



MASTER THESIS | MASTER'S THESIS

Titel | Title

REGULATORY CONVERGENCE OR DIVERGENCE?

Analysing Whether DORA Will Push US Regulators Toward a More Unified Framework

verfasst von | submitted by

Robert Erik Kittler

angestrebter akademischer Grad | in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien | Vienna, 2026

Studienkennzahl lt. Studienblatt |
Degree programme code as it appears on the
student record sheet:

UA 999 082

Universitätslehrgang lt. Studienblatt |
Postgraduate programme as it appears on the
student record sheet:

Europäisches und Internationales Wirtschaftsrecht
[Vollzeit Englisch]

Betreut von | Supervisor:

Dipl.-Jur. Dr. Maria Elisabeth Sturm LL.M.

ABSTRACT

DORA, applicable from 17 January 2025, establishes the most comprehensive unified framework for ICT risk management, incident reporting, resilience testing, and oversight of critical third-party providers in the EU financial sector. The United States, by contrast, maintains a fragmented multi-agency architecture without a harmonised federal statute.

This thesis examines whether DORA's extraterritorial reach and the Brussels Effect will catalyse regulatory convergence in the United States, or whether structural and political differences will sustain transatlantic divergence.

The thesis concludes that DORA generates selective de facto convergence at the operational level, particularly among cloud infrastructure providers facing strong Brussels Effect pressures, while de jure legal divergence persists due to US path dependency and the absence of federal legislative authority.

Keywords: DORA; Digital Operational Resilience Act; Brussels Effect; regulatory convergence; transatlantic financial regulation; ICT risk; extraterritoriality; cloud computing.

ZUSAMMENFASSUNG

DORA, die ab dem 17. Januar 2025 gilt, schafft den umfassendsten einheitlichen Rahmen für das Management von ICT-Risiken, die Meldung von Vorfällen, Resilienztests und die Aufsicht über zentrale Drittanbieter im EU-Finanzsektor. Die USA hingegen haben eine fragmentierte Multi-Agentur-Struktur ohne ein harmonisiertes Bundesgesetz.

Die Arbeit untersucht, ob DORAs extraterritoriale Reichweite und der Brüssel-Effekt eine regulatorische Konvergenz in den USA auslösen werden oder ob strukturelle und politische Unterschiede eine anhaltende transatlantische Divergenz begründen werden.

Die Arbeit kommt zu dem Ergebnis, dass DORA eine selektive De-facto-Konvergenz auf operativer Ebene erzeugt, insbesondere bei Cloud-Infrastrukturanbietern mit starkem Brüssel-Effekt-Druck, während eine De-jure-Divergenz aufgrund von Pfadabhängigkeiten und fehlender bundesgesetzlicher Rechtsgrundlage fortbesteht.

Schlüsselwörter: DORA; Brüssel-Effekt; regulatorische Konvergenz; transatlantische Finanzregulierung; IKT-Risiko; Extraterritorialität; Cloud Computing.

TABLE OF CONTENTS

ABSTRACT	2
ZUSAMMENFASSUNG.....	2
TABLE OF CONTENTS	4
TABLE OF ABBREVIATIONS	6
CHAPTER 1: INTRODUCTION	7
1.1 Background and Context	8
1.2 Research Question and Objectives	9
1.3 Theoretical Framework	10
1.3.1 Brussels Effect Theory	10
1.3.2 Regulatory Convergence and Divergence Theory	12
1.3.3 Extraterritoriality in Financial Regulation	13
1.4 Methodology	13
1.5 Structure Overview.....	14
CHAPTER 2: THE EU'S DIGITAL OPERATIONAL RESILIENCE ACT (DORA).....	16
2.1 Legislative History and Policy Objectives	16
2.2 Scope and Application.....	17
2.2.1 Personal Scope: Financial Entities	17
2.2.2 Material Scope: ICT-Related Risks.....	18
2.2.3 Territorial Scope and Third-Country Dimension	18
2.3 The Five Pillars of DORA	18
2.3.1 First Pillar: ICT Risk Management Framework (Articles 5-16)	18
2.3.2 Second Pillar: ICT-Related Incident Management and Reporting (Articles 17-23).....	19
2.3.3 Third Pillar: Digital Operational Resilience Testing (Articles 24-27)	19
2.3.4 Fourth Pillar: Third-Party ICT Risk Management (Articles 28-30).....	20
2.3.5 Fifth Pillar: Oversight Framework for Critical Third-Party Providers (Articles 31-44)	21
2.4 DORA's Extraterritorial Reach.....	24
2.5 Penalties and Enforcement	25
CHAPTER 3: US OPERATIONAL RESILIENCE REGULATORY FRAMEWORK.....	26
3.1 Overview of US Financial Regulatory Structure.....	26
3.2 Key US Operational Resilience Guidance and Rules.....	27
3.2.1 Federal Reserve and OCC: Sound Practices to Strengthen Operational Resilience (2020)	27
3.2.2 Computer-Security Incident Notification Rule (2021).....	28
3.2.3 Interagency Guidance on Third-Party Relationships: Risk Management (2023).....	29
3.2.4 SEC: Cybersecurity Risk Management Rules (2023-2024).....	30
3.2.5 Other Relevant Frameworks	30
3.3 Comparative Analysis: US vs. DORA	31
3.4 Gaps and Weaknesses in US Framework	33

CHAPTER 4: MECHANISMS OF EXTRATERRITORIAL INFLUENCE AND THE BRUSSELS EFFECT	35
4.1 Theoretical Framework: The Brussels Effect Applied to Financial Regulation.....	35
4.1.1 Condition One: Market Size.....	35
4.1.2 Condition Two: Regulatory Capacity	35
4.1.3 Condition Three: Stringency	36
4.1.4 Condition Four: Inelastic Targets.....	36
4.1.5 Condition Five: Non-Divisibility	37
4.1.6 Overall Assessment: Will DORA Generate a Brussels Effect?	37
4.2 DORA's Extraterritorial Mechanisms in Detail.....	38
4.2.1 Direct Mechanism: The EU Subsidiary Requirement.....	38
4.2.2 Indirect Mechanism: The Contractual Cascade.....	39
4.2.3 Market Access Conditioning and Competitive Dynamics	39
4.2.4 Global Standard-Setting Through First-Mover Advantage	40
4.3 Practical Impact on US Third-Party Providers	40
4.3.1 Amazon Web Services, Microsoft Azure, and Google Cloud Platform	40
4.3.2 Other Potential Critical Third-Party Providers.....	41
4.3.3 Compliance Costs and Strategic Responses	42
4.4 Limitations and Countervailing Forces	42
4.4.1 US Market Size as Counterweight	42
4.4.2 US Regulatory Resistance and Jurisdictional Competition	43
4.4.3 Geopolitical Factors and Strategic Technology Competition.....	43
4.4.4 Technical and Economic Limits to Non-Divisibility	43
4.4.5 'Brussels Effect in Retreat'? Recent Scholarly Skepticism.....	43
CHAPTER 5: EVIDENCE OF CONVERGENCE AND DIVERGENCE.....	45
5.1 Evidence of Convergence Pressures.....	45
5.1.1 Market-Driven Convergence Through Provider Adaptation.....	45
5.1.2 International Regulatory Dialogue and Coordination	46
5.1.3 Industry-Led Operational Resilience Initiatives.....	46
5.2 Evidence of Persistent Divergence	47
5.2.1 Structural and Institutional Obstacles to US Convergence	47
5.2.2 Philosophical and Political Divergence.....	47
5.2.3 Persistent Absence of Direct Third-Party Oversight Authority.....	48
5.3 Case Study: Amazon Web Services' Response to DORA	48
CHAPTER 6: ANALYSIS AND IMPLICATIONS	50
6.1 Degree of Convergence: Assessment	50
6.1.1 High Convergence: Operational Capabilities and Best Practices.....	50
6.1.2 Moderate Convergence: Contractual Practices	50
6.1.3 Low Convergence: Legal Frameworks and Direct Oversight	50
6.2 Explanatory Factors: Why Convergence and Divergence Coexist.....	51

6.2.1 Why Convergence Occurs: Market Forces and Technical Non-Divisibility	51
6.2.2 Why Divergence Persists: Institutional Path Dependency and Political Constraints	51
6.3 Implications for Financial Institutions and Technology Providers.....	51
CHAPTER 7: CONCLUSION	53
7.1 Summary of Findings	53
7.2 Theoretical Contributions.....	53
7.3 Policy Recommendations	54
7.4 Future Research Directions	54
TABLE OF CASES AND LEGISLATION.....	55
Table of Cases	55
Table of EU Legislation	55
Table of US Legislation.....	55
BIBLIOGRAPHY.....	56
PRIMARY SOURCES	56
European Union	56
United States	56
Cases	56
SECONDARY SOURCES.....	56
Books	56
Journal Articles	56
Chapters in Edited Books.....	57
Reports and Policy Documents	57
International Standards and Guidance.....	58
Online Sources	58

TABLE OF ABBREVIATIONS

AML	Anti-Money Laundering
AWS	Amazon Web Services
BSA	Bank Secrecy Act
CEO	Chief Executive Officer
CFPB	Consumer Financial Protection Bureau
CFR	Code of Federal Regulations
CFTC	Commodity Futures Trading Commission
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus Disease 2019
CRD	Capital Requirements Directive
CTPP	Critical ICT Third-Party Provider
DORA	Digital Operational Resilience Act (Regulation (EU) 2022/2554)
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ESA	European Supervisory Authority/ies

ESMA	European Securities and Markets Authority
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FINRA	Financial Industry Regulatory Authority
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSB	Financial Stability Board
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679)
ICT	Information and Communication Technology
IIF	Institute of International Finance
LLM	Legum Magister (Master of Laws)
MiCA	Markets in Crypto-Assets Regulation (Regulation (EU) 2023/1114)
MiFID II	Markets in Financial Instruments Directive II (Directive 2014/65/EU)
NAIC	National Association of Insurance Commissioners
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OJ	Official Journal of the European Union
RTS	Regulatory Technical Standards
SEC	Securities and Exchange Commission
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TIBER-EU	Threat Intelligence-based Ethical Red-teaming for the European Union
TLPT	Threat-Led Penetration Testing
UCITS	Undertakings for Collective Investment in Transferable Securities
USC	United States Code

CHAPTER 1: INTRODUCTION

The digitalisation of financial services has created unprecedented dependencies on ICT infrastructure. As institutions have migrated to cloud platforms, operational resilience has emerged as a critical regulatory concern, a trend accelerated by the COVID-19 pandemic, which exposed vulnerabilities in operational continuity arrangements worldwide.

Keeping in mind the dangers the financial sector could face, the European Union adopted the Digital Operational Resilience Act (DORA) in December 2022, with the Regulation entering into force on 16 January 2023 and becoming applicable from 17 January 2025. DORA represents the EU's most comprehensive effort to harmonise operational resilience requirements across the financial sector, establishing a unified framework for ICT risk management, incident reporting, resilience testing, third-party risk management. Most notably, direct regulatory oversight of critical ICT third-party service providers is established by DORA.¹

In contrast, the United States maintains a fragmented regulatory landscape for operational resilience. Multiple federal regulators, including the Federal Reserve, the Office of the Comptroller of the Currency (OCC), the

¹ Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [2022] OJ L333/1, arts 31-44.

Federal Deposit Insurance Corporation (FDIC), and the Securities and Exchange Commission (SEC) promulgate their own guidance and rules for the institutions under their respective jurisdictions. While these agencies have coordinated on certain limited initiatives, most notably the 2020, “Sound Practices to Strengthen Operational Resilience” guidance, the US approach remains predominantly principles-based, supervisory in nature, and lacks the prescriptive, harmonised character of DORA.² This divergence in regulatory approaches raises the central question of whether DORA’s extraterritorial reach and the ‘Brussels Effect’, which represents the European Union’s capacity to unilaterally shape global regulatory standards, will catalyse regulatory convergence in the United States, or whether structural and political differences will sustain persistent transatlantic divergence.

1.1 Background and Context

The contemporary focus on operational resilience in financial regulation emerged from multiple converging developments. The 2008 global financial crisis prompted regulators to strengthen prudential requirements and expand macroprudential oversight, but initially concentrated primarily on capital adequacy, liquidity, and systemic risk. This reactive policy directly addressed the acute vulnerabilities identified during that period. However, it was not until the following decade that operational resilience, in particular ICT-related operational risk, gained prominence as a distinct regulatory concern.³

Several converging factors drove this shift in regulatory attention. The rapid digitalisation of financial services created new categories of vulnerability that traditional prudential regulation was poorly equipped to address: before the advent of cloud computing, there was only limited need for robust, harmonised approaches to ICT risk within the financial sector. As traditional brick-and-mortar banking gave way to online and mobile banking, as algorithmic trading replaced manual execution, and as cloud computing emerged as the dominant infrastructure model, these technological advances increased efficiency dramatically, but they also concentrated risk within ICT systems and infrastructure in ways the existing regulatory architecture had not anticipated.

This technological shift was reinforced by a series of high-profile cyber incidents that demonstrated, with increasing clarity, the potential systemic impact of ICT failures. The 2016 SWIFT Bangladesh Bank heist, in which hackers stole \$81 million through compromised credentials, exposed serious vulnerabilities in critical financial infrastructure that had previously been assumed secure.⁴ The 2017 WannaCry ransomware attack

²Federal Reserve, SR Letter 20-24, 'Sound Practices to Strengthen Operational Resilience' (2 November 2020) <<https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm>> accessed 30 June 2026; Office of the Comptroller of the Currency, OCC Bulletin 2020-94, 'Operational Risk: Sound Practices to Strengthen Operational Resilience' (30 October 2020) <<https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-94.html>> accessed 30 June 2026; Federal Deposit Insurance Corporation, FIL-103-2020, 'Sound Practices to Strengthen Operational Resilience' (2 November 2020) <<https://www.fdic.gov/news/financial-institution-letters/2020/fdic-publishes-sound-practices-strengthen-operational>> accessed 30 June 2026.

³ Basel Committee on Banking Supervision, 'Basel III: A global regulatory framework for more resilient banks and banking systems' (December 2010, revised June 2011).

⁴ Krishna N Das and Jonathan Spicer, 'How Hackers Stole \$81 Million from the Bangladesh Central Bank' Reuters (Dhaka/New York, 18 May 2016) <<https://2017.sopawards.com/wp-content/uploads/2017/03/The-Bangladesh-Bank-Heist.pdf>> accessed 30 June 2026.

disrupted financial institutions globally, crippling operations across multiple jurisdictions simultaneously,⁵ while the 2020 SolarWinds supply chain attack and the 2021 Colonial Pipeline ransomware incident⁶ underscored that cyber threats had evolved into sophisticated, state-sponsored operations capable of incapacitating critical infrastructure on a scale regulators had not previously confronted.⁷

The COVID-19 pandemic then served as an unplanned but instructive stress test for financial institutions' operational resilience. The abrupt shift to remote work in March 2020 forced institutions to scale up their technological infrastructure virtually overnight, and while most major institutions demonstrated adequate business continuity capabilities under this pressure, the pandemic nonetheless revealed gaps in incident response planning, third-party dependency management, and operational risk governance that had gone largely untested in calmer periods.⁸

Compounding these developments, the concentration of critical ICT services among a small number of providers, principally Amazon Web Services, Microsoft Azure, and Google Cloud Platform, raised legitimate systemic risk concerns of its own. These 'Big Three' providers collectively host the majority of financial institutions' cloud workloads, creating single points of failure that could precipitate system-wide disruption should any one of them experience a significant outage.⁹ The shift to cloud computing thus meant that critical financial operations increasingly depended on entities that sat entirely outside the financial regulatory perimeter, a structural gap that both DORA and the fragmented US response examined in this thesis can be understood as attempts to close.¹⁰

1.2 Research Question and Objectives

This thesis addresses the following primary research question: whether the EU's Digital Operational Resilience Act (DORA) will drive regulatory convergence in US financial operational resilience frameworks, or whether it will instead reinforce divergence between transatlantic approaches. This primary research question encompasses several subsidiary inquiries, addressed in turn below.

⁵ National Cyber Security Centre, 'Ransomware: 'WannaCry' Guidance for Enterprise Administrators' (May 2017) <<https://www.ncsc.gov.uk/guidance/ransomware-wannacry-guidance-enterprise-administrators-1>> accessed 30 June 2026.

⁶ US Cybersecurity and Infrastructure Security Agency, 'SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity' Alert AA20-352A (17 December 2020); Collin Eaton and Dustin Volz, 'Colonial Pipeline CEO Tells Why He Paid Hackers a \$4.4 Million Ransom' The Wall Street Journal (19 May 2021) <<https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636>> accessed 30 June 2026.

⁷ Financial Stability Board, 'Effective Practices for Cyber Incident Response and Recovery' (19 October 2020) <<https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/>> accessed 30 June 2026.

⁸ Federal Reserve Board, 'Supervision and Regulation Report' (November 2020) 27-30.

⁹ European Banking Authority, 'Report on the Use of Digital Platforms in the EU Banking and Payments Sector' (EBA/REP/2021/26, 21 September 2021) <https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2021/1019865/EBA%20Digital%20platforms%20report%20-%20210921.pdf> accessed 30 June 2026.

¹⁰ Financial Stability Board, 'Third-party dependencies in cloud services: Considerations on financial stability implications' (9 December 2019).

First, the thesis examines the key extraterritorial mechanisms through which DORA extends its regulatory influence beyond EU borders, and how they operate in practice vis-à-vis US ICT service providers. Second, the thesis analyses how the current US operational resilience regulatory framework operates, its structural characteristics, and the substantive gaps relative to DORA across the five regulatory pillars.

Third, the thesis examines what market pressures facilitate regulatory convergence between the EU and US approaches, applying the ‘Brussels Effect’ theoretical framework to assess whether DORA satisfies the conditions for unilateral regulatory globalisation. This involves analysing the strategic responses of major US ICT service providers to DORA’s requirements, in particular whether these providers are adopting DORA-compliant practices globally or maintaining region-specific compliance strategies. Fourth, this thesis isolates the structural, institutional, political, and philosophical determinants that impede convergence and sustain divergence between both regulatory regimes.

The thesis delimits its scope to operational resilience regulation related to ICT risks, concentrating on the transatlantic EU–US relationship and covering developments from approximately 2020 through early 2026. Other major financial centers such as the UK, Singapore, and Hong Kong fall outside the primary scope, as does broader fintech policy.

1.3 Theoretical Framework

This thesis employs two complementary theoretical frameworks to analyse the potential for regulatory convergence or divergence: the Brussels Effect theory and regulatory convergence/divergence theory from international political economy.

1.3.1 Brussels Effect Theory

The Brussels Effect, theorised by Anu Bradford, describes the European Union's capacity to unilaterally regulate global markets, which should be traditionally beyond the EU’s jurisdiction. Bradford identifies two variants: the de facto Brussels Effect, where market actors voluntarily adopt EU standards globally to access the EU market, and the de jure Brussels Effect, where foreign jurisdictions formally codify EU mandates within their domestic legislation. This thesis primarily concerns the former, though it remains alert to evidence of the latter.¹¹ Bradford identifies five conditions that must be satisfied for the Brussels Effect to operate, conditions that together provide the analytical framework applied to DORA throughout Chapter 4 of this thesis.

The first is market size: the EU must constitute a sufficiently large market that global firms cannot afford to forgo access to it. The EU’s financial services market, representing approximately 20% of global financial assets, comfortably meets this threshold for most major financial institutions and technology providers.¹² The second is regulatory capacity: the EU must possess the institutional capability to promulgate and enforce stringent

¹¹ Anu Bradford, 'The Brussels Effect' (2012) 107 Northwestern University Law Review 1.

¹² European Central Bank, 'Financial Integration and Structure in the Euro Area' (June 2024) 12.

regulations, a condition satisfied by the European Supervisory Authorities — comprising the European Banking Authority, the European Insurance and Occupational Pensions Authority, and the European Securities and Markets Authority — which together provide a centralised regulatory capacity largely absent in more institutionally fragmented jurisdictions such as the United States.¹³

The third condition is stringency: EU regulations must be more demanding than those of competing jurisdictions, and DORA's extensive requirements for ICT risk management, mandatory resilience testing, and direct oversight of third-party providers arguably exceed US guidance in specificity, enforceability, and overall scope.¹⁴ The fourth is the presence of inelastic targets: regulated entities must have limited practical ability to exit the EU market altogether. Major global financial institutions typically require an EU presence to serve European clients, while technology providers such as cloud computing platforms derive substantial revenue from EU financial services contracts that they are commercially unwilling to forfeit.

The fifth and final condition, non-divisibility, holds that compliance costs must be structured such that firms find global standardisation more economical than maintaining separate EU-compliant and non-EU operations side by side. As Chapter 4 develops at length, this fifth condition is the one whose satisfaction is most genuinely contested in DORA's case, and the degree to which it holds — fully, partially, or only for certain categories of provider — does much of the analytical work in explaining why this thesis finds selective rather than comprehensive convergence.¹⁵

Bradford herself recognises important limitations to the Brussels Effect in financial regulation. She notes that financial services present unique challenges because capital is mobile, potentially enabling financial institutions to relocate operations to avoid and circumvent stringent regulation - a dynamic known as “regulatory arbitrage”. However, DORA's focus on operational resilience rather than prudential requirements may mitigate this concern. Operational resilience standards relate more to processes and infrastructure than to balance sheet requirements that might trigger relocation.¹⁶

Recent scholarship has questioned whether the Brussels Effect remains as potent as Bradford's original 2012 analysis suggested. Critics point to increasing regulatory nationalism, with major jurisdictions such as the United States, China, and India explicitly designing regulatory frameworks that diverge from EU standards.¹⁷ The EU's

¹³ Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing the European Banking Authority [2010] OJ L331/12; Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing the European Insurance and Occupational Pensions Authority [2010] OJ L331/48; Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing the European Securities and Markets Authority [2010] OJ L331/84.

¹⁴ Basel Committee on Banking Supervision, 'Principles for operational resilience' (March 2021).

¹⁵ Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020) 23-51.

¹⁶ Bradford (n 15) 282-285.

¹⁷ 'The Brussels Effect in Retreat: How US Economic Might and Political Interference Trump EU Regulation' EuropeanRelations.com (26 September 2025) <<https://europeanrelations.com/the-brussels-effect-in-retreat/>> accessed 16 February 2026.

declining share of global GDP and the rise of alternative regulatory poles, such as China's techno-nationalist approach to technology governance, may constrain the EU's unilateral regulatory power.¹⁸

1.3.2 Regulatory Convergence and Divergence Theory

The second theoretical framework draws on international political economy literature examining why regulatory systems converge or diverge. Beth Simmons' foundational work on regulatory harmonisation identifies several mechanisms through which convergence occurs: regulatory competition (jurisdictions compete to attract mobile capital), policy learning (regulators learn from each other's experiences), and coercion (powerful actors compel weaker jurisdictions to adopt preferred rules).¹⁹

Emily Jones and Alexandra Zeitz's more recent work on regulatory convergence in the financial periphery extends this analysis, demonstrating that convergence patterns vary systematically based on power asymmetries, economic interdependence, and the presence of international standards. Their spatial econometric analysis of Basel II adoption reveals that peripheral jurisdictions' regulatory choices are significantly influenced by core financial centers. However, this influence operates through multiple channels such as trade linkages, financial integration, and membership in international organisations rather than through simple coercion.²⁰

Path dependency theory provides a complementary perspective on regulatory divergence. Regulatory systems become “locked in” to particular trajectories due to sunk costs and political constituencies benefiting from existing structures.²¹ The US financial regulatory system's fragmentation across multiple agencies, each with distinct statutory authorities and political constituencies, exemplifies path dependency. Attempts to consolidate regulatory authority such as proposals for a single federal banking regulator have repeatedly failed despite theoretical efficiency gains. The reason behind the failure stems precisely from existing institutional arrangements which create vested interests resistant to reform.²²

Hwa-Jin Kim's analysis of transatlantic financial regulatory convergence introduces an additional consideration: even when convergence appears to occur, it may reflect “shallow” or superficial rather than “deep” harmonisation. Shallow harmonisation involves adopting similar regulatory language while permitting significant discretion in implementation, enforcement, and interpretation. Deep harmonisation requires not merely textual similarity but genuine functional equivalence in how rules operate in practice. This distinction proves critical for

¹⁸ A Chander and UP Lê, 'Data Nationalism' (2015) 64 Emory Law Journal 677.

¹⁹ Beth A Simmons, 'The International Politics of Harmonization: The Case of Capital Market Regulation' (2001) 55 International Organization 589.

²⁰ Emily Jones and Alexandra O Zeitz, 'Regulatory Convergence in the Financial Periphery: How Interdependence Shapes Regulators' Decisions' (2019) 63 International Studies Quarterly 908.

²¹ Paul Pierson, 'Increasing Returns, Path Dependence, and the Study of Politics' (2000) 94 American Political Science Review 251.

²² Roberta Romano, 'The Sarbanes-Oxley Act and the Making of Quack Corporate Governance' (2005) 114 Yale Law Journal 1521, 1528-1532.

assessing whether DORA-induced changes in US practices constitute meaningful convergence or merely superficial alignment.²³

1.3.3 Extraterritoriality in Financial Regulation

The third theoretical component addresses extraterritoriality. Extraterritoriality concerns the application of a jurisdiction's laws beyond its territorial borders. Legal scholarship distinguishes between “territorial extension” (regulating the local effects of foreign conduct) and “genuine extraterritoriality” (regulating conduct occurring entirely outside the jurisdiction).²⁴

DORA employs both mechanisms. The EU subsidiary requirement imposes obligations directly on foreign entities based on their relationships with EU financial institutions — genuine extraterritoriality. The contractual cascade, requiring EU financial entities to impose DORA-compliant terms on non-EU providers, represents territorial extension operating through private contract.

The “effects doctrine” in competition law provides a relevant analogy. The European Court of Justice's jurisprudence permits EU competition law to apply to foreign conduct that produces effects within the EU market. DORA's oversight of critical third-party providers operates on similar logic: even though providers such as Amazon Web Services or Microsoft Azure are domiciled in the United States, their provision of services to EU financial institutions creates regulatory nexus sufficient to justify EU oversight.²⁵

Public international law's permissive approach to prescriptive jurisdiction further contextualises DORA's extraterritorial assertions. While international law restricts enforcement jurisdiction because states generally cannot enforce their laws in foreign territory without the territorial state's consent, prescriptive jurisdiction (the authority to promulgate rules applicable to foreign conduct) receives greater latitude. DORA's requirements fall primarily within prescriptive jurisdiction; the EU does not purport to conduct inspections on US soil without consent, but rather conditions EU market access on compliance with EU standards.²⁶

1.4 Methodology

This thesis employs a comparative legal methodology, examining EU and US operational resilience frameworks through doctrinal analysis of primary legal sources supplemented by institutional analysis of regulatory structures and practices. The doctrinal component involves close reading of DORA's text, particularly its extraterritorial provisions, third-party oversight framework, and implementing technical standards.

²³ Hwa-Jin Kim, 'Toward Transatlantic Convergence in Financial Regulation' in Kern Alexander and Rahul Dhumale (eds), *Research Handbook on International Financial Regulation* (Edward Elgar 2012) 358.

²⁴ Cedric Ryngaert, *Jurisdiction in International Law* (2nd edn, Oxford University Press 2015) 31-48.

²⁵ Case C-413/14 P *Intel Corp Inc v Commission* ECLI:EU:C:2017:632.

²⁶ Restatement (Third) of Foreign Relations Law § 402 (American Law Institute 1987).

The institutional analysis examines the organisational structures through which operational resilience regulation operates. For the EU, this includes the role of the ESAs in DORA implementation, the Lead Overseer designation process, and the operation of joint examination teams.

The comparative dimension employs structured, focused comparison rather than an attempt at exhaustive coverage of every facet of operational resilience regulation. The analysis instead concentrates on specific points of comparison that are most revealing of convergence or divergence: legal form (regulation versus supervisory guidance), harmonisation (a single unified standard versus a fragmented patchwork of agency-specific rules), third-party oversight (direct regulatory examination of providers versus indirect oversight mediated through the financial institutions that contract with them), testing requirements (mandatory threat-led penetration testing versus voluntary, unstandardised exercises), and incident reporting (harmonised templates and timelines versus inconsistent, agency-specific notification regimes). Structuring the comparison around these five dimensions allows like to be compared with like, rather than producing the kind of impressionistic, surface-level comparison that risks overstating either convergence or divergence.

The analysis draws on three types of evidence to assess convergence or divergence. The first is textual evidence drawn from regulatory documents, technical standards, and implementing guidance, which establishes the formal requirements that each jurisdiction imposes. The second is behavioural evidence drawn from the public statements, contractual amendments, and compliance documentation of major ICT service providers, which reveals whether market actors are in practice converging on common operational standards regardless of the formal legal position. The third is institutional evidence drawn from bilateral and multilateral regulatory dialogue between EU and US authorities, which indicates whether convergence pressures are being channelled into coordinated policy responses or are instead generating friction between the two regulatory systems.

The thesis acknowledges several methodological limitations. DORA only became applicable in January 2025, so empirical evidence remains limited and the analysis incorporates predictive elements. Access to confidential supervisory information or proprietary compliance strategies is unavailable, and the EU–US focus means multilateral dynamics receive limited attention.

1.5 Structure Overview

The thesis proceeds as follows. Chapter 2 provides comprehensive analysis of DORA, covering its legislative history, five substantive pillars, and extraterritorial mechanisms. Chapter 3 maps the fragmented US operational resilience landscape. Chapter 4 applies the Brussels Effect framework to DORA, assessing each of its five conditions and analysing the direct and indirect legal and commercial mechanisms through which DORA’s influence extends to US providers. Chapter 5 assembles the empirical evidence of convergence and divergence, culminating in the AWS case study. Chapter 6 synthesises this evidence into a three-tier assessment of convergence and explains why market-driven convergence and legal divergence coexist. Chapter 7 concludes with a summary of findings, theoretical contributions, policy recommendations, and directions for future research.

CHAPTER 2: THE EU'S DIGITAL OPERATIONAL RESILIENCE ACT (DORA)

The Digital Operational Resilience Act represents the European Union's most ambitious effort to establish a comprehensive, harmonised framework for managing ICT-related operational risks in the financial sector.

2.1 Legislative History and Policy Objectives

DORA emerged from the European Commission's broader Digital Finance Package, announced in September 2020. According to the Commission, fragmented national approaches to ICT risk management obstructed single-market integration in financial services while incentivising regulatory arbitrage. Prior to DORA, operational resilience requirements for financial institutions derived from multiple sources: the Capital Requirements Directive IV (CRD IV) for banks, the Second Payment Services Directive (PSD2) for payment services, the Markets in Financial Instruments Directive II (MiFID II) for investment firms, and Solvency II for insurance undertakings. These sectoral frameworks addressed ICT risks inconsistently, with different definitions, requirements, and supervisory approaches across sectors and Member States.²⁷

The Commission's September 2020 proposal for DORA aimed to address these gaps through horizontal harmonisation by establishing uniform requirements applicable across the financial sector rather than sector-specific rules. The proposal also responded to the concentration of ICT services among a small number of large providers (the cloud computing platforms) by creating a direct oversight framework for “critical ICT third-party service providers”. This represented a novel approach that extended regulatory authority beyond traditional financial institutions to technology companies operating outside the financial sector.²⁸

The European Parliament and Council negotiated DORA through the ordinary legislative procedure, reaching political agreement in May 2022. The final text was formally adopted on 14 December 2022 as Regulation (EU) 2022/2554, accompanied by Directive (EU) 2022/2556 amending existing sectoral directives to align with DORA. The Regulation took effect on 16 January 2023, granting a 24-month transitional grace period to financial entities and external ICT providers before DORA became fully binding on 17 January 2025.²⁹

DORA articulates three principal policy objectives. First, harmonisation: establishing uniform requirements across all 27 Member States and all categories of financial entities eliminates regulatory arbitrage opportunities and reduces compliance costs for cross-border institutions. Second, operational resilience: prescriptive requirements for ICT risk management, incident response, and resilience testing aim to strengthen individual institutions' capacity to withstand and recover from ICT disruptions. Third, financial stability: by addressing

²⁷ European Commission, 'Proposal for a Regulation on Digital Operational Resilience for the Financial Sector' COM(2020) 595 final, 2-3.

²⁸ *ibid* 4-5.

²⁹ Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector [2022] OJ L333/80.

concentration risk in critical ICT services and establishing oversight of systemically important third-party providers, DORA seeks to mitigate systemic vulnerabilities that could precipitate financial instability.³⁰

The European Supervisory Authorities have developed extensive implementing technical standards (ITS) and regulatory technical standards (RTS) pursuant to DORA's numerous empowerments. These delegated acts, adopted by the European Commission, provide detailed specifications for incident reporting templates, resilience testing methodologies, third-party contractual arrangements, and oversight procedures. The ESAs published final draft technical standards throughout 2024, with the Commission's adoption occurring in phases during 2024 and early 2025.³¹

2.2 Scope and Application

DORA's scope encompasses three dimensions: personal scope (which entities are subject to the Regulation), material scope (which activities are covered), and territorial scope (where DORA applies).

2.2.1 Personal Scope: Financial Entities

Article 2(1) of DORA defines 'financial entity' to include 21 categories of institutions. These categories encompass virtually the entire regulated financial sector.³²

Credit institutions under Regulation (EU) No 575/2013 constitute the largest and most systemically significant category. Insurance undertakings, UCITS managers, AIFMs, credit rating agencies, critical benchmark administrators, and crowdfunding service providers extend DORA's reach across the full breadth of the financial sector.

Notably, DORA integrates with the Markets in Crypto-Assets Regulation (MiCA) by including crypto-asset service providers within its scope, reflecting the EU's comprehensive approach to regulating digital finance. This ensures that entities offering crypto-asset custody, exchange, or advisory services face the same operational resilience requirements as traditional financial institutions.³³

DORA provides limited exemptions for small and non-interconnected institutions. Microenterprises as defined in the Accounting Directive may benefit from simplified requirements under certain conditions, though competent authorities retain discretion to require full compliance based on risk profile. This proportionality principle recognises that imposing identical requirements on a major international bank and a small local credit union would be inefficient, though the baseline standards apply broadly.³⁴

³⁰ DORA (n 1) recitals 3-7.

³¹ European Supervisory Authorities, 'ESAs publish final package of policy and technical standards under DORA' (17 January 2024) <<https://www.esma.europa.eu>> accessed 16 February 2026.

³² DORA (n 1) art 2(1).

³³ DORA (n 1) art 2(1)(u); Regulation (EU) 2023/1114 on markets in crypto-assets [2023] OJ L150/40 (MiCA).

³⁴ DORA (n 1) art 4.

2.2.2 Material Scope: ICT-Related Risks

DORA's material scope covers risks arising from the use of information and communication technology, defined broadly to encompass both internal ICT systems and externally sourced ICT services. Article 6 requires financial entities to maintain an ICT risk management framework covering identification, classification, mitigation, and management of ICT risks, with clear internal accountability. Financial entities retain ultimate responsibility even when ICT services are outsourced.

2.2.3 Territorial Scope and Third-Country Dimension

DORA's territorial scope follows the general principle that EU Regulations apply to entities established within the EU. Financial entities authorised or registered in Member States fall within DORA's scope regardless of where their parent companies are domiciled. This means that the EU subsidiaries of US banking groups, for instance, must comply with DORA's requirements.

The Regulation's treatment of third-country branches reveals nuance. DORA extends to third-country ICT providers through two mechanisms: Article 30 mandates DORA-compliant contractual terms in all ICT arrangements; and Articles 31–44 establish direct EU oversight of designated critical providers, with Article 31(12) requiring non-EU providers to establish an EU subsidiary within 12 months of designation.

2.3 The Five Pillars of DORA

DORA's substantive requirements organise into five thematic 'pillars' corresponding to Chapters II through V of the Regulation. These pillars create an integrated framework addressing the full lifecycle of ICT risk management.

2.3.1 First Pillar: ICT Risk Management Framework (Articles 5-16)

Chapter II establishes comprehensive ICT risk management requirements applicable to all financial entities. Article 6 mandates an internal governance and control framework ensuring effective and prudent management of ICT risk, with clear allocation of ICT risk management responsibilities at all organisational levels.

Articles 8 through 13 prescribe specific elements of the ICT risk management framework. Financial entities must implement policies for identifying all ICT risk, including risks to data integrity and availability, risks from third-party dependencies, and risks from ICT legacy systems.

Response and recovery measures must enable rapid response to incidents and ensure timely recovery of ICT services. Article 14 addresses communication requirements, mandating that financial entities establish crisis communication plans for ICT-related incidents.

Article 13 establishes learning mechanisms. Financial entities must implement processes to identify lessons from ICT-related incidents, vulnerabilities, and near-misses. Article 15 addresses further harmonisation through

regulatory technical standards, while Article 16 provides a simplified ICT risk management framework for smaller and less complex entities.

2.3.2 Second Pillar: ICT-Related Incident Management and Reporting (Articles 17-23)

Chapter III establishes a comprehensive framework for managing and reporting ICT-related incidents, creating harmonised incident notification procedures across the EU financial sector. Article 17 requires financial entities to establish and implement an ICT-related incident management process for detecting, managing, and notifying ICT-related incidents. The harmonised reporting architecture established by Article 19 comprises three distinct phases: an initial notification delivering preliminary information upon incident awareness, intermediate updates outlining operational status, and a final report assessing systemic impact and implemented corrective measures.

Initial notification must occur within four hours of the incident’s classification as major and, in any event, no later than 24 hours after the financial entity becomes aware of it. An intermediate report follows within 72 hours of the initial notification, with further updates required upon material status changes, and a final report is due within one month of the submission of the intermediate report.

Article 19 also addresses the voluntary notification of significant cyber threats: financial entities may notify competent authorities of significant cyber threats to which they are exposed, even where such threats have not materialised into actual incidents. The ESAs’ implementing technical standards on incident reporting provide detailed specifications for the content, format, and taxonomies of incident reports.

Beyond this pillar’s reporting framework, Article 45 — located in Chapter VI of the Regulation — permits voluntary reciprocal information sharing on cyber threats, vulnerabilities, and incidents through trusted communities. Participation remains voluntary but benefits from legal clarity that good-faith sharing does not breach contractual or regulatory information restrictions.

2.3.3 Third Pillar: Digital Operational Resilience Testing (Articles 24-27)

Chapter IV mandates comprehensive testing of ICT systems, tools, and processes to assess operational resilience and identify vulnerabilities before they can be exploited. The testing framework encompasses multiple methodologies: vulnerability assessments, network security assessments, gap analyses, physical security reviews, source code reviews, scenario-based testing, compatibility testing, performance testing, and end-to-end testing.

Article 25 addresses the frequency and scope of testing. Financial entities must conduct tests at least annually, with frequency increasing based on risk profile. Article 26 introduces advanced testing for systemically important financial entities through threat-led penetration testing (TLPT).

Mandatory TLPT applies to systemically important institutions (G-SIIs and O-SIIs) and critical financial market infrastructures, at minimum every three years, with competent authorities able to require higher frequency. Smaller but significant entities may be subject to TLPT, though proportionality considerations typically allow pooled testing arrangements. TLPT involves three phases: preparation (threat intelligence gathering and team

assembly), testing (controlled cyber attack simulation using realistic TTPs), and closure (findings analysis, remediation planning, and reporting).

Article 27 establishes requirements for testing by ICT third-party service providers. Where financial entities rely on third-party providers for critical or important functions, testing must extend to the third party's systems and processes.

2.3.4 Fourth Pillar: Third-Party ICT Risk Management (Articles 28-30)

Chapter V, Section I addresses ICT third-party risk management—a critical component given financial institutions' extensive reliance on external technology providers. Article 28 requires financial entities to manage ICT third-party risk as an integral part of their overall ICT risk management framework. Financial entities must maintain a register of all contractual arrangements for ICT services specifying: provider identification, contract duration, description of services, data storage and processing locations, and whether the arrangement supports critical or important functions.

Article 28(4) requires financial entities to assess, before entering into contractual arrangements, whether third-country providers create obstacles to effective supervision, particularly where the US CLOUD Act or analogous regimes may impair supervisory access to information or investigations. Where such obstacles exist, entities must implement remedial measures or consider alternative arrangements.

Article 29 requires financial entities to identify and assess concentration risk from collective reliance on a small number of dominant ICT providers, including at provider, technology, and geographic levels. The ESAs monitor sectoral concentration risk and may issue recommendations to address systemic vulnerabilities.

Article 30 establishes detailed requirements for contractual arrangements with ICT third-party service providers. This article represents one of DORA's most prescriptive provisions and merits detailed examination due to its extraterritorial implications. Article 30(2) imposes a series of mandatory contractual terms that, taken together, represent one of the most prescriptive elements of DORA's entire framework, addressing several distinct categories of requirement that can usefully be grouped into four clusters covering scope and performance, data protection, oversight and exit, and continuity and notification.

The first cluster concerns the scope and performance of the services themselves. Contracts must provide a clear and complete description of all functions and ICT services to be provided, including whether subcontracting is permitted and, if so, under what conditions, specifying the locations where data will be processed and stored, the locations from which ICT services will be provided, and any cross-border data transfers involved. They must also set out service level agreements defining availability targets, performance benchmarks, and quality standards that are specific, measurable, and aligned with the criticality of the supported functions, together with the remedies available to the financial entity should the third-party provider fail to meet agreed service levels.

The second cluster addresses data protection. Contracts must contain full specifications regarding data availability, authenticity, accuracy, integrity, and protection, covering encryption requirements, backup arrangements, data retention periods, and the procedures for data return or secure deletion upon contract termination — provisions that anticipate, and are designed to prevent, exactly the kind of data-handling ambiguity that has historically complicated the unwinding of large outsourcing relationships.

The third cluster concerns oversight and exit. Contracts must grant extensive access and audit rights to the financial entity, its appointed auditors, and competent authorities, and they must establish termination rights enabling the financial entity to exit the arrangement under specified circumstances, including material breach, deterioration in the provider's financial condition, or regulatory intervention; these termination provisions must be realistic and executable in practice, not merely theoretical entitlements that prove impossible to exercise when actually needed.

The fourth and final cluster addresses continuity and notification. Contracts must set out detailed exit strategies ensuring business continuity should the arrangement terminate, specifying the transition assistance the provider will furnish, including data extraction, documentation transfer, and temporary continued service during migration to an alternative provider, alongside requirements for business continuity and disaster recovery that bind the third-party provider to maintain and test its own operational resilience capabilities, with defined recovery time and recovery point objectives. Finally, contracts must mandate prompt incident notification by third-party providers regarding any disruptions, vulnerabilities, or threats affecting ICT services, thereby enabling the financial entity to satisfy its downstream statutory reporting requirements under Articles 17 to 23.

These contractual requirements fundamentally alter the dynamics of ICT procurement for EU financial institutions. Prior to DORA, contract terms were largely a matter of commercial negotiation, with large technology providers often imposing standardised terms that financial institutions, despite their regulatory obligations, accepted.

Article 30 operates through private contract rather than direct regulatory assertion. DORA regulates EU financial entities, which must impose specific contractual terms on service providers.

2.3.5 Fifth Pillar: Oversight Framework for Critical Third-Party Providers (Articles 31-44)

Chapter V, Section II establishes DORA's most innovative and controversial provision: direct EU oversight of critical ICT third-party service providers. This framework extends regulatory authority beyond traditional financial institutions to technology companies, marking a significant expansion of financial services regulation's perimeter.

Article 31 defines the criteria and process for designating ICT third-party service providers as ‘critical’. Designation occurs where a provider’s failure or severe operational disruption would pose systemic risk to the EU financial system, and the ESAs assess this question against four interrelated factors.

The first factor is systemic impact: whether the failure of the ICT third-party service provider would cause disruption to financial entities or financial markets at a level likely to have serious negative consequences. The second is the systemic importance of dependent financial entities, measured by the number, nature, and systemic relevance of the financial entities that rely on the provider for critical or important functions — a designation is more likely where the provider’s client base includes globally systemically important institutions than where it serves only smaller, less interconnected firms.

The third factor is the degree of reliance for critical or important functions, capturing how deeply financial entities depend on the provider for operations essential to their functioning, as opposed to peripheral or easily substitutable services. The fourth and final factor is the degree of substitutability: the availability of alternative providers capable of furnishing equivalent services. Where multiple providers offer comparable services and switching costs remain manageable, designation may be less warranted than where a provider maintains a near-monopoly position or possesses unique capabilities that would be difficult or impossible to replicate elsewhere in the market.

Article 31(4) establishes the designation procedure. The ESAs (EBA, EIOPA, ESMA acting jointly) conduct the assessment based on information submitted by financial entities through their competent authorities and information gathered directly from ICT third-party service providers. Once the ESAs officially designate an ICT provider as critical, Article 31(12) enforces a structural prerequisite: non-EU critical third-party vendors are legally required to establish a corporate subsidiary within the Union within 12 months.

The EU subsidiary requirement raises practical and legal questions. The subsidiary must be adequately capitalised, maintain real governance, and have sufficient authority over the parent’s provision of services to EU clients to render oversight meaningful — a brass-plate entity would not satisfy DORA’s objectives. Article 32 establishes the Structure of the Oversight Framework, including the Oversight Forum, which brings together the ESAs and relevant national competent authorities.

Article 35 establishes the Lead Overseer’s powers, which parallel supervisory authorities’ powers over traditional financial entities and are elaborated further across Articles 36 to 41. Article 37 grants power to request information from critical ICT third-party service providers, while Article 38 authorises general investigations: where the Lead Overseer has reason to believe a critical provider may pose risks to financial stability or fail to comply with oversight recommendations, it may conduct investigations requiring the provider to produce documents, submit staff to interviews, and provide explanations of its activities and risk management practices.

Article 39 permits on-site inspections. The Lead Overseer may enter the critical provider’s business premises to examine books, records, procedures, and ICT systems.

Article 35 also establishes the Lead Overseer's core oversight mechanism: recommendations. Under this oversight framework, information synthesised from official requests, investigations, and physical inspections enables the Lead Overseer to issue strategic recommendations to designated critical ICT third-party providers regarding risks to financial stability or broader operational resilience.

Critically, Article 35 imposes a 'comply or explain' obligation on recipients of these recommendations. Critical providers must either implement the Lead Overseer's recommendations or provide written explanations for non-compliance. If the Lead Overseer finds the explanation inadequate or non-compliance persists, the same article authorises pecuniary remedies.

Article 35 empowers the Lead Overseer to impose periodic penalty payments on critical ICT third-party service providers that fail to comply with recommendations without adequate justification. Penalties may reach up to 1% of the provider's average daily worldwide turnover, calculated based on the preceding business year, for each day of non-compliance for up to six months. Article 40 further establishes an ongoing oversight obligation, requiring the Lead Overseer to monitor designated critical providers on a continuing basis rather than through one-off assessments.

Article 43 establishes oversight fees. Critical ICT third-party service providers must pay fees to the ESAs to cover the costs of oversight activities. Fees are calculated based on the provider's annual revenue attributable to ICT services provided to EU financial entities, ensuring that oversight costs are borne by those subject to oversight rather than taxpayers.

The oversight framework's extraterritorial dimension extends beyond the EU subsidiary requirement. Even where providers establish EU subsidiaries, questions arise regarding the territorial scope of ESA examination powers over operations conducted outside the EU.

2.4 DORA's Extraterritorial Reach

DORA's extraterritorial reach operates through multiple complementary mechanisms, collectively creating substantial pressure for global alignment with EU operational resilience standards. Understanding these mechanisms is essential to assessing whether DORA will drive convergence in US regulatory approaches.

Article 31(12)'s EU subsidiary requirement is the principal direct extraterritorial mechanism: non-EU critical ICT third-party service providers must establish an EU subsidiary within 12 months of designation. The legal basis derives from the EU's internal market competence and authority to regulate entities operating within the EU financial system.

From a public international law perspective, DORA's approach aligns with the effects doctrine recognised in competition law and financial regulation. Where foreign conduct produces substantial effects within a jurisdiction's territory, international law generally permits that jurisdiction to prescribe rules governing such conduct.

The indirect extraterritorial mechanism operates through Article 30's mandatory contractual provisions. As analysed above, Article 30 requires EU financial entities to impose specific contractual terms on all ICT third-party service providers, including those domiciled outside the EU.

The contractual cascade mechanism represents territorial extension rather than genuine extraterritoriality. The EU directly regulates only EU financial entities, not the US providers themselves.

Market access conditioning constitutes a third extraterritorial mechanism. Non-EU ICT service providers wishing to serve EU financial institution clients face a choice: accept DORA-compliant contractual terms and potentially submit to EU oversight if designated as critical, or forgo the EU market.

Because cloud infrastructure cannot be structurally partitioned, DORA's extraterritorial mandates exert amplified compliance pressures on foreign providers. Providers operate global platforms with shared infrastructure and standardised procedures. Maintaining separate EU-compliant and non-EU operational regimes would require costly duplication that, for governance and incident response capabilities, may be technically infeasible. This non-divisibility creates incentives for global standardisation around EU requirements.

DORA's extraterritorial reach extends even to providers not serving EU clients directly but positioned as subcontractors in the service delivery chain. Article 30(2)(a) requires that contracts specify whether subcontracting is permitted and, if so, require that subcontractors comply with DORA-equivalent standards.

Comparing DORA's extraterritoriality to the GDPR reveals both similarities and differences. Both Regulations extend EU standards globally through a combination of direct requirements (GDPR's Article 3 territorial scope; DORA's Article 31(12) subsidiary requirement) and contractual transmission (GDPR's processor requirements; DORA's Article 30 contractual provisions). DORA's direct oversight under Articles 31–44 applies only to designated critical providers, unlike GDPR which extends to all entities processing EU personal data.

2.5 Penalties and Enforcement

DORA's enforcement framework combines administrative penalties, supervisory measures, and potential criminal sanctions to ensure compliance with operational resilience requirements. For financial entities, Article 50 does not itself prescribe fine levels: it instead requires Member States to lay down administrative penalties and remedial measures that are effective, proportionate, and dissuasive, and to confer on competent authorities a minimum set of powers, including cease-and-desist orders, measures of a pecuniary nature, and public notices. The resulting national penalty regimes diverge considerably in their turnover-based ceilings and absolute caps — a notable pocket of fragmentation within an otherwise harmonising Regulation.

For critical ICT third-party service providers, Article 35(6) authorises the Lead Overseer to impose periodic penalty payments of up to 1% of the provider's average daily worldwide turnover, applied for each day of non-compliance for up to six months, including where a provider fails to comply with oversight measures or to establish an EU subsidiary within the required 12-month period. Article 51 in turn directs competent authorities, when determining the type and level of penalties imposed on financial entities, to take account of circumstances such as the materiality, gravity, and duration of the breach and the responsibility and financial strength of the person concerned.

The penalty structure reflects DORA's dual regulatory architecture. For financial entities, penalties operate through national competent authorities—the same supervisors responsible for prudential oversight. This ensures coordination between operational resilience enforcement and broader supervisory activities.

Article 50(5) addresses personal liability, empowering competent authorities to hold members of financial entities' management bodies personally liable for failures in ICT risk management or operational resilience where national law so permits.

Article 52 preserves Member States' authority to impose criminal penalties for DORA violations, recognising that some breaches may warrant criminal rather than merely administrative sanction under national law. Beyond monetary penalties, competent authorities possess various supervisory measures. For critical ICT third-party service providers, the Lead Overseer's primary enforcement tool is recommendations combined with periodic penalty payments for non-compliance.

The ultimate enforcement mechanism — not expressly articulated in DORA — is market exclusion. Persistent non-compliance with oversight recommendations could lead competent authorities to require financial entities to transition to alternative providers, using their general powers to ensure safety and soundness.

CHAPTER 3: US OPERATIONAL RESILIENCE REGULATORY FRAMEWORK

In contrast to DORA's comprehensive and harmonised approach, the United States maintains a markedly fragmented operational resilience framework, one that reflects its broader regulatory architecture of overlapping federal agencies, coordination mechanisms that encourage rather than mandate uniformity, and a longstanding institutional preference for principles-based guidance over prescriptive rulemaking. This chapter examines that framework in detail, mapping the institutional landscape, analysing the principal guidance documents and rules that govern operational resilience, and comparing the resulting US approach systematically against DORA's five pillars.

3.1 Overview of US Financial Regulatory Structure

The United States regulates financial institutions through a complex, multi-layered system that divides supervisory authority among numerous federal agencies and state regulators, a structure that stands in sharp contrast to the unified architecture established by DORA. At the federal level, banking regulation divides primarily among three agencies. The Office of the Comptroller of the Currency, housed within the Department of the Treasury, charters and supervises national banks and federal savings associations, while the Federal Reserve governs bank holding companies, state member banks, and foreign banking organisations operating within the United States.

This division of labour produces overlapping jurisdiction even within a single corporate group: JPMorgan Chase Bank NA, the operating bank subsidiary, falls under OCC supervision, while JPMorgan Chase & Co, the parent holding company, falls under Federal Reserve supervision. The Federal Deposit Insurance Corporation completes the trio of primary banking regulators, supervising state-chartered banks that are not members of the Federal Reserve System, together with certain savings associations.

Beyond banking, securities regulation operates through the Securities and Exchange Commission, which oversees exchanges, broker-dealers, investment advisers, and public company disclosure, and the Commodity Futures Trading Commission, which regulates derivatives markets. Neither agency possesses comprehensive authority over operational resilience standards applicable across the entire financial sector. A further layer of complexity arises from the Financial Industry Regulatory Authority, which, although technically a private self-regulatory organisation, exercises quasi-governmental authority over broker-dealers under SEC oversight, promulgating rules, conducting examinations, and enforcing compliance for its approximately 3,400 member firms.³⁵

State regulators retain significant authority over insurance companies, state-chartered banks, and various non-bank financial entities, a division that reflects constitutional federalism but adds yet another layer of jurisdictional complexity to an already fragmented landscape. The practical consequence is that a major operational disruption

³⁵ Financial Industry Regulatory Authority, FINRA Rule 3110 (Supervision).

at a large banking organisation could simultaneously implicate the OCC, the Federal Reserve, the FDIC, the SEC, and the CFTC, with no single agency possessing comprehensive authority to mandate operational resilience standards across the entire financial sector.

Some coordination does exist. The Federal Financial Institutions Examination Council, established in 1979 and comprising the OCC, the Federal Reserve, the FDIC, the National Credit Union Administration, and the Consumer Financial Protection Bureau, develops uniform examination principles through its IT Examination Handbook.³⁶ These principles, however, constitute guidance rather than binding regulation, and each member agency retains discretion in how it applies them. Constitutional and political constraints further impede more ambitious reform: proposals to consolidate banking supervision under a single federal regulator have circulated periodically since the 2008 financial crisis but have repeatedly failed to gain political traction. The result is an institutional landscape in which, unlike the EU's unified ESA architecture, no single US agency can mandate operational resilience standards applicable across the entire financial sector, leaving the system to rely on coordination mechanisms that remain fundamentally voluntary in nature.

3.2 Key US Operational Resilience Guidance and Rules

Despite this institutional fragmentation, US banking regulators have developed substantial operational resilience frameworks, primarily through supervisory guidance rather than formal rulemaking. This section examines the key components of that architecture in turn, before Section 3.3 draws the threads together in a systematic comparison with DORA.

3.2.1 Federal Reserve and OCC: Sound Practices to Strengthen Operational Resilience (2020)

In October 2020, the Federal Reserve, the OCC, and the FDIC jointly issued 'Sound Practices to Strengthen Operational Resilience', published respectively as SR Letter 20-24, OCC Bulletin 2020-94, and FDIC FIL-103-2020.³⁷ The guidance articulates seven core principles that together form the backbone of US supervisory expectations for operational resilience. Governance sits at the foundation: banking organisations must establish clear governance structures, with the board of directors and senior management bearing responsibility for setting strategy, allocating resources, and overseeing implementation. Building on this foundation, organisations must maintain comprehensive operational risk management frameworks capable of identifying, measuring, monitoring, and controlling risks arising from technology failures, cyber threats, third-party dependencies, and natural disasters.

The remaining principles address the practical mechanics of resilience. Organisations must develop and maintain business continuity plans that enable the rapid resumption of critical operations following disruption, and they

³⁶ Federal Financial Institutions Examination Council, 'IT Examination Handbook' <<https://ithandbook.ffiec.gov>> accessed 30 June 2026.

³⁷Federal Reserve, OCC and FDIC, 'Sound Practices to Strengthen Operational Resilience' (n 2).

must map the interconnections and dependencies among business lines, legal entities, systems, and service providers so as to understand how disruptions propagate through the organisation. Particular attention is paid to third-party dependency management, reflecting growing supervisory concern about reliance on external technology providers, alongside requirements that information systems be designed, implemented, and maintained with appropriate security controls, redundancy, and recovery capabilities. The final principle, surveillance and reporting, requires organisations to monitor their operational resilience posture through key risk indicators and incident tracking, with material operational incidents reported to senior management and, where appropriate, to supervisors and other stakeholders.

An accompanying appendix to the guidance provides additional detail on cyber risk management, incorporating principles drawn from prior cybersecurity guidance and addressing governance, risk assessment, cyber threat intelligence, security awareness training, access controls, incident response planning, and resilience testing. Taken as a whole, this principles-based architecture contrasts sharply with DORA's prescriptive, rule-bound approach, a divergence that reflects both regulatory philosophy and underlying legal constraints. US banking agencies have traditionally favoured risk-based supervision that accommodates institutional diversity, and supervisory guidance offers a speed and flexibility that formal notice-and-comment rulemaking under the Administrative Procedure Act cannot match.³⁸

This legal status as supervisory expectations rather than binding rules carries significant practical implications. Violation of the guidance does not, in itself, constitute a violation of law; rather, supervisors may treat inadequate operational resilience practices as unsafe or unsound banking practices, exposing institutions to enforcement action through that more indirect route rather than through direct sanction for non-compliance with the guidance itself.

3.2.2 Computer-Security Incident Notification Rule (2021)

In November 2021, the Federal Reserve Board, the OCC, and the FDIC jointly adopted a final rule establishing computer-security incident notification requirements for banking organisations, codified at 12 CFR Part 53.³⁹ This rule represents a comparatively rare instance of formal rulemaking in the US operational resilience landscape, standing in contrast to the agencies' typical reliance on supervisory guidance. The rule defines a 'notification incident' as one that has materially disrupted, or is reasonably likely materially to disrupt, banking operations or the ability to deliver services to a material portion of the customer base, and it triggers a 36-hour notification obligation to the institution's primary federal regulator once such a determination has been made.

Notably, the 36-hour window begins not when the incident first occurs but when the banking organisation determines that a notification incident has taken place, a distinction that gives institutions some latitude in conducting an initial assessment before the clock formally starts. Bank service providers, defined as entities

³⁸ Administrative Procedure Act 1946, 5 USC § 553.

³⁹ Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 12 CFR pt 53 (effective 1 May 2022).

performing services for banking organisations under the Bank Service Company Act, face a complementary notification obligation of their own, ensuring that incidents affecting outsourced functions are not left outside the reporting net.

The underlying purpose of these requirements is to establish a supervisory early warning system: by learning of incidents quickly, regulators can assess potential systemic implications, coordinate with other affected institutions, and provide supervisory support during incident response. Measured against DORA's incident reporting framework, however, the US rule reveals significant gaps. DORA establishes harmonised reporting templates, specifies detailed content requirements, mandates initial notification within four hours and a final report within one month, and channels all reports through a centralised mechanism operated by the ESAs.⁴⁰ The US rule, by comparison, imposes only a bare 36-hour notification obligation without prescribing format, content, or any mechanism for cross-agency aggregation of the resulting data.

3.2.3 Interagency Guidance on Third-Party Relationships: Risk Management (2023)

In June 2023, the Federal Reserve Board, the OCC, and the FDIC jointly issued updated interagency guidance on managing risks associated with third-party relationships.⁴¹ This guidance superseded prior guidance dating from 2013, reflecting the evolving landscape of third-party dependencies and, in particular, the dramatic increase in reliance on cloud computing and other outsourced technology services over the intervening decade. The 2023 guidance applies to all banking organisations regardless of size, though it emphasises throughout that risk management practices should be commensurate with the level of risk and complexity presented by each third-party relationship, a proportionality principle that recurs across much of the US framework.

The guidance organises third-party risk management around a lifecycle of five stages. During the planning stage, banking organisations are expected to conduct risk assessments to determine whether to outsource an activity at all and, if so, which third parties to consider; for activities deemed 'critical' to the organisation's operations, planning should identify the potential impact of third-party failure and assess whether adequate alternative providers exist. Due diligence follows, assessing the prospective third party's financial condition, operational capabilities, information security practices, business continuity planning, regulatory compliance record, and reputation.

The third phase centers on contract negotiation, a process that establishes the baseline for service delivery and governance by regulating performance metrics, audit authority, information security, operational resilience frameworks, and termination or dispute mechanisms. Crucially, the guidance frames these as risk management considerations to be addressed through negotiated contracts, not as mandatory contractual terms imposed by regulation — a structural distinction that marks one of the sharpest points of divergence from DORA's Article 30, which specifies mandatory contractual content.

⁴⁰ DORA (n 1) arts 17-23.

⁴¹ Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation, 'Interagency Guidance on Third-Party Relationships: Risk Management' (6 June 2023).

Ongoing monitoring, the fourth stage, tracks the third party's performance against contractual commitments, assesses changes in its risk profile, reviews audit reports and certifications, and evaluates the banking organisation's continued reliance on the relationship. Termination planning, the final stage, ensures that banking organisations can exit third-party relationships without disrupting critical operations; contracts are expected to specify the transition assistance the third party will provide, including data return, documentation transfer, and continued service during migration to alternative providers or in-sourcing. The guidance also addresses concentration risk, echoing concerns central to DORA, but its status as supervisory expectations rather than binding requirements creates flexibility at the cost of legal certainty.

3.2.4 SEC: Cybersecurity Risk Management Rules (2023-2024)

The Securities and Exchange Commission has developed its own operational resilience framework for entities under its jurisdiction, one that diverges in several respects from the banking agencies' approach. In July 2023, the SEC adopted final rules requiring public companies to disclose material cybersecurity incidents on Form 8-K within four business days of determining that an incident is material, alongside an annual disclosure requirement covering cybersecurity risk management, strategy, and governance in Form 10-K annual reports.⁴²

For incident disclosure, companies must describe the material aspects of the incident's nature, scope, and timing, together with its material impact or reasonably likely material impact on the company. The annual disclosure requirement, by contrast, addresses companies' cybersecurity risk management processes, board oversight of cybersecurity risks, and management's role and expertise in assessing and managing those risks — a structural pairing of incident-specific and ongoing governance disclosure that has no direct counterpart in the banking agencies' guidance.

In October 2023, the SEC extended this framework further by adopting amendments to Regulation S-P that expand data breach notification requirements for broker-dealers, investment advisers, and other regulated entities.⁴³ For broker-dealers and investment advisers specifically, the SEC has also proposed rules requiring annual reporting of significant operational events, including cybersecurity incidents, though these proposals do not extend to third-party oversight of the kind found in DORA. The SEC's overall approach emphasises disclosure to investors and clients over supervisory notification, a choice that reflects the Commission's statutory mandate to protect investors and ensure market transparency, in contrast to the banking agencies' focus on safety and soundness supervision.

3.2.5 Other Relevant Frameworks

Beyond the primary guidance and rules examined above, several additional frameworks shape US financial institutions' operational resilience practices. While these frameworks lack the legal force of regulations or the

⁴² Securities and Exchange Commission, Final Rule, 'Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure' Release No 33-11216 (26 July 2023), codified at 17 CFR § 229.106 (Item 106 of Regulation S-K).

⁴³ Securities and Exchange Commission, Final Rule, 'Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information' Release No 34-98990 (16 May 2024).

supervisory weight of formal guidance, they provide important standards and benchmarks that institutions draw upon in practice. The National Institute of Standards and Technology Cybersecurity Framework, first published in 2014 and substantially updated in 2024, organises cybersecurity activities into six core functions — Govern, Identify, Protect, Detect, Respond, and Recover — and has become a widely referenced, if voluntary, benchmark across the financial sector.⁴⁴

The Cybersecurity and Infrastructure Security Agency provides guidance, threat intelligence, and incident response support for financial services, its authority expanded in recent years by Presidential executive orders on cybersecurity; even so, CISA's role remains primarily advisory. A parallel example of industry self-organisation can be found in information-sharing through the Financial Services Information Sharing and Analysis Center, which operates without any regulatory mandate behind it.⁴⁵

At the state level, insurance regulators coordinated through the National Association of Insurance Commissioners have developed the Insurance Data Security Model Law, requiring comprehensive information security programmes and incident response plans.⁴⁶ Because adoption proceeds state by state, the result is a patchwork of requirements, though the core elements remain relatively consistent across adopting jurisdictions. FINRA, for its part, maintains cybersecurity and technology governance requirements for broker-dealers under Rule 3110, which requires firms to maintain supervisory systems reasonably designed to achieve regulatory compliance — a further illustration of how authority over operational resilience in the United States is distributed across sector-specific regulators rather than consolidated in a single body.⁴⁷

Finally, the Bank Secrecy Act and Anti-Money Laundering framework imposes its own technology requirements on financial institutions through transaction monitoring and suspicious activity reporting obligations.⁴⁸ Although these requirements are not designed primarily with operational resilience in mind, they nonetheless compound the overall fragmentation of the US landscape: institutions must navigate a patchwork of standards drawn from banking supervision, securities regulation, state insurance law, self-regulatory rules, and financial crime compliance, each developed independently and pursuing its own regulatory objectives.

3.3 Comparative Analysis: US vs. DORA

Comparing the US operational resilience framework with DORA reveals fundamental differences across legal form, regulatory philosophy, institutional structure, and substantive requirements. In legal form, DORA operates as a directly applicable Regulation supplemented by binding technical standards, whereas the US framework

⁴⁴ National Institute of Standards and Technology, 'The NIST Cybersecurity Framework (CSF) 2.0' (26 February 2024) <<https://doi.org/10.6028/NIST.CSWP.29>> accessed 30 June 2026.

⁴⁵ Financial Services Information Sharing and Analysis Center, 'DORA Implementation Guide for FS-ISAC Members' (FS-ISAC, September 2024).

⁴⁶ National Association of Insurance Commissioners, 'Insurance Data Security Model Law' (MDL-668, adopted 2017).

⁴⁷ FINRA (n 35).

⁴⁸ Bank Secrecy Act 1970, 31 USC § 5311 et seq.

consists primarily of supervisory guidance, with only isolated instances of formal rulemaking on specific issues such as incident notification and SEC disclosure.

In regulatory philosophy, DORA is prescriptive, specifying ICT risk management requirements, testing methodologies, incident reporting formats, and mandatory contractual terms in considerable detail. US guidance, by contrast, is principles-based, articulating supervisory expectations while leaving the specifics of implementation to institutional judgement. In harmonisation, DORA creates uniform requirements across all twenty-seven Member States and twenty-one categories of financial entities, eliminating regulatory arbitrage by design; the US framework, by contrast, varies by agency — banking, broker-dealer, investment adviser, and insurance sectors each face different requirements — and even within banking, requirements vary further by institution size.

Most significantly, the two frameworks diverge sharply on third-party oversight. DORA empowers the ESAs to designate critical providers, require the establishment of EU subsidiaries, conduct direct inspections, and impose penalties. The US framework offers no comparable mechanism: regulators supervise financial institutions' management of third-party risk but possess no authority to examine or regulate the providers themselves. This absence of direct third-party oversight reflects both legal and philosophical constraints. Banking agency examination authority does not extend to cloud providers, which fall outside the scope of the Bank Service Company Act, and extending such authority would require new Congressional legislation — a step that, as discussed further in Section 3.4, faces substantial political obstacles. The table below summarises these points of comparison across the principal dimensions of operational resilience regulation.

Dimension	DORA (EU)	US Framework
Legal Nature	Directly applicable Regulation with force of law; supplemented by regulatory technical standards	Primarily supervisory guidance; limited rules on specific issues (incident notification, SEC disclosure)
Approach	Prescriptive, detailed requirements	Principles-based, supervisory expectations
Harmonisation	Uniform across EU-27 and 21 categories of financial entities	Fragmented across agencies; varies by institution type and size
Scope	All financial entities; comprehensive coverage	Large banking organisations for main guidance; varies by agency for others

Third-Party Oversight	Direct EU oversight of critical third-party providers via ESAs	Indirect only—institutions manage third-party risk; no direct provider oversight
Contractual Requirements	Mandatory terms specified in Article 30	General risk management considerations; terms negotiated
Testing Requirements	Mandatory TLPT for significant entities; three-year cycle	Testing encouraged; no mandatory methodologies or timelines
Incident Reporting	Harmonised templates, timelines, and aggregation	36-hour notification (banking); 4-day disclosure (SEC); no harmonised templates
Penalties	Set by Member States (national regimes vary); periodic penalties up to 1% of average daily worldwide turnover (CTPPs)	Varies by violation; enforcement discretion; no specified maximums in guidance
Extraterritoriality	Strong: EU subsidiary requirement for CTPPs; contractual cascade	Limited: territorial jurisdiction; no extraterritorial assertions

This comparative table illuminates the profound differences between the EU and US approaches. DORA represents a comprehensive, prescriptive, and harmonised regulatory regime with direct third-party oversight and a strong extraterritorial reach, while the US framework remains fragmented, principles-based, and confined to indirect oversight exercised only through the financial institutions that contract with third-party providers. These structural differences form the analytical backbone for the discussion of extraterritorial influence and convergence pressures that follows in Chapters 4 and 5.

3.4 Gaps and Weaknesses in US Framework

The US operational resilience framework's fragmented, principles-based character produces several significant gaps and weaknesses when measured against DORA's comprehensive approach. The most consequential of these concerns the absence of any mechanism for direct regulatory oversight of critical ICT third-party providers. The Bank Service Company Act provides only limited authority over certain service providers, and cloud platforms typically structure their relationships with financial institutions in ways that fall outside even this narrow scope.⁴⁹ As a result, US regulators can assess how well a bank manages its relationship with a cloud provider, but they

⁴⁹ Bank Service Company Act 1962, 12 USC § 1861 et seq.

cannot examine the cloud provider itself — a structural gap that DORA’s Articles 31 to 44 were specifically designed to close.

A second weakness flows from the guidance-based approach itself, which creates uncertainty and inconsistency in practice. Banking organisations understand that supervisors expect robust third-party risk management, yet they often lack clear, codified standards for what ‘robust’ means in any given context. This ambiguity falls unevenly across the sector: large banks can navigate principles-based guidance by erring toward comprehensive implementation, absorbing the resulting compliance costs as a matter of course, whereas smaller institutions with more limited resources struggle to calibrate against an undefined supervisory expectations floor, making proportionate compliance considerably harder to achieve in practice.

Testing requirements present a further point of contrast. US guidance encourages institutions to test their operational resilience capabilities but mandates no particular methodology, frequency, or documentation standard, leaving testing rigour largely to institutional discretion. DORA, by comparison, requires threat-led penetration testing for significant institutions on a structured three-year cycle under the TIBER-EU framework, with detailed methodological requirements specified centrally.⁵⁰ Incident reporting reveals a similar pattern of fragmentation: the Computer-Security Incident Notification Rule requires banking organisations to notify their primary regulator within thirty-six hours but specifies no standardised template, in sharp contrast to DORA’s harmonised incident reporting framework, in which all major ICT-related incidents are reported through standardised templates to competent authorities, with the ESAs maintaining centralised visibility across the entire EU financial sector.⁵¹

Coverage gaps compound these structural weaknesses. Smaller banks, credit unions, non-bank financial institutions, fintech companies, and digital asset exchanges may face less comprehensive supervisory expectations or fall outside traditional regulatory perimeters altogether, leaving meaningful portions of the financial ecosystem only thinly covered by any operational resilience standard. Voluntary frameworks such as the NIST Cybersecurity Framework, while valuable as a point of reference, lack legal force and therefore cannot substitute for binding requirements where institutions choose not to adopt them.

Political obstacles compound these technical and institutional gaps. Congressional gridlock, combined with sustained industry lobbying against prescriptive operational resilience requirements, makes comprehensive DORA-equivalent legislation politically infeasible for the foreseeable future, and a broader anti-regulatory sentiment within certain constituencies further constrains the appetite for reform.⁵² None of this is to suggest that US financial institutions lack meaningful operational resilience capabilities: many large banks invest heavily in cybersecurity, business continuity planning, and third-party risk management as a matter of competitive necessity and prudent risk management, regardless of the precise regulatory floor beneath which they operate. The point, rather, is structural: where DORA establishes a uniform, enforceable, and directly supervised baseline across the

⁵⁰ DORA (n 1) arts 24-27.

⁵¹ DORA (n 1) arts 17-23.

⁵² Administrative Procedure Act (n 38).

entire EU financial sector, the US relies on a patchwork of guidance, voluntary standards, and institution-specific practice that varies considerably in rigour and that leaves the providers at the centre of the financial system's technological infrastructure beyond the direct reach of any single regulator.

CHAPTER 4: MECHANISMS OF EXTRATERRITORIAL INFLUENCE AND THE BRUSSELS EFFECT

4.1 Theoretical Framework: The Brussels Effect Applied to Financial Regulation

Anu Bradford's Brussels Effect theory provides a framework for assessing whether DORA will drive global regulatory convergence despite the EU's inability to directly regulate non-EU entities. Applying Bradford's five conditions to DORA illuminates both the mechanism's potential and its limitations.

4.1.1 Condition One: Market Size

The first condition requires that the EU constitute a sufficiently large market that global firms cannot afford to forgo access. For DORA, this assessment occurs at two levels: the EU financial services market itself and the EU's share of global cloud computing and ICT services revenue. EU financial institutions hold approximately €33 trillion in banking assets (~20–25% of global banking assets), with the world's second-largest equity and bond markets and annual insurance premiums exceeding €1.3 trillion.

For ICT service providers, the calculus focuses on EU financial services revenue. Industry estimates suggest the Big Three cloud providers collectively generate several billion euros annually from EU financial institutions.

The relevant question is whether the EU market is large enough that foregoing it is commercially unacceptable. For large US cloud providers serving global financial institutions, the answer is clearly yes: EU financial services revenues are material and strategically irreplaceable.

For smaller, specialised ICT providers, the calculus may differ. A US-based software vendor serving primarily domestic clients might rationally decline to pursue EU financial services business rather than accept DORA's compliance costs.

Bradford acknowledged that capital mobility poses challenges for the Brussels Effect in financial services. However, DORA targets operational infrastructure, not capital allocation. Cloud services cannot easily relocate: data localisation requirements, latency constraints for real-time trading, and EU regulatory access rights make geographical evasion impractical.

4.1.2 Condition Two: Regulatory Capacity

The second condition requires that the EU possess institutional capacity to promulgate and enforce stringent regulations. DORA demonstrates such capacity in several respects. Institutionally, the European Supervisory

Authorities provide centralised standard-setting and enforcement mechanisms absent in more fragmented jurisdictions.

Legally, DORA's status as a directly applicable Regulation eliminates implementation discretion that might dilute requirements. Member States cannot opt out of provisions, water down standards, or delay application. The Regulation's detailed prescriptive requirements further limit interpretive discretion, ensuring relatively uniform implementation across the EU. The regulatory technical standards developed by the ESAs operationalise DORA's framework, providing detailed specifications that enhance enforceability.

Enforcement capacity remains to be fully demonstrated. Periodic penalty payments up to 1% of worldwide daily turnover create substantial leverage, but whether the ESAs will exercise this power against major US technology companies — given political sensitivities and systemic importance concerns — awaits testing.

4.1.3 Condition Three: Stringency

The third condition requires that EU regulations be more stringent than those of competing jurisdictions. DORA definitely demonstrates a higher degree of regulatory stringency than comparable US frameworks. DORA's prescriptive approach — mandating specific contractual provisions, testing methodologies, reporting formats, and governance requirements — contrasts with the US principles-based approach, which articulates supervisory expectations while leaving implementation to institutional judgment. Most significantly, DORA establishes direct regulatory oversight of critical ICT third-party providers—a mechanism entirely absent from the US framework. This stringency differential creates Brussels Effect pressure: if cloud providers must meet DORA's requirements to serve EU clients, and extending those requirements globally proves more economical than maintaining dual operational regimes, DORA becomes the de facto global standard even for non-EU operations.

Potential counterarguments exist. US regulators might claim that principles-based supervision produces equivalent outcomes through tailored examination and enforcement, making formal rule differences less meaningful than they appear.

4.1.4 Condition Four: Inelastic Targets

The fourth condition requires that regulated entities have limited ability to exit the EU market or relocate operations to avoid regulation. For DORA, this assessment differs between financial entities and ICT providers.

For EU financial entities, exit is largely infeasible. An EU bank cannot relocate to avoid DORA while maintaining its EU banking license and customer base.

For US financial institutions with EU operations, DORA applies to their EU subsidiaries and branches. JPMorgan Chase's European subsidiaries must comply with DORA regardless of the parent company's US domicile. For ICT service providers, inelasticity depends on revenue concentration and alternative market opportunities.

Alternative markets exist for US cloud providers, but financial services represent strategically important clients. The combination of large contract values, long-term relationships, and reputational significance makes losing major EU financial institution clients commercially unacceptable for AWS, Azure, and Google Cloud.

The target elasticity assessment must also consider dynamic effects. If DORA successfully establishes direct oversight of critical ICT providers, and if the framework proves effective at enhancing operational resilience, other jurisdictions might adopt similar approaches.

4.1.5 Condition Five: Non-Divisibility

The fifth and perhaps most critical condition for DORA requires that compliance costs be such that firms find global standardisation more economical than maintaining separate EU-compliant and non-EU operational regimes. This non-divisibility condition proves particularly salient for cloud infrastructure and ICT services. Cloud computing operates on shared infrastructure platforms.

Certain DORA requirements resist geographic segregation. Specifically, the audit provisions within Article 30 necessitate that cloud vendors integrate data-access systems, thereby enabling both EU financial entities and their respective regulators to review comprehensive operational logs. Similarly, DORA's incident notification requirements (Article 30(3)(b)) mandate that providers notify financial entities promptly of incidents, vulnerabilities, or threats.

Governance and risk management requirements further favour non-divisibility. DORA's Lead Overseer recommendations target enterprise-level governance structures, risk frameworks, and business continuity plans that cannot easily be maintained separately for EU versus non-EU operations without operational inefficiency.

However, non-divisibility has limits. Certain DORA requirements can be geographically segregated. The EU subsidiary requirement under Article 31(12) applies only to designated critical providers serving EU clients.

The divisibility assessment depends on cost structure. Fixed-cost elements such as governance frameworks, risk management systems, and monitoring infrastructure favour global standardisation.

Empirical assessment of non-divisibility for DORA will emerge only as cloud providers and other critical ICT service providers respond to designation and oversight. Initial indications suggest that major providers are evaluating global standardisation for certain operational capabilities while maintaining geographic differentiation for contractual and compliance elements.

4.1.6 Overall Assessment: Will DORA Generate a Brussels Effect?

Applying Bradford's five conditions to DORA yields a nuanced assessment. The EU market is sufficiently large (condition one), the ESAs provide regulatory capacity (condition two), and DORA is more stringent than US frameworks (condition three). Targets are substantially inelastic (condition four), given the commercial importance of EU financial services revenue to major providers. The pivotal and most contested condition is non-

divisibility (condition five), which holds strongly for shared operational infrastructure and enterprise-level governance but only partially for contractual and compliance arrangements.

This suggests that DORA will likely generate a partial or selective Brussels Effect rather than comprehensive global regulatory convergence. Major US cloud providers (AWS, Azure, Google Cloud) will likely adopt DORA-compliant operational practices globally for fixed-cost elements like governance frameworks, incident response capabilities, and risk management systems.

The Brussels Effect framework must also account for Bradford's distinction between de facto and de jure effects. Limitations on DORA's Brussels Effect arise from several sources: US regulatory resistance (agencies may adopt divergent approaches to signal independence); geopolitical tensions in technology governance; competing regulatory poles from China, the UK and others; and political backlash risk if aggressive EU oversight triggers US legislative responses.

4.2 DORA's Extraterritorial Mechanisms in Detail

Beyond the theoretical Brussels Effect framework, DORA's extraterritorial influence operates through specific legal and commercial mechanisms that extend its reach to non-EU entities.

4.2.1 Direct Mechanism: The EU Subsidiary Requirement

Article 31(12) contains DORA's most direct extraterritorial assertion: financial entities may only make use of the services of an ICT third-party service provider established in a third country and designated as critical under Article 31(1)(a) if that provider has established a subsidiary in the Union within 12 months of the designation. This provision extends EU regulatory authority to foreign entities based solely on their commercial relationships with EU financial institutions. The EU subsidiary requirement serves three regulatory objectives: subjecting the provider to EU jurisdiction; enabling ESA examination without international legal assistance; and creating an enforcement target against which penalties and, ultimately, market restrictions can be applied.

The subsidiary must be substantive: a letterbox entity would not satisfy DORA's objectives. The ESAs' oversight assumes the subsidiary exercises meaningful authority over the parent's provision of ICT services to EU clients, controls access to those services, and can implement Lead Overseer recommendations.

For a company like Amazon Web Services, establishing a meaningful EU subsidiary entails substantial restructuring. AWS currently operates through various EU entities for different purposes (sales, customer support, data center operations), but may lack a single subsidiary with comprehensive authority over AWS services to EU financial institutions.

The subsidiary requirement creates potential conflicts of law. An EU subsidiary subject to EU oversight but owned by a US parent subject to the CLOUD Act faces impossible compliance demands: EU authorities may require restricting US government access to EU customer data, while US law may compel the parent to provide such access regardless of where data is stored. DORA does not explicitly address such conflicts, beyond Article

36(1)'s provision that third-country inspections require the provider's consent and the third country's non-objection.⁵³

4.2.2 Indirect Mechanism: The Contractual Cascade

Article 30's mandatory contractual provisions create DORA's primary indirect extraterritorial mechanism. By requiring EU financial entities to impose specific contractual terms on all ICT third-party service providers regardless of the provider's domicile, DORA transmits regulatory requirements through private contract rather than direct public law assertion.

The contractual cascade operates as follows: DORA requires EU financial entities to include Article 30's specified provisions in contracts with ICT providers (Article 30(2)).⁵⁴ Article 30's most significant contractual requirements for purposes of extraterritoriality include: full access and audit rights for financial entities, competent authorities, and their representatives (Article 30(3)(e)); termination rights enabling the financial entity to exit the arrangement (Article 30(2)(h)); exit strategies ensuring business continuity during transitions (Article 30(3)(f)); and obligations regarding incident notification and cooperation with supervisory authorities.

DORA shifts the contractual balance in ICT service procurement. Prior to DORA, cloud providers typically imposed standardised contracts with limited negotiability. DORA effectively requires providers to accept less favourable terms than they might otherwise impose, with EU financial entities obliged to secure specific protections as a matter of regulatory compliance.

Article 30(3)(e) exemplifies extraterritorial transmission: contracts must enable EU supervisors to inspect facilities and systems potentially located in the US or other third countries. For a US cloud provider, this means accepting that EU supervisory authorities may, upon proper authorisation, access and audit its premises and data. The contractual cascade extends beyond first-tier providers to subcontractors under Article 30(2)(a), which requires contracts to specify whether subcontracting of ICT services supporting critical or important functions is permitted and, where it is, the conditions applying to such subcontracting — supplemented by the ESAs' technical standards on subcontracting, which carry equivalent protections down the service delivery chain.⁵⁵

4.2.3 Market Access Conditioning and Competitive Dynamics

DORA conditions EU market access on compliance with operational resilience requirements, creating competitive pressures that extend beyond legal mandates. EU financial entities seeking to demonstrate regulatory compliance will prefer providers that proactively align with DORA requirements over providers that resist or minimally comply.

This dynamic operates through procurement decisions. An EU bank selecting a cloud provider for critical workloads must ensure DORA-compliant contractual terms. Providers unwilling to accept these terms risk

⁵³ DORA (n 1) art 36(1).

⁵⁴ DORA (n 1) art 30(2).

⁵⁵ DORA (n 1) art 30(2)(a).

exclusion from EU financial institution procurement, creating powerful commercial pressure toward contractual convergence.

The competitive dynamic also operates among providers. Conversely, if all major providers resist particular DORA provisions, arguing they are technically infeasible or commercially unreasonable, EU financial institutions may struggle to source compliant services.

4.2.4 Global Standard-Setting Through First-Mover Advantage

DORA's January 2025 application date gives it first-mover advantage in comprehensive operational resilience regulation for ICT providers. Other jurisdictions developing similar frameworks may reference DORA as a model, creating path dependency toward EU standards.

The UK's Financial Services and Markets Act 2023 empowers HM Treasury and financial regulators to designate critical third parties to the financial sector; the Bank of England, Prudential Regulation Authority, and Financial Conduct Authority finalised the accompanying oversight regime in November 2024, with the rules taking effect on 1 January 2025⁵⁶ and explicitly designed for interoperability with DORA. Other jurisdictions—Singapore's Monetary Authority, the Australian Prudential Regulation Authority, Hong Kong's financial regulators—are observing DORA's implementation and may adopt similar third-party oversight mechanisms.

International standard-setting bodies provide additional convergence mechanisms. The Financial Stability Board published a third-party risk management toolkit in December 2023⁵⁷, and the Basel Committee on Banking Supervision finalised its own Principles for the Sound Management of Third-Party Risk in the Banking Sector in December 2025, building on a July 2024 consultation and explicitly referencing the Financial Stability Board's toolkit as a complementary framework⁵⁸.

4.3 Practical Impact on US Third-Party Providers

DORA's extraterritorial mechanisms translate into concrete compliance burdens and strategic decisions for US ICT service providers. This section examines anticipated impacts on major providers and their likely responses.

4.3.1 Amazon Web Services, Microsoft Azure, and Google Cloud Platform

The three dominant cloud computing platforms—Amazon Web Services, Microsoft Azure, and Google Cloud Platform—collectively serve the majority of financial institutions' cloud workloads globally and hold even higher market shares among large, complex institutions.

⁵⁶ Bank of England, Prudential Regulation Authority and Financial Conduct Authority, 'PS16/24 – Operational Resilience: Critical Third Parties to the UK Financial Sector' (12 November 2024); Financial Conduct Authority, 'New Rules to Strengthen Resilience of UK's Financial Sector' (12 November 2024).

⁵⁷ Financial Stability Board, 'Enhancing Third-Party Risk Management and Oversight – A Toolkit for Financial Institutions and Financial Authorities' (4 December 2023) <<https://www.fsb.org/wp-content/uploads/P041223-1.pdf>> accessed 30 June 2026.

⁵⁸ Basel Committee on Banking Supervision, 'Principles for the Sound Management of Third-Party Risk in the Banking Sector' (10 December 2025) <<https://www.bis.org/bcbs/publ/d605.pdf>> accessed 30 June 2026.

AWS holds approximately 32% global cloud market share as of 2024⁵⁹ and serves numerous EU financial institutions. Its EU regional infrastructure (Frankfurt, Ireland, Paris, Stockholm, Milan) demonstrates market commitment, but its US-centralised organisational structure would require substantial adaptation to comply with Article 31(12)'s subsidiary requirement.

Microsoft Azure, with approximately 23% global market share, faces similar considerations. Azure already maintains substantial EU presence through Microsoft's longstanding European operations, potentially easing subsidiary establishment compared to AWS. Microsoft has been more vocal than AWS in supporting regulatory frameworks for cloud security and operational resilience.

Google Cloud Platform, with approximately 11% global market share, occupies a smaller but growing position in financial services. Google Cloud has invested heavily in financial services-specific capabilities, including specialised compliance offerings and partnerships with financial technology companies.

For all three providers, critical designation appears likely if the ESAs apply Article 31's criteria rigorously. Each provider serves numerous systemically important EU financial institutions, supports critical functions (payment processing, trading systems, risk management), and lacks readily available substitutes offering equivalent capabilities at comparable scale.

4.3.2 Other Potential Critical Third-Party Providers

Beyond the Big Three cloud providers, several other US technology companies may face critical designation based on their provision of services to EU financial institutions. IBM, while less dominant in public cloud infrastructure than AWS, Azure, or Google Cloud, maintains substantial financial services technology operations. IBM's core banking systems, mainframe infrastructure, and enterprise software serve major EU banks, particularly legacy institutions with long-standing IBM technology dependencies.

Oracle provides database management systems, enterprise resource planning software, and cloud infrastructure services to financial institutions globally. Salesforce, the dominant customer relationship management (CRM) platform provider, serves financial institutions for client management, sales automation, and customer service.

Bloomberg LP provides market data, analytics, and trading platforms essential to capital markets operations. Bloomberg terminals and enterprise platforms support trading, risk management, and investment decision-making across EU financial institutions.

SWIFT (Society for Worldwide Interbank Financial Telecommunication), while technically a cooperative society rather than a US company, provides critical payment messaging infrastructure. SWIFT's unique position in international payment systems makes it difficult to classify under DORA's framework, but its criticality is undeniable.

⁵⁹ Synergy Research Group, 'Cloud Market Share Q4 2024 and Full Year 2024' (Synergy Research Group, February 2025), reporting Amazon Web Services holding approximately 30-32% of the global cloud infrastructure market through 2024.

4.3.3 Compliance Costs and Strategic Responses

US providers designated as critical will incur substantial compliance costs. Ongoing oversight compliance generates additional costs. Responding to Lead Overseer information requests requires dedicating legal, compliance, and technical staff to gather, review, and provide requested materials.

Contractual amendments to comply with Article 30 also impose costs. Strategic responses to DORA vary by provider, but four broad approaches can be identified. A first approach favours direct operational compliance: providers absorb the necessary costs, adapt existing infrastructure and contractual templates to meet DORA's requirements, and treat compliance as a routine cost of doing business in the EU market, without actively seeking to influence the framework's substance or scope.

A second approach seeks to influence DORA implementation to minimise burdens: engage with the ESAs during designation processes, advocate for proportionate oversight, request clarification of ambiguous requirements, and participate in industry working groups developing best practices. A third approach escalates to political channels: lobby the US government to raise DORA concerns with EU authorities, seek US legislative protections against conflicting requirements, or advocate for bilateral US-EU agreements clarifying jurisdictional boundaries. A fourth approach, global standardisation, treats DORA compliance as an opportunity to demonstrate superior operational resilience globally.

4.4 Limitations and Countervailing Forces

While DORA possesses substantial mechanisms for extraterritorial influence, several factors limit its global regulatory impact and may perpetuate US-EU divergence.

4.4.1 US Market Size as Counterweight

The United States financial services market exceeds the EU's in most dimensions. For cloud providers and other ICT service providers, US financial services revenue exceeds EU revenue.

This market size differential creates countervailing pressure to DORA's Brussels Effect. If US regulators or industry groups resist DORA-compliant practices, arguing they impose unnecessary costs or conflicts with US requirements, providers face competing pressures: EU regulators demanding DORA compliance versus US stakeholders resisting it.

The Brussels Effect counterweight operates if US regulators explicitly adopt divergent standards or if geopolitical tensions escalate into regulatory fragmentation. Neither appears imminent, but the risk of politically-driven US-EU regulatory divergence in technology governance has increased since 2022.

4.4.2 US Regulatory Resistance and Jurisdictional Competition

US financial regulators may resist DORA-driven convergence to preserve regulatory autonomy and assert US supervisory authority. The Federal Reserve, OCC, and other agencies jealously guard their jurisdictional authority and may view DORA's extraterritorial reach as encroachment on US regulatory sovereignty.

This resistance could manifest through several mechanisms. First, US regulators might promulgate guidance or regulations that deliberately diverge from DORA to signal regulatory independence.

Historical precedents exist for such resistance.

US regulatory culture's emphasis on principles-based supervision, institution responsibility, and market-driven solutions conflicts with DORA's prescriptive, comprehensive, regulatory approach. This philosophical divergence may generate persistent resistance to DORA-style operational resilience regulation even if acknowledging operational resilience's importance.

4.4.3 Geopolitical Factors and Strategic Technology Competition

US-EU relations, while generally cooperative among allies, involve strategic competition in technology governance, digital regulation, and economic policy. DORA implementation occurs against this backdrop of competition, potentially constraining cooperative convergence.

The United States views technology leadership as essential to national security and economic competitiveness. Data sovereignty constitutes a particular flashpoint.

China's emergence as a third regulatory pole further complicates convergence dynamics. Chinese technology regulations, data localisation requirements, and cybersecurity rules create a separate regulatory regime.

4.4.4 Technical and Economic Limits to Non-Divisibility

While non-divisibility creates pressure for global standardisation, technical and economic realities permit more geographic segmentation than initial Brussels Effect analysis might suggest. Cloud providers have invested heavily in regional infrastructure, data residency capabilities, and geographic isolation precisely to address data sovereignty and regulatory requirements. AWS, Azure, and Google Cloud all offer region-specific services enabling financial institutions to specify where data resides and where computing occurs.

The economics of divisibility depend on the specific requirements. Data localisation and regional infrastructure impose manageable costs, as providers already maintain regional data centers. However, certain DORA requirements resist divisibility.

4.4.5 'Brussels Effect in Retreat'? Recent Scholarly Skepticism

Recent scholarship has questioned whether the Brussels Effect remains as potent as Bradford's original formulation suggested. While these critiques do not definitively discount DORA's extraterritorial efficacy, they suggest a more measured approach when forecasting global regulatory convergence.

Critics point to growing regulatory nationalism, with major jurisdictions explicitly designing frameworks that diverge from EU standards. Brazil's data protection law (LGPD), while initially characterised as GDPR-inspired, includes significant departures reflecting Brazilian priorities.

The EU's declining share of global GDP—from approximately 30% in 2000 to approximately 17% in 2024—reduces its market power. While the EU remains a large market, its relative importance has diminished as Asian economies, particularly China and India, have grown. This demographic and economic shift may reduce the EU's capacity to set global standards through market size alone.

Technology industry pushback has intensified. In earlier Brussels Effect cases (data protection, chemicals regulation), regulated industries often accepted EU requirements as reasonable.

The precedent of Brexit demonstrates that even deeply integrated Member States may prioritise domestic regulatory autonomy over supranational harmonisation when structural political conditions align. The United Kingdom's departure from the EU included express commitments to regulatory divergence in areas where the UK perceives competitive advantage.

These considerations suggest that DORA's Brussels Effect, while real, faces greater obstacles than earlier EU regulatory globalisations. The thesis must assess both mechanisms supporting convergence and forces perpetuating divergence to reach balanced conclusions.

CHAPTER 5: EVIDENCE OF CONVERGENCE AND DIVERGENCE

5.1 Evidence of Convergence Pressures

Multiple mechanisms generate pressure toward transatlantic convergence in operational resilience standards, ranging from market-driven provider responses to international regulatory coordination.

5.1.1 Market-Driven Convergence Through Provider Adaptation

In response to DORA, leading US cloud infrastructure providers have begun recalibrating their service-level agreements and technical protocols; significantly, early data indicates that these upgraded capabilities are being deployed uniformly across global networks rather than via regionalised EU frameworks. Amazon Web Services published guidance in late 2024 addressing DORA compliance for financial services customers, emphasising AWS's existing capabilities in areas such as incident response, resilience testing, and audit support.⁶⁰

AWS's guidance documents indicate willingness to negotiate enhanced contractual provisions with EU financial institutions, including provisions addressing Article 30's requirements for access rights, exit strategies, and incident notification. Significantly, AWS has indicated that certain operational improvements implemented to support DORA compliance—such as enhanced incident detection and notification systems—will be deployed globally rather than maintained as EU-specific capabilities.⁶¹

Microsoft Azure has similarly published DORA compliance frameworks emphasising Azure's alignment with DORA requirements. Microsoft's documentation highlights existing certifications and audit capabilities that address DORA expectations, while acknowledging areas requiring contractual enhancements or operational adjustments.⁶² Microsoft's approach emphasises that cloud providers' global operational resilience capabilities, developed to meet various regulatory frameworks worldwide, already substantially align with DORA principles.

Google Cloud Platform has engaged with financial services clients and regulators on DORA implementation, though with less public documentation than AWS or Microsoft. Industry reports suggest Google Cloud is adapting standard financial services contracts to incorporate DORA-compliant provisions, with particular attention to data residency, access controls, and audit rights.⁶³

These provider responses demonstrate market-driven convergence consistent with Brussels Effect predictions. Rather than refusing EU financial services business or maintaining entirely separate EU and non-EU operational regimes, major providers are adapting to DORA requirements while extending certain enhancements globally.

⁶⁰ Amazon Web Services, 'Navigating DORA: AWS Guidance for Financial Services Customers' (AWS Financial Services Blog, November 2024) <<https://aws.amazon.com/blogs/financial-services>> accessed 16 February 2026.

⁶¹ *ibid.*

⁶² Microsoft Azure, 'Azure Compliance and DORA' (Microsoft Trust Center, December 2024) <<https://azure.microsoft.com/compliance/dora>> accessed 16 February 2026.

⁶³ Google Cloud, 'Improve Financial Resilience with Google Cloud' (Google Cloud Blog, 2026) <<https://cloud.google.com/blog/topics/financial-services/improve-financial-resilience-with-google-cloud>> accessed 30 June 2026.

5.1.2 International Regulatory Dialogue and Coordination

International standard-setting bodies have intensified attention to operational resilience, creating forums where EU and US regulatory approaches may converge through coordinated guidance. The Financial Stability Board's work on third-party dependencies in cloud services, initiated before DORA's adoption but continuing during its implementation, provides a multilateral framework addressing similar concerns.⁶⁴

The Basel Committee on Banking Supervision's Principles for Operational Resilience, published in March 2021, establish international standards that both DORA and US guidance reference. While the Basel principles remain non-binding and principles-based rather than prescriptive, they create common vocabulary and shared objectives across jurisdictions.⁶⁵ To the extent that US and EU regulators both implement Basel principles, convergence occurs indirectly through common adherence to international standards.

Bilateral US-EU regulatory dialogues, including the Financial Markets Regulatory Dialogue established by the US Treasury and European Commission, provide forums for discussing operational resilience frameworks. These dialogues have addressed DORA's implications for US financial institutions and technology providers, with both sides seeking to minimise regulatory conflicts and identify areas for coordination.⁶⁶ However, regulatory dialogue evidence also reveals limits to convergence.

5.1.3 Industry-Led Operational Resilience Initiatives

Financial services industry initiatives demonstrate voluntary convergence toward enhanced operational resilience standards. Sheltered Harbor, a US banking industry initiative established in 2015, provides data vaulting and rapid recovery capabilities enabling banks to restore critical systems and customer data following catastrophic failures.⁶⁷ While predating DORA, Sheltered Harbor reflects similar operational resilience objectives and has expanded participation following DORA's adoption, suggesting that regulatory attention to resilience amplifies industry self-regulatory efforts.

The Financial Services Information Sharing and Analysis Center (FS-ISAC) has developed DORA implementation guidance for its global membership, including US financial institutions. This guidance facilitates convergence by helping US institutions understand DORA requirements and adopt compatible practices even where not legally required to do so.⁶⁸

Industry associations have advocated for greater regulatory harmonisation in operational resilience frameworks. The Institute of International Finance, representing global financial institutions, has called for internationally coordinated approaches to third-party risk management and operational resilience, arguing that fragmented

⁶⁴FSB (n 10); FSB, 'Regulation and Supervision of Cloud Service Providers' (July 2023).

⁶⁵ Basel Committee on Banking Supervision (n 14).

⁶⁶ US Department of the Treasury and European Commission, 'US-EU Financial Markets Regulatory Dialogue: Joint Statement' (16 March 2024).

⁶⁷ Sheltered Harbor, 'About Sheltered Harbor' <<https://www.shelteredharbor.org>> accessed 16 February 2026.

⁶⁸ FS-ISAC (n 45).

requirements impose unnecessary compliance costs without corresponding risk management benefits.⁶⁹ Such advocacy creates pressure on US regulators to consider alignment with international approaches including DORA.

5.2 Evidence of Persistent Divergence

Despite convergence pressures, substantial evidence indicates persistent and potentially deepening divergence between US and EU operational resilience frameworks.

5.2.1 Structural and Institutional Obstacles to US Convergence

The US regulatory system's fragmentation continues to impede comprehensive operational resilience reform. The absence of legislative action reflects both political gridlock and industry resistance to prescriptive federal requirements. Technology firms have actively opposed the extension of financial regulatory authority over cloud infrastructure, arguing that such expansion creates overlapping jurisdictions and duplicates the established enforcement mandates of the Federal Trade Commission and parallel administrative bodies.⁷⁰

US banking regulators, while acknowledging operational resilience's importance, have not moved toward DORA-style prescriptive rulemaking. The agencies' 2023 third-party risk management guidance maintains the principles-based approach of prior guidance, providing expectations rather than mandatory requirements.

The agencies' reluctance to pursue prescriptive rulemaking partly reflects legal constraints. The Administrative Procedure Act's notice-and-comment requirements make rulemaking time-consuming and subject to litigation challenges. Guidance, while lacking binding legal force, can be issued more quickly and updated more easily.⁷¹

However, this legal-procedural explanation does not fully account for regulatory choices; agencies could pursue formal rulemaking if political and policy commitments supported it. The continuation of guidance-based approaches suggests deeper institutional preferences for flexibility over harmonisation.

5.2.2 Philosophical and Political Divergence

Fundamental philosophical differences between US and EU regulatory cultures continue to divide approaches to operational resilience. The US regulatory tradition emphasises principles-based supervision, risk-based tailoring, and market-driven solutions. This philosophical commitment to principles-based regulation persists across political administrations.

Recent US regulatory trends under the Biden administration (2021-2025) have emphasised prudential strengthening, including proposed Basel III endgame capital requirements, but operational resilience has not received comparable prescriptive attention. The focus remains on ensuring institutions have adequate programs

⁶⁹ Institute of International Finance, 'Operational Resilience: A Framework for Global Financial Institutions' (IIF Special Report, June 2024) 15-18.

⁷⁰ US Department of the Treasury, 'The Financial Services Sector's Adoption of Cloud Services' (February 2023); American Bankers Association, 'Cloud Outsourcing Issues and Considerations' (July 2024).

⁷¹ Administrative Procedure Act (n 38).

rather than mandating specific program elements.⁷² Anti-regulatory sentiment in certain political constituencies further constrains reform.

5.2.3 Persistent Absence of Direct Third-Party Oversight Authority

Most significantly, no movement toward establishing US regulatory authority for direct oversight of critical technology providers has emerged. DORA's most innovative feature—direct ESA oversight of critical ICT third-party providers—has no US parallel and shows no signs of development.

US financial regulators lack statutory authority to examine cloud providers directly, and no legislative proposals to grant such authority have gained traction. The Bank Service Company Act provides limited authority over certain service providers to banks, but cloud platforms typically structure relationships to fall outside this statute's scope. US technology policy debates focus on antitrust enforcement, content moderation, and data privacy rather than operational resilience for financial services.

The absence of direct third-party oversight authority represents the most fundamental divergence between US and EU frameworks. DORA's ability to designate Amazon Web Services or Microsoft Azure as critical providers, require EU subsidiaries, conduct inspections, and impose penalties has no US equivalent and no plausible path to adoption absent major legislative reform.

5.3 Case Study: Amazon Web Services' Response to DORA

Amazon Web Services' response to DORA offers a particularly instructive case study because the company combines two characteristics that, under Bradford's framework, predict an especially strong Brussels Effect: a dominant share of the global cloud infrastructure market and a business model in which the underlying technical architecture is genuinely difficult to fragment along jurisdictional lines. As the largest cloud provider serving financial services globally, AWS was always among the most likely candidates for designation as a critical ICT third-party service provider under Article 31, and on 18 November 2025 the European Supervisory Authorities confirmed exactly this outcome, naming AWS, Microsoft, and Google Cloud among the first cohort of nineteen designated critical ICT third-party providers under DORA.⁷³

This confirmed designation subjects AWS to direct oversight by a Lead Overseer drawn from the ESAs, including the power to conduct inspections, issue recommendations, and ultimately require remedial action where governance or risk management frameworks are found inadequate. AWS has addressed DORA publicly through several channels, including a dedicated guidance document for financial services customers and broader public materials on financial resilience, which together set out how the company's existing security, compliance, and

⁷² Federal Reserve Board, 'Federal Reserve Board invites public comment on broad set of proposed changes to improve the strength and resilience of large banks' (Press Release, 27 July 2023).

⁷³ European Supervisory Authorities, 'ESAs Designate First Critical ICT Third-Party Providers under DORA' (18 November 2025); Morgan Lewis, 'DORA: EU Regulators Announce List of Critical ICT Third-Party Providers' (Tech & Sourcing Blog, 18 November 2025) <<https://www.morganlewis.com/blogs/sourcingatmorganlewis/2025/11/dora-eu-regulators-announce-list-of-critical-ict-third-party-providers>> accessed 30 June 2026.

contractual frameworks map onto DORA's five pillars and identify the areas in which both AWS and its customers must adapt.⁷⁴

Several specific areas of adaptation stand out. Contractual provisions must be enhanced to address Article 30's detailed requirements, particularly regarding access rights for EU financial institutions and their supervisors, exit strategies that facilitate transitions to alternative providers without unacceptable disruption, and incident notification obligations that align with DORA's harmonised reporting timelines.⁷⁵ These are not minor adjustments: they require AWS to renegotiate elements of its standard contractual architecture that has historically been offered on a largely take-it-or-leave-it basis to customers worldwide, illustrating concretely how DORA's contractual cascade mechanism translates regulatory requirements into commercial leverage that EU financial institutions can exercise against even the largest global providers.

Confirmed designation also resolves what had previously been the central uncertainty surrounding AWS's compliance posture: whether its existing European corporate and operational presence, spanning data centre infrastructure in Frankfurt, Ireland, Paris, Stockholm, and Milan, would satisfy Article 31(12)'s requirement that critical providers establish an adequately capitalised EU subsidiary with genuine authority over service provision to EU clients. Designated providers must now establish or confirm such a subsidiary within twelve months, and the ESAs' oversight framework formally assumes that the subsidiary exercises meaningful authority over the parent's EU-facing operations rather than functioning as a nominal entity. How AWS structures this relationship in practice, and whether it requires substantive organisational restructuring beyond its existing European footprint, will become clearer as the Lead Overseer's engagement with AWS develops over the coming oversight cycle.

More striking, from the perspective of this thesis's central convergence question, is AWS's indication that certain operational improvements implemented to support DORA compliance will apply globally rather than being confined to EU operations. This is precisely the dynamic that Bradford's non-divisibility condition predicts: where the underlying infrastructure, governance processes, and incident response capabilities are shared across a global platform, it is frequently cheaper and operationally simpler for a provider to raise its baseline practices worldwide than to maintain a permanently bifurcated EU-compliant and non-EU-compliant set of systems. AWS's public messaging around DORA compliance has consistently emphasised this global uplift in security and resilience practices, framing DORA-driven changes as enhancements to the platform as a whole rather than as EU-specific carve-outs.

Even so, AWS has been equally clear about the limits of this convergence. Contractual provisions, the company has indicated, will continue to vary by jurisdiction based on local legal requirements and regulatory expectations, meaning that the specific terms offered to EU financial institutions under Article 30 will not necessarily be extended verbatim to customers in other markets. This bifurcation between operational and contractual convergence tracks closely with the three-tier convergence pattern identified in Chapter 6: AWS's case suggests

⁷⁴ AWS (n 60).

⁷⁵ *ibid.*

that operational capabilities migrate toward DORA-aligned global standards relatively readily, that contractual practices converge only partially and selectively, and that the underlying legal framework governing AWS's relationship with US regulators remains entirely untouched by DORA's requirements, notwithstanding its new status as a directly supervised EU critical provider. The AWS case study thus serves as an empirical microcosm of this thesis's central thesis: DORA catalyzes tangible yet structurally bounded convergence. This trend toward harmonisation accelerates where technical and market rationales encourage global uniformity. Conversely, it encounters an institutional impasse when compliance requires foreign entities to accept the extraterritorial extension of EU law over corporate structures or liability frameworks anchored in US jurisprudence.

CHAPTER 6: ANALYSIS AND IMPLICATIONS

6.1 Degree of Convergence: Assessment

The evidence supports a conclusion of limited, selective convergence rather than comprehensive harmonisation. Convergence manifests primarily as de facto market-driven standardisation of operational capabilities, while de jure legal divergence persists and may deepen.

6.1.1 High Convergence: Operational Capabilities and Best Practices

Certain dimensions exhibit high convergence. Operational resilience capabilities—incident detection and response systems, business continuity planning, resilience testing methodologies, and third-party risk assessment frameworks—demonstrate substantial alignment between leading US and EU financial institutions and their technology providers. Cloud providers' incident response capabilities, security monitoring, and infrastructure resilience practices increasingly converge toward global standards that meet or exceed DORA requirements.

6.1.2 Moderate Convergence: Contractual Practices

Contractual practices for ICT services demonstrate moderate convergence. US financial institutions are increasingly negotiating enhanced contractual provisions with cloud providers and other technology vendors, including provisions resembling DORA Article 30 requirements regarding access rights, audit capabilities, exit strategies, and incident notification. However, contractual convergence remains incomplete and variable.

6.1.3 Low Convergence: Legal Frameworks and Direct Oversight

Legal frameworks exhibit low convergence, with fundamental structural differences persisting. The EU's comprehensive, prescriptive, harmonised Regulation contrasts with the US's fragmented, principles-based guidance. Most critically, DORA's direct oversight of critical ICT third-party providers has no US equivalent and no plausible path to adoption. This legal divergence matters because it affects enforceability, consistency, and supervisory authority.

6.2 Explanatory Factors: Why Convergence and Divergence Coexist

The coexistence of convergence in operational practices and divergence in legal frameworks reflects the interaction of market forces, institutional structures, and political constraints. Understanding why these two dynamics operate simultaneously, rather than one simply displacing the other, requires separating the distinct causal logics that drive each. The following subsections examine convergence and divergence in turn: Section 6.2.1 explains why market-driven pressures generate convergence in operational capabilities despite the absence of formal legal harmonisation, while Section 6.2.2 explains why institutional path dependency and domestic political constraints sustain divergence at the level of binding legal frameworks.

6.2.1 Why Convergence Occurs: Market Forces and Technical Non-Divisibility

Convergence in operational capabilities reflects market-driven dynamics. International standards provide coordination mechanisms enabling convergence. The Basel Committee and Financial Stability Board establish common principles that both EU and US regulators reference, creating baseline alignment even absent formal harmonisation.

DORA's Brussels Effect operates through these market mechanisms. By establishing stringent EU requirements, DORA raises the global baseline as providers extend DORA-compliant capabilities worldwide rather than restricting them to EU operations. This market-driven convergence occurs without US formal adoption of DORA's legal framework.⁷⁶

6.2.2 Why Divergence Persists: Institutional Path Dependency and Political Constraints

Legal divergence persists due to institutional path dependency and political constraints. Regulatory philosophy differences reflect deeper cultural and political commitments. US preference for principles-based supervision, market-driven solutions, and institutional responsibility represents more than pragmatic choice; it embodies political ideology about appropriate government roles in markets. European preference for prescriptive harmonisation similarly reflects political commitments to centralised standard-setting and comprehensive regulatory frameworks.⁷⁷

Political economy factors reinforce divergence. Industry lobbying from both financial institutions and technology companies resists prescriptive US regulation.

6.3 Implications for Financial Institutions and Technology Providers

The coexistence of convergence and divergence creates complex compliance landscapes for financial institutions and technology providers operating transatlantically. For global financial institutions, dual compliance burdens

⁷⁶Bradford (n 15) ch 3.

⁷⁷ Kathryn C Lavelle, 'The Foundations of Regulatory Convergence and Divergence Between the Federal Reserve and European Central Bank' (2014) 45 *Georgetown Journal of International Law* 1165, 1185-1190.

arise. EU operations must comply with DORA's prescriptive requirements, while US operations follow principles-based guidance.

For US-domiciled financial institutions without significant EU presence, DORA creates indirect exposure. For ICT third-party service providers, DORA creates strategic choices between compliance and market exit, between global standardisation and geographic differentiation.

CHAPTER 7: CONCLUSION

7.1 Summary of Findings

This thesis examined whether the EU's Digital Operational Resilience Act will drive regulatory convergence in US financial operational resilience frameworks or reinforce transatlantic divergence. The analysis yields a nuanced answer: DORA will generate limited, market-driven de facto convergence in operational practices, while de jure legal divergence persists and may deepen.

DORA establishes the EU's most comprehensive operational resilience framework for financial services, creating uniform requirements across 27 Member States and 21 categories of financial entities. In contrast, the United States maintains a fragmented operational resilience framework characterised by principles-based supervisory guidance from multiple federal agencies, limited formal rules addressing specific issues, and absence of direct regulatory oversight of technology providers.

Applying the Brussels Effect theoretical framework reveals that DORA satisfies several but not all conditions for unilateral regulatory globalisation. The EU market is sufficiently large, regulatory capacity exists through the ESAs, DORA is more stringent than US frameworks, and targets are substantially inelastic.

Evidence of convergence includes cloud providers' global deployment of enhanced operational resilience capabilities, contractual terms increasingly reflecting DORA-like provisions even in US agreements, and industry initiatives promoting similar operational resilience practices. The thesis concludes that DORA generates a selective Brussels Effect: market-driven convergence in operational practices coexists with persistent legal and institutional divergence.

7.2 Theoretical Contributions

This thesis contributes to Brussels Effect scholarship by demonstrating that the framework's five conditions operate with varying intensity across different regulatory dimensions. Non-divisibility, conventionally treated as a binary condition, proves more nuanced: some regulatory requirements (operational capabilities) exhibit strong non-divisibility favoring global standardisation, while others (contractual provisions, legal compliance) permit economically viable geographic differentiation.⁷⁸ The analysis also illuminates Brussels Effect limitations in financial regulation.

For regulatory convergence theory, the thesis demonstrates that convergence can occur through market mechanisms even absent formal legal harmonisation. De facto convergence through provider voluntary action differs fundamentally from de jure convergence through legal adoption, with important implications for assessing regulatory power and international influence.

⁷⁸This finding builds on Bradford (n 15) while identifying dimensionality within the non-divisibility condition that Bradford treats more uniformly.

7.3 Policy Recommendations

For US regulators, enhanced interagency coordination, harmonised incident reporting standards, consistent third-party risk expectations, and reduced fragmentation could improve the framework without requiring legislation. EU regulators should recognise the Brussels Effect's limits. Comprehensive US legal convergence is unrealistic; cooperative mechanisms — mutual recognition arrangements, coordinated oversight of global providers, and bilateral agreements addressing jurisdictional conflicts — are more likely to achieve resilience objectives than unilateral requirements alone.

For financial institutions, the analysis emphasises the need for flexible compliance infrastructure capable of accommodating multiple regulatory frameworks. Rather than viewing US and EU requirements as contradictory, institutions should identify areas of alignment and build compliance programs that efficiently address both frameworks. For international standard-setters, particularly the Financial Stability Board and Basel Committee, the analysis underscores opportunities to facilitate convergence through high-quality international standards.

7.4 Future Research Directions

This thesis necessarily relies on early evidence and preliminary responses to DORA, as the Regulation only became applicable in January 2025. Comparative analysis extending beyond the US-EU dyad would enrich understanding of DORA's global influence.

Detailed case studies of specific providers' responses—combining public information with confidential interviews if possible—would provide granular insight into strategic decisions, compliance costs, and operational adaptations. Such case studies could test this thesis's predictions about selective convergence and non-divisibility.

Analysis of enforcement actions and case law as they develop will be essential. How EU supervisors actually exercise oversight of critical providers, whether they impose penalties for non-compliance, and how courts resolve any resulting disputes will shape DORA's practical impact beyond its formal legal provisions.

Finally, research examining DORA's impact on financial innovation would address questions beyond this thesis's scope. Whether DORA's requirements facilitate or impede fintech innovation, cloud adoption, and technological advancement in financial services deserves systematic investigation with implications for regulatory design globally.

TABLE OF CASES AND LEGISLATION

Table of Cases

Case C-413/14 P *Intel Corp Inc v Commission* ECLI:EU:C:2017:632

Table of EU Legislation

Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) [2010] OJ L331/12

Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority) [2010] OJ L331/48

Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority) [2010] OJ L331/84

Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector [2022] OJ L333/80

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L333/1 (DORA)

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets [2023] OJ L150/40 (MiCA)

Table of US Legislation

Administrative Procedure Act 1946, 5 USC § 553

Bank Secrecy Act 1970, 31 USC § 5311 et seq

Bank Service Company Act 1962, 12 USC § 1861 et seq

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 12 CFR pt 53

Cybersecurity, Regulation S-K Item 106, 17 CFR § 229.106

Table of UK Legislation

Financial Services and Markets Act 2023

BIBLIOGRAPHY

PRIMARY SOURCES

European Union

Directive (EU) 2022/2556 of the European Parliament and of the Council of 14 December 2022 amending Directives 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 and (EU) 2016/2341 as regards digital operational resilience for the financial sector [2022] OJ L333/80

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector [2022] OJ L333/1

Regulation (EU) 2023/1114 on markets in crypto-assets [2023] OJ L150/40

Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority) [2010] OJ L331/12

Regulation (EU) No 1094/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Insurance and Occupational Pensions Authority) [2010] OJ L331/48

Regulation (EU) No 1095/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Securities and Markets Authority) [2010] OJ L331/84

United States

Administrative Procedure Act 1946, 5 USC § 553

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 12 CFR pt 53

Cybersecurity, Regulation S-K Item 106, 17 CFR § 229.106

Bank Secrecy Act 1970, 31 USC § 5311 et seq

Financial Industry Regulatory Authority, FINRA Rule 3110 (Supervision)

Cases

Case C-413/14 P *Intel Corp Inc v Commission* ECLI:EU:C:2017:632

SECONDARY SOURCES

Books

American Law Institute, Restatement (Third) of the Foreign Relations Law of the United States (American Law Institute 1987)

Bradford A, The Brussels Effect: How the European Union Rules the World (Oxford University Press 2020)

Ryngaert C, Jurisdiction in International Law (2nd edn, Oxford University Press 2015)

Journal Articles

Bradford A, 'The Brussels Effect' (2012) 107 Northwestern University Law Review 1

Chander A and *Lê UP*, 'Data Nationalism' (2015) 64 Emory Law Journal 677

- Jones E and Zeitz AO*, 'Regulatory Convergence in the Financial Periphery: How Interdependence Shapes Regulators' Decisions' (2019) 63 *International Studies Quarterly* 908
- Lavelle KC*, 'The Foundations of Regulatory Convergence and Divergence Between the Federal Reserve and European Central Bank' (2014) 45 *Georgetown Journal of International Law* 1165
- Pierson P*, 'Increasing Returns, Path Dependence, and the Study of Politics' (2000) 94 *American Political Science Review* 251
- Romano R*, 'The Sarbanes-Oxley Act and the Making of Quack Corporate Governance' (2005) 114 *Yale Law Journal* 1521
- Simmons BA*, 'The International Politics of Harmonization: The Case of Capital Market Regulation' (2001) 55 *International Organization* 589

Chapters in Edited Books

- Kim H-J*, 'Toward Transatlantic Convergence in Financial Regulation' in Kern Alexander and Rahul Dhumale (eds), *Research Handbook on International Financial Regulation* (Edward Elgar 2012)

Reports and Policy Documents

- American Bankers Association, 'Cloud Outsourcing Issues and Considerations' (July 2024)
- Bank of England, Prudential Regulation Authority and Financial Conduct Authority, 'PS16/24 – Operational Resilience: Critical Third Parties to the UK Financial Sector' (12 November 2024)
- Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation, 'Interagency Guidance on Third-Party Relationships: Risk Management' (6 June 2023)
- European Banking Authority, 'Report on the Use of Digital Platforms in the EU Banking and Payments Sector' (EBA/REP/2021/26, 21 September 2021)
<https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2021/1019865/EB A%20Digital%20platforms%20report%20-%2020210921.pdf> accessed 30 June 2026
- European Central Bank, 'Financial Integration and Structure in the Euro Area' (June 2024)
- European Commission, 'Proposal for a Regulation on Digital Operational Resilience for the Financial Sector' COM(2020) 595 final
- European Supervisory Authorities, 'ESAs Designate First Critical ICT Third-Party Providers under DORA' (18 November 2025)
- European Supervisory Authorities, 'ESAs publish final package of policy and technical standards under DORA' (17 January 2024)
- Federal Reserve Board, 'Federal Reserve Board invites public comment on broad set of proposed changes to improve the strength and resilience of large banks' (Press Release, 27 July 2023)
- 'Supervision and Regulation Report' (November 2020)
- Financial Conduct Authority, 'New Rules to Strengthen Resilience of UK's Financial Sector' (12 November 2024)
- Financial Services Information Sharing and Analysis Center, 'DORA Implementation Guide for FS-ISAC Members' (FS-ISAC, September 2024)
- Institute of International Finance, 'Operational Resilience: A Framework for Global Financial Institutions' (IIF Special Report, June 2024)

National Association of Insurance Commissioners, 'Insurance Data Security Model Law' (MDL-668, adopted 2017)

National Cyber Security Centre, 'Ransomware: WannaCry Guidance for Enterprise Administrators' (May 2017)

National Institute of Standards and Technology, 'The NIST Cybersecurity Framework (CSF) 2.0' (26 February 2024) <<https://doi.org/10.6028/NIST.CSWP.29>> accessed 30 June 2026

Securities and Exchange Commission, Final Rule, 'Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure' Release No 33-11216 (26 July 2023)

—— Final Rule, 'Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information' Release No 34-98990 (16 May 2024)

Synergy Research Group, 'Cloud Market Share Q4 2024 and Full Year 2024' (February 2025)

US Cybersecurity and Infrastructure Security Agency, 'SolarWinds and Active Directory/M365 Compromise: Detecting Advanced Persistent Threat Activity' (Alert AA20-352A, 17 December 2020)

US Department of the Treasury, 'The Financial Services Sector's Adoption of Cloud Services' (February 2023)

US Department of the Treasury and European Commission, 'US-EU Financial Markets Regulatory Dialogue: Joint Statement' (16 March 2024)

International Standards and Guidance

Basel Committee on Banking Supervision, 'Basel III: A global regulatory framework for more resilient banks and banking systems' (December 2010, revised June 2011)

—— 'Principles for operational resilience' (March 2021)

—— 'Principles for the Sound Management of Third-Party Risk in the Banking Sector' (10 December 2025) <<https://www.bis.org/bcbs/publ/d605.pdf>> accessed 30 June 2026

Financial Stability Board, 'Effective Practices for Cyber Incident Response and Recovery' (19 October 2020)

—— 'Enhancing Third-Party Risk Management and Oversight – A Toolkit for Financial Institutions and Financial Authorities' (4 December 2023) <<https://www.fsb.org/wp-content/uploads/P041223-1.pdf>> accessed 30 June 2026

—— 'Regulation and Supervision of Cloud Service Providers' (July 2023)

—— 'Third-party dependencies in cloud services: Considerations on financial stability implications' (9 December 2019)

Online Sources

Amazon Web Services, 'Navigating DORA: AWS Guidance for Financial Services Customers' (AWS Financial Services Blog, November 2024) <<https://aws.amazon.com/blogs/financial-services>> accessed 16 February 2026

Das KN and Spicer J, 'How Hackers Stole \$81 Million from the Bangladesh Central Bank' *Reuters* (Dhaka/New York, 13 December 2017) <<https://2017.sopawards.com/wp-content/uploads/2017/03/The-Bangladesh-Bank-Heist.pdf>> accessed 30 June 2026

Eaton C and Volz D, 'Colonial Pipeline CEO Tells Why He Paid Hackers a \$4.4 Million Ransom' *The Wall Street Journal* (19 May 2021) <<https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636>> accessed 30 June 2026

Federal Financial Institutions Examination Council, 'IT Examination Handbook' <<https://ithandbook.ffiec.gov>> accessed 30 June 2026

Google Cloud, 'Improve Financial Resilience with Google Cloud' (Google Cloud Blog, 2026) <<https://cloud.google.com/blog/topics/financial-services/improve-financial-resilience-with-google-cloud>> accessed 30 June 2026

Microsoft Azure, 'Azure Compliance and DORA' (Microsoft Trust Center, December 2024) <<https://azure.microsoft.com/compliance/dora>> accessed 16 February 2026

Morgan Lewis, 'DORA: EU Regulators Announce List of Critical ICT Third-Party Providers' (Tech & Sourcing Blog, 18 November 2025) <<https://www.morganlewis.com/blogs/sourcingatmorganlewis/2025/11/dora-eu-regulators-announce-list-of-critical-ict-third-party-providers>> accessed 30 June 2026

Sheltered Harbor, 'About Sheltered Harbor' <<https://www.shelteredharbor.org>> accessed 16 February 2026

'The Brussels Effect in Retreat: How US Economic Might and Political Interference Trump EU Regulation' EuropeanRelations.com (26 September 2025) <<https://europeanrelations.com/the-brussels-effect-in-retreat/>> accessed 16 February 2026