industries), focusing on a new "*govern*[15]" function, however, over far fewer outcomes, the gap to meet EU DORA requirements in 2025 widens.

Overcoming Diverging Approaches

The frameworks, NIST CSF 2.0 and EU DORA are both aimed at enhancing cybersecurity, because of their approach and distinct methodologies taking divergent approaches to address digital resilience is catalyzing the cybersecurity industry to evolve with greater alacrity. The introduction of the new "*Govern*" function, marks a significant shift in approach. In fact, one of the key strengths of NIST CSF 2.0 is its flexibility and broader applicability to all industries compared to FFIEC CAT and its Financial Services focused Inherent Risk Profile and

[14] *Digital Operational Resilience Ac*t (DORA) Regulation (EU) 2022/2554
[15] National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Version 2.0 February 26, 2024 added a new "*Govern*" function added to the existing five core functions (Identify, Protect, Detect, Respond, and Recover)

Cybersecurity Maturity. Similarly the CMMI 2.0 focuses on process improvement and maturity levels to improve capability and performance in organizations, but is also broad ands applicable to all industries. While this addition elevates the importance of organizational cybersecurity governance, integrating it as a core component of the framework, consolidating governance-related activities it is nowhere near as prescriptive as EU DORA.

The NIST CSF 2.0 framework and CMMI2 are designed to be industry-agnostic, making it suitable for organizations of all sizes across various sectors, but also effectively driving it towards a lower common denominator approach. This adaptability and flexibility comes with a trade-off as NIST CSF 2.0 provides fewer specific outcomes compared to its predecessors, potentially creating challenges for organizations needing to meet more detailed regulatory requirements. EU DORA, as *lex specialis*, takes precedence over general cybersecurity regulations like NIS2 and even NIST CSF 2.0 in the financial sector in and related to the EU. At its most basic, EU DORA prescribes an additional layer of EU supervision, while NIST CSF 2.0 does not have a direct regulatory enforcement mechanism. Where NIST CSF 2.0, similar to NIS2 is broadly applicable, DORA specifically targets the financial sector, creating potential conflicts for global organizations.

US Financial Institutions may therefore need to bridge the gap between NIST CSF 2.0's broader approach and DORA's specific requirements, potentially necessitating additional frameworks or tools. For example, DORA enforces stringent incident reporting timelines, requiring critical incidents to be reported within four hours, which may not be explicitly covered in NIST CSF 2.0. There have been multiple efforts to create synergies and unify efforts towards reporting that would harmonize incident reporting such as the Financial Stability Board's (FSB) and the Format for Incident Reporting Exchange (FIRE) as a standardized format for financial firms to report operational incidents, including cyber incidents.

Promoting convergence and harmonization in reporting to address operational challenges from reporting to multiple authorities, and foster better communication within and across jurisdictions. FIRE is very flexible (of the 99 information items defined in the standard, 51 are optional) in this way authorities can adopt FIRE to differing breadth and depths, leveraging its features and definitions to promote convergence and facilitate the translation between existing frameworks. This flexibility ensures that FIRE can be integrated into existing regulatory regimes without significant disruption, but it may lead to inconsistencies in reporting practices across jurisdictions, require significant resources, especially for smaller financial institutions.

Differences and Similarities

Feature	EU DORA	FIRE
Scope	Primarily focused on operational resilience within the EU financial sector, encompassing a wide range of operational risks.	A standardized format for reporting operational incidents, including cyber incidents, to regulators and authorities.

Mandate	A binding EU regulation with specific requirements for financial institutions operating within the EU.	A voluntary standard adopted by financial institutions to improve the quality and consistency of incident reporting.
Incident Reporting	Requires detailed incident reporting, including root cause analysis, impact assessment, and remediation actions.	Provides a structured framework for reporting incidents, including key details such as the incident type, severity, affected systems, and impact.
Timely Reporting	Mandates timely reporting of significant operational disruptions and cyber incidents.	Encourages timely reporting of incidents to facilitate rapid response and coordination.
Data Privacy and Security	Emphasizes the importance of protecting sensitive information and ensuring data privacy in incident reporting.	Includes provisions for protecting sensitive information and ensuring confidentiality in incident reporting.

FIRE represents a significant step towards enhancing operational incident reporting in the financial sector, but its implementation is not without significant hurdles. Key challenges include striking a delicate balance between comprehensive reporting and data privacy, ensuring consistent interpretation of reports, adapting to the rapidly evolving cyber threat landscape, and aligning with existing national and international frameworks. Additionally, achieving standardized data quality, integrity and provenance for an immutable audit trail across diverse institutions and jurisdictions poses a significant challenge, as does overcoming resistance to adopting new reporting systems from both financial institutions and regulatory authorities.

Balancing the need for comprehensive incident reporting with the protection of sensitive data becomes a complex challenge. Even with detailed guidelines, there may be instances of misinterpretation of incident reports across different jurisdictions. In light of these challenges, innovative solutions[16] offer promising avenues for improvement. Such platforms can provide a secure and compliant environment for storing and protecting sensitive data, addressing many of the concerns associated with FIRE implementation. By enhancing data security, simplifying compliance processes, improving operational efficiency, and building trust with customers and regulators, these solutions can help financial institutions mitigate the risks associated with incident reporting. Ultimately, the adoption of such advanced technologies can contribute significantly to improving data security and bolstering the overall operational resilience of financial institutions in an increasingly complex regulatory and technological landscape.

Prescriptiveness

EU DORA however mandates the concomitant implementation of prescriptive ICT security policies, procedures, protocols, and tools that aim to ensure the security of networks and data

[16] Disclosure: Weiyee In is an IBM Champion and sits on multiple related councils and working groups

and prevent ICT-related incidents, which aside being “non-trivial” In principle it is widely understood and agreed upon that outdated or legacy infrastructures often would not be up to the standards of advanced cybersecurity, incident response, and reporting capabilities that DORA demands. From a practical level however, financial institutions with diverse infrastructures and systems from mergers will be challenged to deliver a detailed mapping of all technologies, software and cryptographic bills of materials, integrations and third party services, much less do so while maintaining active data exchange and interoperability. Conducting a comprehensive review of any combined IT infrastructure in its entirety, including all inherited systems from mergers and acquisitions

The depth of DORA would require most US financial institutions to restructure their risk management departments, redo their risk management frameworks and invest in new technologies and upskill personnel. By contrast, because the US frameworks are more principles-based US financial institutions have been afforded greater flexibility in how they meet resilience objectives. From an overall commercial and operational efficiency perspective the US approach has been advantageous for financial institutions to enable faster adoption of solutions that tailor their approaches to their specific needs and risk profiles and use cases of the financial institutions and their stakeholders. However, the principled approach may have also led to uncertainty or ambivalence about what constitutes adequate compliance, especially for security and data governance.

DORA's more prescriptive approach extends deeply into security practices, with specific requirements for "vulnerability assessments, open-source analyses, and network security assessments" . This can lead to a more standardized and potentially more robust security posture across the EU financial sector. DORA requires regular vulnerability assessments to identify and address potential weaknesses in systems and applications. This DORA requirement is at least in part a response and best practices directed towards mitigating risks of past incidents like the 2017 Equifax data breach, or WannCry exploiting a known vulnerability in Windows systems. Similarly DORA's focus on open-source analyses is to again prevent incidents such as the 2017 Equifax breach by ensuring thorough scrutiny of open-source components used in financial systems as that breach was also partly attributed to a vulnerability in an open-source component (Apache Struts). The 2014 JPMorgan Chase breach, which is cited to have affected 76 million households and 7 million small businesses, and was attributed to a compromised employee password that gave attackers access to the bank's network. Similarly the forensics in the aftermath of the 2016 SWIFT banking network attacks, which affected multiple banks globally, and the varying levels of security measures implemented by different financial institutions highlighted the potential risks of a less prescriptive approach. These and similar incidents helped drive DORA's requirement for regular network security assessments to proactively identify and address vulnerabilities.

However while DORA's prescriptive approach and more stringent requirements can lead to a stronger and more standardized security posture, it may also create a more predictable security landscape that sophisticated attackers could potentially exploit. In the US currently most financial institutions and ICT/CSPs are ardently following NIST 800 53 and FedRAMP High guidelines as EU financial institutions ramp towards EU DORA requirements. The risk is that financial institutions believe that these are a panacea and if all financial institutions follow the same security “best” practices, a vulnerability in one could potentially be exploited across the sector. DORA, FedRAMP and NIST guidelines often prescribe specific security configurations or technical requirements. The 2014 JPMorgan Chase breach, the Equifax etc. all highlight vulnerabilities despite regular penetration testing, authentication and white listing, web application firewalls as parts of an overall security posture are not enough and how even standardized incident response procedures could be exploited. Where bad actors are aware of technical or security requirements, typical response timelines and procedures, as well as prescribed security recommended configurations, it allows them to exploit the predictability of that prescriptiveness.

While DORA, FedRAMP and NIST raise the overall security baseline, it can also create a predictable attack surface for sophisticated adversaries. The more prescriptive, and thereby predictable the security landscape or the data governance and data structure, counter-intuitively the higher the risk for more sophisticated attackers to find a means for exploitation. The forensics of the 2020 SolarWinds supply chain attack shows that attackers exploited the widespread use of a single software provider across numerous organizations, especially among financial institutions. The bad actors took advantage of the predictable update processes and security configurations mandated by various frameworks and the ubiquity of SolarWinds. The prescriptive data governance frameworks, especially coupled with requirements for sharing information, also often lead to similar data structures and management practices across organizations. The breadth of the 2017 Equifax breach was similarly a result of a single point of failure across multiple organizations due to a vulnerability in a widely-used open-source component (Apache Struts).

The standardized use of components, technologies, governance frameworks, data structures, etc. creates concentration risk and a plethora of single points of failure across multiple organizations. Counter-intuitively in the past decade as financial institutions try to increase and harden their security posture, the industry has consolidated through mergers and acquisitions with regulatory bodies focused far more on market share, revenues and monopolization concerns for these M&A activities in commercial terms rather than the systemic risks that are resulting across the industry globally. As more organizations rely on a small number of popular vendors for cloud services, for B2B SaaS, code generation, testing and security services, the risk becomes concentrated. Any flaw in one widely-used model could affect countless systems and create domino effects akin the impacts of Log4j.

Counter-intuitively the greater the standardization and homogeneity the higher the predictability for malicious actors. The use of standard hardening security implementations and frameworks or guidelines believing them to be a panacea in fact creates predictable patterns that sophisticated attackers could learn to exploit. If bad actors can either access or reverse-engineer the frameworks used by financial institutions for security implementations, they could potentially predict and exploit common weaknesses and through concentration and standardization, across multiple targets. If multiple financial institutions use the same or even similar security platforms, hardening or even “best practices” to implement DORA-compliant security measures, FFIEC or FedRAMP guidelines or other broadly baseline security measures a vulnerability in any particular platform could potentially affect all users simultaneously.

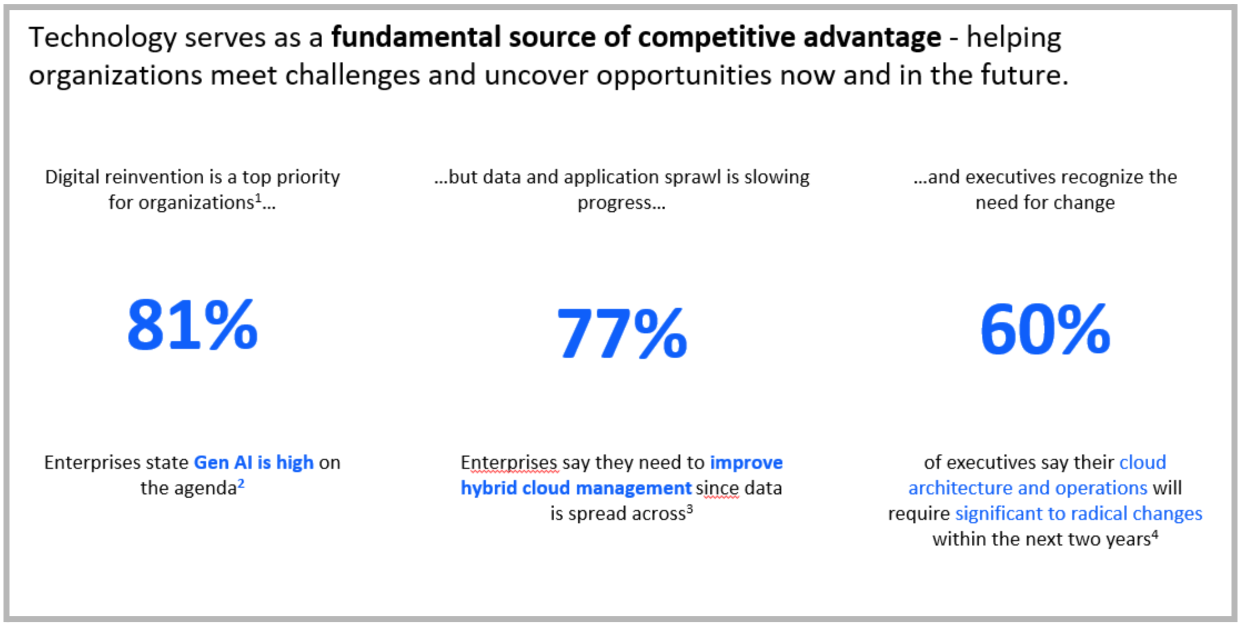
This risk is now being increased by orders of magnitude today with the advent of natural language processing and low code/no code implementations of generativeAI (Large Language Models) and their growing ubiquity. In many current cases through the growing pervasiveness of generative AI LLMs and their natural language interfaces the potential concentration of low code use or similarity also increases as they are spit out from the same or similar training data. The data governance challenges of training data come to the fore and harken back to the earliest days of data and the adage garbage in garbage out but with a dimensionality of vulnerability and risk. If an LLM is trained on datasets that include data or security practices that do not bear the data integrity down to provenance and accountability, its use could propagate multiple vulnerabilities across numerous organizations that rely on its output for security implementations.

Generating new challenges

The use of generative AI (LLMs) while touted by many vendors as the salvation for privacy and resilience actually introduces massive new data governance and security challenges, particularly around the control, provenance, integrity and understanding of how data is being used and processed. Beyond financial institutions using chatbots and generative AI for data analysis or customer interactions inadvertently exposing sensitive information, if the models are not properly governed or if they retain information from interactions that present hallucinations, bias, drift, etc. that lack of control and understanding of how data is being used and processed passes onto becoming sources of truth that taint the future integrity of models and regulatory filings.

The use of generative AI and LLMs for code generation (or worse - low-code generation) and security implementation can lead to a mass homogenization of practices across financial institutions globally. This is particularly concerning with low-code/no-code platforms. In a large financial institution, the use of genAI and LLMs for code generation or security implementation can lead to a homogenization of codes and practices across the broader financial institution. If multiple financial institutions use similar LLMs to generate code for security implementations or data governance policies, in all likelihood they may end up with very similar code bases or practices. This similarity would create a homogenized monoculture of coding and security practices vulnerable to large-scale sophisticated attacks.

The potential here to rapidly propagate flawed or tainted data increases by orders of magnitude. Low-code/no-code platforms regularly rely on pre-built components or templates. If a vulnerability exists in one of these components, it can quickly spread as developers unknowingly use and replicate it across multiple applications. With low-code/no-code platforms and LLMs, flaws or vulnerabilities can propagate rapidly across systems and organizations and today this risk is being massively amplified by the ease of use and wider adoption of these technologies. Low-code/no-code platforms regularly rely on pre-built components or templates. If a vulnerability exists in one of these components, it can quickly spread as developers unknowingly use and replicate it across multiple applications. This becomes a dire issue for data security across a financial institution's ecosystem of third party vendors and also becomes a massive challenge as the end points for data in flight increase exponentially towards nth-Party security and resilience. How financial services firms leverage technologies manage IT risk and governance for a competitive advantage comes to the fore more than ever before.



Technology serves as a **fundamental source of competitive advantage** - helping organizations meet challenges and uncover opportunities now and in the future.

Digital reinvention is a top priority for organizations[1]…

81%

Enterprises state **Gen AI is high** on the agenda[2]

…but data and application sprawl is slowing progress…

77%

Enterprises say they need to **improve hybrid cloud management** since data is spread across[3]

…and executives recognize the need for change

60%

of executives say their cloud architecture and operations will require significant to radical changes within the next two years[4]

Slide from Alan Peacock's keynote presentation "*AI & Hybrid Cloud Innovation Journey*" [17]

As noted consistently across *Accelerate,*[18] hybrid-cloud and AI technologies today have become the cornerstones to creating seamless compliance experiences, scaling quickly to meet regulatory demands, and most importantly, fueling growth while maintaining operational resilience for sustainability as well as regulatory compliance. Financial institutions are constantly looking to address the divergent regulatory requirements, optimize their risk management processes, make their ICT systems more resilient, and improve overall operational stability. In the context of EU DORA and FFIEC guidelines, technology serves as a fundamental source of competitive advantage, helping financial institutions meet regulatory challenges and uncover opportunities for compliance and operational resilience.

Conclusion

The industry need for robust security features that can enhance a financial institution's operational resilience (beyond just the tests mandated by DORA) become paramount as we

[17] Fast Company, IBM and Intel ***Accelerate***, New York October 2024
[18] Fast Company, IBM and Intel ***Accelerate***, New York October 2024

enter the age of Quantum computing and the growing needs for cryptographic telemetry[19] while also supporting the more flexible testing approaches encouraged by US frameworks. The added challenges of financial services today being so multi-jurisdictional and needing cross-border compliance financial institutions need not only uniformity of solution across divergent regulatory requirements but the flexibility to deal with both the prescriptive as well as flexible nature of frameworks that result from EU DORA and FFIEC guidelines. The need for securing data in transit within data exchanges with vendors and partners, to maintain control over sensitive information and maintain resilience across disparate heterogeneous hybrid and multi-cloud environments drives the need for next generation technologies.

References

- European Insurance and Occupational Pensions Authority. (n.d.). Digital Operational Resilience Act (DORA).
- Federal Deposit Insurance Corporation. (2021, June 30). Updated FFIEC IT Examination Handbook. Financial Institution Letter FIL-47-2021
- Federal Financial Institutions Examination Council, "Architecture, Infrastructure, and Operations (AIO) Booklet", 2021
- Board of Governors of the Federal Reserve System. (2021, June 30). SR 21-11: FFIEC Architecture, Infrastructure, and Operations Examination Handbook. Supervision and Regulation Letters, from https://www.federalreserve.gov/supervisionreg/srletters/SR2111.htm
- IBM:. What Is the Digital Operational Resilience Act (DORA)? https://www.ibm.com/topics/digital-operational-resilience-act
- European Securities and Markets Authority. Digital Operational Resilience Act (DORA). Retrieved November 16, 2024, from https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
- Citigroup. (2024, September 19). DORA: The EU's New Regulatory Framework on Digital Operational Resilience., from https://www.citigroup.com/global/insights/dora-the-eu-new-regulatory-framework-on-digital-operational-resilience
- Oxfeldt, M. (2024, July 17). What is the EU Digital Operational Resilience Act (DORA)? Keepit. Retrieved November 16, 2024, from https://www.keepit.com/blog/what-is-dora/
- ISACA. (2024, August 28). DORA Compliance: Navigating the New EU Regulation. Retrieved November 16, 2024, from https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/dora-compliance-navigating-the-new-eu-regulation

[19] Weiyee In, Kurt Hardesty, Jefferson Dance, "*Cryptographic Telemetry*" November, 2024 https://eclypses.com/white-papers/cryptographic-telemetry