PIFS

Program on International Financial Systems

The E.U.'s Digital Operational Resilience Act: Cloud Services & Financial Companies

Hal S. Scott,
Emeritus Nomura Professor of International Financial Systems,
Harvard Law School

AUGUST 2021

The Program on International Financial Systems (PIFS) is a 501(c)(3) organization that conducts research on issues impacting the global financial system. PIFS also hosts international symposia, executive education programs and special events that foster dialogue and promote education on these issues. PIFS was founded in 1986, by Hal S. Scott, now Professor Emeritus of Harvard Law School. Over thirty years later, Hal Scott continues to lead PIFS.

Amazon Web Services, Inc. is a financial sponsor of PIFS.

The E.U.’s Digital Operational Resilience Act: Cloud Services & Financial Companies

Hal S. Scott,
Emeritus Nomura Professor of International Financial Systems
Harvard Law School

AUGUST 2021

Contents

Executive Summary [1]

In September 2020, the European Commission released a proposed regulation on digital operational resilience for the financial sector ("**DORA**").[2] DORA aims to establish a detailed and comprehensive framework on digital operational resilience for financial entities in the European Union ("**EU**"). DORA includes provisions governing the management of risks associated with financial institutions' outsourcing of technology functions to technology providers and mandating direct regulatory oversight of critical technology providers. Those provisions, and their application to cloud service providers, are the focus of this report.

Our report begins by providing an overview of the costs and benefits of cloud technology for financial companies; we find that cloud technology can offer significant benefits to financial companies. We then describe the current regulatory frameworks that apply to financial institutions' use of third-party technology providers, including cloud service providers, in various jurisdictions. Next, we describe key provisions of DORA that apply to cloud and other technology service providers and how such provisions are similar to or diverge from the current frameworks described in the previous section. We conclude by recommending that the EU revise DORA in certain key respects to better align with the approach in other jurisdictions as DORA's divergences from other jurisdictions' regulation of cloud and other third-party technology services may unnecessarily discourage the adoption of such services by financial companies.

Part I of the report provides background on technology outsourcing in the financial sector and current regulatory and supervisory frameworks. It provides a brief overview of financial institutions' use of technology outsourcing and its risks and benefits, focusing on cloud computing. It then describes current supervisory frameworks governing outsourcing in the financial sector, with a focus on outsourcing guidelines issued by EU financial regulators.

Part II describes provisions in DORA governing the management of third-party risk by financial institutions, which include key principles governing sound management of third-party risk and a framework for direct oversight of third-party service providers deemed "critical" by EU supervisory authorities. It identifies similarities between DORA's key principles governing third-party risk management and existing supervisory frameworks for outsourcing. It then describes key elements of DORA's direct oversight framework, which represents a significant departure from current supervisory approaches to technology outsourcing.

---

[1] PIFS would like to thank Javier Arias, William Coen, Andreas Dombret and Kay Swinburne for reviewing and providing comments on this report.

[2] EUROPEAN COMMISSION, Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014, Articles 28-29 (Sept. 29, 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN ["**DORA**"].

Part III of the report then turns to an evaluation of DORA's proposed direct oversight framework, in light of its stated goals as well as its divergence from current outsourcing frameworks. DORA's aims include establishing a proportionate and risk-based framework for digital operational resilience, which takes into account both the likelihood and magnitude of potential risks, as well as the cost of mitigating them; facilitating innovation while promoting digital operational resilience; and promoting cross-border regulatory harmonization and coordination. Part III of the report shows where the DORA's direct oversight framework falls short on those measures and outlines changes that could improve the effectiveness of the proposed oversight framework.

Part I: Technology Outsourcing in the Financial Sector; Regulatory and Supervisory Frameworks

a. Technology Outsourcing in the Financial Sector – Benefits and Risks

Financial institutions in the United States, EU, and other major markets increasingly outsource certain functions to technology service providers ("**TSPs**"). For example, banks, insurers, and asset managers frequently contract with TSPs for data storage and infrastructure, network management, analytics, and software.[3] These tools help financial institutions manage customer relations, monitor regulatory compliance, and execute core business functions like lending and trading.[4]

One growing segment of technology outsourcing involves cloud computing: the use of computing resources over a network (such as the internet) in a manner that scales automatically with demand and allows customers to pay based on their usage.[5] Financial institutions use cloud services to support various functions, such as delivering mobile services to clients and processing payments.[6] Cloud adoption by financial institutions increased threefold from 2016 to 2018,[7] and this trend is expected to continue.[8]

The use of cloud services by financial institutions is associated with both benefits and risks.[9] Cloud computing can help enhance security and operational resilience in the financial sector. Benefitting from economies of scale compared to their individual clients, cloud service providers can make larger investments in digital security and automated

---

[3] FINANCIAL STABILITY BOARD, *Third-party dependencies in cloud services: Considerations on financial stability implications*, 24-26 (Dec. 9, 2019): https://www.fsb.org/wp-content/uploads/P091219-2.pdf.

[4] U.S. DEPT. OF THE TREASURY, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, 48 (July 2018), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation.pdf.

[5] PROGRAM ON INTERNATIONAL FINANCIAL SYSTEMS, *Cloud Computing in the Financial Sector: A Global Perspective*, 1 (July 2019), https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf; Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing*, U.S. DEPT. OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Sept. 2011), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[6] PROGRAM ON INTERNATIONAL FINANCIAL SYSTEMS, *Cloud Computing in the Financial Sector: A Global Perspective*, 3-4 (July 2019), https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf.

[7] Michael Tang, *Cloud banking: More than just a CIO conversation*, DELOITTE (2019): https://www2.deloitte.com/global/en/pages/financial-services/articles/bank-2030-financial-services-cloud.html. *See also* Joseph A. McCahery and F. Alexander De Roode, *Governance of Financial Services Outsourcing: Managing Misconduct and Third-Party Risks*, EUROPEAN CORPORATE GOVERNANCE INSTITUTE (Sept. 2018), https://ecgi.global/sites/default/files/working_papers/documents/finalmccaheryderoode1.pdf; EUROPEAN BANKING FEDERATION, *The use of Cloud Computing by Financial Institutions* (June 4, 2020), https://www.ebf.eu/wp-content/uploads/2020/06/EBF-Cloud-Banking-Forum_The-use-of-cloud-computing-by-financial-institutions.pdf.

[8] Laurence Goasduff, *Modernize IT Infrastructure in a Hybrid World*, GARTNER (March 5, 2019), https://www.gartner.com/smarterwithgartner/modernize-it-infrastructure-in-a-hybrid-world/.

[9] See generally PROGRAM ON INTERNATIONAL FINANCIAL SYSTEMS, *Cloud Computing in the Financial Sector: A Global Perspective*, 6-14 (July 2019), https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf.

systems to detect and remedy issues quickly.[10] Major cloud platforms are built to support stringent security requirements, allowing clients to manage cyber risk using best practices, standards, data encryption and activity logging. The distributed nature of storage and processing in the cloud can also provide financial institutions with greater operational resiliency: cloud providers, for example, can distribute data centers geographically in order to mitigate the impact of disruptions in any single region.[11] The computing resources made available through the cloud can also facilitate the deployment, by both financial institutions and their regulators, of stronger data analytics tools, which can improve compliance monitoring, risk management, and supervisory analysis.[12]

Another potential benefit of cloud computing is lower costs. The use of cloud services can help lower financial institutions' technology infrastructure costs, by obviating the need for firms to make significant capital expenditures in proprietary data centers.[13] This translates to increasing agility when financial institutions develop new products and services; the cloud's scalability allows financial institutions to test new scenarios, software tools and alternative configurations without a lengthy purchasing and provisioning process. Widespread use of cloud can also facilitate financial sector competition, by providing smaller firms and start-ups with access to cost-effective technology resources that would otherwise be available only to larger, well-established financial institutions.[14]

The use of cloud services by financial companies may also involve novel risks. Some of these risks arise out of the unique technical features of cloud computing. Cloud computing depends on multi-tenancy: the ability of multiple clients to share the same pool of computing resources. Multi-tenancy can give rise to the risk that other parties may have access to the same computing environment as financial institutions that use the cloud, which could potentially allow unauthorized parties to access financial institutions' data.[15] Cloud service providers protect against this possibility by virtually segregating workloads

---

[10] Novet, Jordan, "Amazon, Microsoft, and Google respond to Intel chip vulnerability," *CNBC* (January 3, 2018): https://www.cnbc.com/2018/01/03/microsoft-google-respond-to-intel-chip-vulnerability.html

[11] "Third-party dependencies in cloud services: Considerations on financial stability implications," *Financial Stability Board* (December 9, 2019): https://www.fsb.org/wp-content/uploads/P091219-2.pdf.

[12] Darrow, Barb, "Pssst, Amazon Cloud Is Not Really New to Banks," *Fortune* (February 25, 2016): https://fortune.com/2016/02/25/yes-banks-do-use-aws/; Davies, Paul, "New Tools Give Better Picture, Literally, of Financial-System Risk," *Wall Street Journal* (April 24, 2017):https://www.wsj.com/articles/new-tools-give-better-picture-literally-of-financial-system-risk-1493086260?mod=article_inline; "Using the Cloud to Improve our Data Science," *FINRA*: http://technology.finra.org/articles/using-cloud-to-improve-our-data-science.html

[13] "Moving Financial Market Infrastructure to the Cloud," *Depository Trust and Clearing Corporation* (May 2017): https://www.dtcc.com/-/media/Files/Downloads/Thought-Leadership/moving-financial-markets-infrastructure-to-the-cloud.pdf

[14] "Chapeau Paper 17," *World Bank Group and IMF Bali Fintech Agenda* (September 19, 2018): http://documents1.worldbank.org/curated/en/390701539097118625/pdf/130563-BR-PUBLIC-on-10-11-18-2-30-AM-BFA-2018-Sep-Bali-Fintech-Agenda-Board-Paper.pdf

[15] Dupré, Lionel and Thomas Haeberlen, "Cloud Computing: Benefits, risks and recommendations for information security," *European Union Agency for Network and Information Security (ENISA)*, 34 (December 2012): https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computingbenefits-risks-and-recommendations-for-information-security.

and data using techniques like firewalls; more advanced cloud providers have addressed multi-tenancy risk by blocking access by unauthorized parties at the chip level.

b. Current Requirements on Financial Sector Technology Outsourcing

In response to the increasing trend of financial institutions outsourcing technology functions to cloud and other TSPs, financial regulators have issued principles-based regulations and guidance addressing outsourcing by financial institutions. This section provides a brief overview of the comprehensive supervisory frameworks governing outsourcing by financial institutions, with a focus on outsourcing guidelines issued by the European Banking Authority ("**EBA**"), European Securities and Markets Authority ("**ESMA**") and the European Insurance and Occupational Pensions Authority ("**EIOPA**") (collectively, the "European Supervisory Authorities" or "**ESAs**").

In 2019, the EBA published revised outsourcing guidelines, which incorporated earlier EBA recommendations on outsourcing to cloud service providers.[16] And in 2020, both ESMA and EIOPA issued cloud-specific outsourcing guidelines.[17] These guidelines, where implemented, superseded existing outsourcing regulations and guidelines issued by national financial regulators.[18] They also overlap with non-financial sector specific cybersecurity legislation, such as the Directive on Security of Network and Information Systems (NIS Directive, which the European Commission recently proposed to revise) and the General Data Protection Regulation (GDPR),[19] that are relevant to technology outsourcing by financial institutions.

---

[16] European Banking Authority, *Final Report on EBA Guidelines on Outsourcing Arrangements*, February 25, 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf. These guidelines generally apply to all financial institutions that are within the scope of the EBA's mandate—credit institutions and investment firms subject to the Directive 2013/36/EU (Capital Requirements Directive), payment institutions and electronic money institutions—as well as their local regulators across the European Economic Area.

[17] European Securities and Markets Authority, *Final Report: Guidelines on outsourcing to cloud service providers*, December 18, 2020, https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf; European Insurance and Occupational Pensions Authority, *Guidelines on outsourcing to cloud service providers*, February 6, 2020, https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf. The ESMA guidelines apply to the institutions that are within the scope of ESMAs authority, including managers and depositaries of alternative investment funds and UCITS, central counterparties, investment firms, and credit rating agencies, as well as their local regulators. The EIOPA guidelines are addressed to local regulators, to provide guidance on how insurers and reinsurers should comply with their legal obligations in connection with outsourcing to cloud service providers.

[18] The EBA has also published related guidelines on information and communication technology (ICT) risk, which include standards that apply to the outsourcing of ICT systems. European Banking Authority, *Final Report on Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP)*, May, 11 , 2017, https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1841624/ef88884a-2f04-48a1-8208-3b8c85b2f69a/Final%20Guidelines%20on%20ICT%20Risk%20Assessment%20under%20SREP%20%28EBA-GL-2017-05%29.pdf?retry=1.

[19] European Parliament and the Council of the European Union, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security*

A common theme of the existing supervisory frameworks for outsourcing is that financial institutions that use TSPs retain primary responsibility for assessing and managing risk in connection with the outsourced services; financial institutions' responsibility and accountability for outsourced services cannot be delegated to TSPs.[20] Another shared principle is that regulatory expectations vary based on the relative importance of outsourced functions: stricter criteria apply where financial institutions outsource material, critical or important functions. Factors that are considered when determining the importance of a function include whether it has a strong impact on a financial institutions' risk profile or internal control framework.[21] Relatedly, supervisory frameworks generally emphasize that financial institutions should assess and monitor outsourcing arrangements, and regulators should review compliance with outsourcing standards, following a risk-based approach—taking into account both the nature of the outsourced function and its potential risks.[22]

1. Outsourcing Prerequisites

Outsourcing frameworks generally impose prerequisites on outsourcing, such as pre-outsourcing risk assessment and due diligence and prior notice to regulators. The EBA guidelines direct financial institutions, before engaging in outsourcing, to undertake a preliminary risk assessment of a TSP and the services to be outsourced.[23] The United States' supervisory framework imposes similar requirements: outsourcing guidelines published by the Federal Financial Institutions Examination Council ("FFIEC"), an interagency body composed of U.S. bank regulators, provide that a banking institution should perform due diligence on a TSP in order to ensure that it meets the institution's needs.[24] In a more recent informational notice on cloud computing, the FFIEC emphasized that security-

---

of Network and Information Systems Across the Union (July 19, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=DE (NIS Directive); European Parliament and the Council of the European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* (May 4, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=DE (GDPR). The European Commission recently published its proposal for a revised NIS Directive (the NIS 2 Directive). European Commission, *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016, 1148* (Dec. 16, 2020), https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166.

[20] *See*, e.g., *EBA Guidelines on Outsourcing Arrangements*, Section 6, par. 35.

[21] See, e.g., *EBA Guidelines on Outsourcing Arrangements*, Section 4.

[22] See, e.g., EBA Guidelines on Outsourcing Arrangements, Section 13.3 (review outsourced function using a risk-based approach) & Title V, par. 114 (national financial regulators should use a risk-based approach). See also Juan Carlos Crisanto, Conor Donaldson, Denise Garcia Ocampo and Jermy Prenio, Regulating and supervising the clouds: emerging prudential approaches for insurance companies, FSI Insights on policy implementation No. 13, 23 (BIS Dec. 2018), https://www.bis.org/fsi/publ/insights13.pdf.

[23] *Id*, Sections 12.2–12.3. See also *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 2 (pre-outsourcing analysis and due diligence); *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 6 (pre-outsourcing analysis), Guideline 8 (risk assessment), Guideline 9 (due diligence).

[24] See FFIEC, *Outsourcing Technology Services, FFIEC: IT Examination Handbook* 10-11 (June 2004), https://ithandbook.ffiec.gov/media/274841/ffiec_itbooklet_outsourcingtechnologyservices.pdf.

related risks should be identified during planning, due diligence, and the selection of the cloud service provider.[25]

The EBA guidelines also provide that financial institutions should inform their respective regulatory authorities in a timely manner or engage in supervisory dialogue with competent authorities regarding planned outsourcing of critical or important functions (or where a previously outsourced function becomes critical or important).[26] Both the ESMA and EIOPA cloud outsourcing guidelines include similar requirements.[27] Other jurisdictions, such as South Korea, require regulatory approval for certain kinds of outsourcing, including the use of cloud services.[28]

2. Data Protection and Security

Regulatory authorities generally emphasize the importance of data protection and security issues in connection with outsourced activities.

The EBA outsourcing guidelines require that financial institutions ensure that service providers comply with appropriate information security standards, and that data and system security requirements are defined within the outsourcing agreement and continue to be monitored for compliance.[29] The guidelines also mandate that financial institutions include in outsourcing contracts for critical or important functions provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data.[30] Similarly, the ESMA guidelines provide that an outsourcing firm should set information security requirements in its cloud services agreement, in a manner that is proportionate to the nature, scale and complexity of the outsourced function.[31] And the EIOPA guidelines direct insurers, when outsourcing critical or important functions to the cloud, to define specific information security requirements in their cloud services agreements and monitor compliance on an ongoing basis.[32]

Although outsourcing frameworks typically do not impose any specific measures regarding the storage and usage of data, they do expect financial institutions to consider whether specific measures are necessary to appropriately protect data.[33] The FFIEC's

---

[25] See FFIEC, *Security in a Cloud Computing Environment*, p. 4 (Apr. 30, 2020), https://www.ffiec.gov/press/PDF/FFIEC_Cloud_Computing_Statement.pdf.
[26] *EBA Guidelines on Outsourcing Arrangements* , Section 11, par. 58.
[27] *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 8; *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 4.
[28] See, e.g., Financial Services Commission (South Korea), Regulation on Supervision of Electronic Financial Transactions, Notice No. 2018-36, Article 14-2 (amended Dec. 21, 2018) (requiring prior approval for the use of cloud for significant activities).
[29] *EBA Guidelines on Outsourcing Arrangements*, Section 13.2.
[30] *Id*, Section 13, par. 75(g).
[31] *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 4.
[32] *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 12.
[33] *See, e.g.*, *EBA Guidelines on Outsourcing Arrangements*, Section 12.2, par. 68(e); *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 4, par. 30; *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 12, par. 49(c).

informational notice on cloud computing, for example, outlines relevant risk management practices for cloud security management, including security controls for data.[34]

3. Additional Requirements for Sensitive Personal Data and Customer Information

Some regulators set forth specific requirements or guidance in connection with sensitive data, such as personal information. The EBA outsourcing guidelines, for example, mandate that financial institutions take a risk-based approach to seeing that sensitive data is adequately protected and kept confidential by TSPs. In particular, financial institutions are required to take into account differences between privacy regimes in different jurisdictions, especially in connection with the requirements imposed by the GDPR.[35] The ESMA and EIOPA guidelines likewise note that financial firms should take special account of sensitive data, and the potential impact of GDPR requirements, when outsourcing to cloud service providers.[36] The FFIEC outsourcing guidelines require banking institutions to ensure that service providers have appropriate measures in place to comply with applicable laws and supervisory expectations governing the confidentiality of customer information.[37]

4. Cross-Border Outsourcing

Outsourcing frameworks also address cross-border outsourcing. The focus on the location of data has become particularly salient in connection with the use of cloud services. The EBA, ESMA and EIOPA outsourcing guidelines require financial institutions to adopt a risk-based approach to data storage and processing locations, and to consider differences between jurisdictions regarding the protection of data.[38] The EBA and ESMA guidelines also direct national financial regulators to ensure that they can perform effective supervision, in particular when institutions outsource critical or important functions, outside the EU/European Economic Area.[39] FFIEC's cloud computing guidance similarly notes that a banking institution should understand the applicability of laws within a host country and the banking institution's ability to control access to its data before transferring data to another jurisdiction.[40] Several jurisdictions have imposed data residency requirements in connection with technology outsourcing, such as the use of cloud services.

---

[34] FFIEC, *Security in a Cloud Computing Environment*, pp. 5-6.
[35] *EBA Guidelines on Outsourcing Arrangements*, Section 13.2, pars. 83-84.
[36] *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 4, par. 30; *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 7, par. 29(f), Guideline 12, par. 47.
[37] FFIEC, *Outsourcing Technology Services* at 26, Banking institutions in the United States are subject to specific privacy requirements under the Gramm-Leach-Bliley Act. See 15 USC §§ 6801–6809.
[38] *EBA Guidelines on Outsourcing Arrangements*, Section 13.2, pars. 83-84; Section 12.1, par. 68; *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 4, par. 30(g); Guideline 2, par. 21(a)(vi); *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 12, par. 49(h); Guideline 8, par. 31(b)(iv).
[39] *EBA Guidelines on Outsourcing Arrangements*, Title V, par. 119; *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 9, par. 47.
[40] See FFIEC, *Outsourced Cloud Computing*, 4 (July 10, 2012), https://ithandbook.ffiec.gov/media/153119/06-28-12_-_external_cloud_computing_-_public_statement.pdf.

China, for example, requires that all storage, processing and analysis of personal financial information must be conducted within China.[41]

5. Business Continuity and Exit Strategies

Outsourcing frameworks generally require that financial institutions put in place business continuity plans dealing with service disruptions and other contingencies—especially the ability to terminate the outsourcing arrangement without disrupting any material functions. The EBA outsourcing guidelines require financial institutions to implement arrangements to maintain their ongoing functions if services provided by a service provider fail or deteriorate to an unacceptable degree.[42] Similarly, the ESMA and EIOPA guidelines direct outsourcing firms, when outsourcing critical or important functions, to ensure that effective business continuity and disaster recovery controls are in place.[43] The cloud computing notice recently published by the FFIEC provides that a banking institution's management should review and assess the resilience capabilities and service options available from a cloud service provider, and the outsourcing contract should outline the capabilities required by the institution. In addition, management should regularly update and test resilience and recovery capabilities—testing which may need to be conducted jointly with the cloud provider.[44]

A critical aspect of business continuity, emphasized across outsourcing frameworks, is the ability to smoothly terminate an outsourcing arrangement. The EBA outsourcing guidelines, for example, provide that a financial institution should make sure that it can exit a service arrangement, if needed, without disrupting provision of services and without being detrimental to the continuity of its services.[45] To that end, the guidelines require that outsourcing financial institutions develop and test comprehensive exit plans and identify alternative solutions to enable them to retrieve outsourced functions and data from a service provider and transfer them to alternative providers or back to the institution.[46] The EBA guidelines also mandate that outsourcing agreements include an obligation for service providers to support, in the event of termination, a financial institution in the transfer of activity, data or services to another service provider or back to the institution.[47] The ESMA and EIOPA cloud outsourcing guidelines impose similar requirements

---

[41] *See* People's Bank of China, *Notice Requesting Financial Institutions to Properly Conduct Personal Financial Information*, Circular 17 (Jan. 21, 2011). Other jurisdictions place limits on cross-border transfers of certain kinds of data, for instance, by requiring that data holders obtain consent before the cross-border transfer of data or that such a transfer be reported to the relevant authorities. More information on restrictions on cross-border data flows is available from the European Centre for International Political Economy at *Digital Trade Estimates Database*, https://ecipe.org/dte/database/.

[42] *EBA Guidelines on Outsourcing Arrangements,* Section 9. The guidelines also allow supervising regulators to request additional information on a financial institution's risk analysis for critical or important outsourced activities, including whether the provider has a service continuity plan that is suitable for the service provided to the financial institution. *Id*, Title V. par. 112.

[43] *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 4, par. 30(f); *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 12, par. 49.

[44] FFIEC, *Security in a Cloud Computing Environment*, pp. 6-7.

[45] *EBA Guidelines on Outsourcing Arrangements*, Section 7, par. 42; Section 15.

[46] *Id*.

[47] *Id,* Section 13.4.

in connection with the termination of cloud outsourcing arrangements.[48] Cloud-specific guidelines issued by other regulators include detailed, specific requirements regarding termination of cloud service arrangements.[49]

6. Ongoing Monitoring and Risk Management

Regulators generally require financial institutions to have monitoring and control frameworks in place for outsourcing arrangements and underscore that risk assessment and management continue after a financial institution enters into an outsourcing arrangement. They mandate that financial institutions review and monitor the performance of service providers on an ongoing basis using a risk-based, proportionate approach.[50] Regulatory authorities focus on two aspects of outsourcing institutions' ongoing responsibilities: (1) securing certain access and information rights, including the right to audit the service provider, and (2) ensuring that monitoring by financial institutions (particularly audits) is sufficient and meets generally recognized standards.[51]

The EBA outsourcing guidelines, for example, require that financial institutions secure from service providers (including cloud providers) both a right to audit as well as a right of physical access to the service providers' relevant business premises. Such access and audit rights are required for both the institutions themselves as well as, with respect to any outsourcing of critical or important functions, their regulatory supervisors.[52] The EBA guidelines also direct financial institutions to ensure that they can carry out penetration testing to assess the effectiveness of security measures and processes.[53] The FFIEC's outsourcing guidelines provide that a banking institution's outsourcing contract should specify the rights of the institution and its regulatory agencies to obtain the results of independent audits in a timely manner.[54]

While each of the EBA, ESMA and EIOPA guidelines allows financial institutions to rely on third-party certifications and reports for ongoing monitoring in certain circumstances, they require that those certifications and reports be based on generally

---

[48] *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 5; *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 15.

[49] See, e.g., Center for Financial Industry Information Systems (Japan), *Security Guidelines on Computer Systems for Financial Institutions*, Section V-2(1) No. 21 (mandating that: data provided by financial institutions be erased in an appropriate manner and time frame; information linking the data management area and data storage area be severed; and that the data storage area be wiped).

[50] *EBA Guidelines on Outsourcing Arrangements*, Section 14 (directing financial institutions to focus on critical or important functions and ensuring the availability, integrity and security of data and information); *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 4, par. 29; Guideline 6, par. 35; *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 14.

[51] *EBA Guidelines on Outsourcing Arrangements*, Section 13.3; *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 3, par. 28(n); Guideline 6; *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 10, par. 37(m), Guideline 11.

[52] *EBA Guidelines on Outsourcing Arrangements*, Section 13.3, par. 87.

[53] *Id*, par. 94.

[54] FFIEC, *Outsourcing Technology Services* at 13.

recognized auditing standards and be performed by auditors with adequate expertise.[55] The guidelines impose consistent standards in connection with community audits organized by a group of financial institutions that appoint a lead auditor from one of the institutions or an independent third-party auditor on their behalf.[56] Similarly, FFIEC's cloud computing guidance recommends that banking institutions make use of auditors to evaluate the adequacy of cloud service providers' internal controls, and in particular, notes that the assistance of third-party auditors with expertise in evaluating cloud environments may be necessary.[57]

7. Authority of Financial Regulators

Importantly, most financial regulators, including the ESAs and national financial regulators in the EU, currently lack the authority to directly supervise TSPs to ensure that regulatory expectations are met, and therefore lack a well-developed framework for using their supervisory tools to engage with TSPs.[58] To the extent that they have the authority to conduct inspections or obtain information from TSPs, it arises indirectly from mandatory audit and access provisions included in outsourcing contracts between financial institutions and TSPs. Their access is limited to what is included in the outsourcing contract.[59] In this respect, the United States is currently an outlier: U.S. bank regulators have statutory authority to supervise TSPs that provide services to banks and the FFIEC has issued guidance to agencies on how they should supervise TSPs.[60]

---

[55] *Id*, Section 13.3, pars. 91-93, 97 (allowing financial institutions to rely on third-party certifications and reports in the case of outsourcing of functions that are not critical or important); *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 6, par. 37; *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 11, pars. 42-43.

[56] *EBA Guidelines on Outsourcing Arrangements*, Section 13.3, par. 91(a); *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 6, par. 37; *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 11, par. 42.

[57] FFIEC, Outsourcing Cloud Computing at 3.

[58] See Basel Committee on Banking Supervision, *Cyber-resilience: Range of practices* 33–34 (BIS Dec. 2018); Juan Carlos Crisanto, Conor Donaldson, Denise Garcia Ocampo and Jermy Prenio, *Regulating and supervising the clouds: emerging prudential approaches for insurance companies*, FSI Insights on policy implementation No. 13, 26–28 (BIS Dec. 2018), https://www.bis.org/fsi/publ/insights13.pdf.

[59] See text accompanying notes 40-43.

[60] 12 U.S.C. §§ 1464(d)(7), 1867(c)(1); FFIEC, Supervision of Technology Providers (Oct. 2012).

Part II: The Digital Operational Resilience Act

a. DORA's Approach to the Management of ICT Third-Party Risk

DORA aims to establish a comprehensive framework on digital operational resilience for EU financial entities. It focuses on: (1) information and communication technologies ("ICT") risk management; (2) management, classification and reporting of ICT-related incidents; (3) digital operational resilience testing; and (4) managing ICT third-party risk. If enacted, the DORA provisions concerning the management of ICT third-party risk would alter the regulatory framework that applies to technology outsourcing by financial institutions in the EU, including their use of cloud services. DORA and any regulations promulgated thereunder would supersede current national regulatory provisions and supervisory approaches governing operational resilience and ICT security.[61] To the extent that DORA conflicts with existing outsourcing guidelines issued by each of the ESAs, the ESAs are expected to bring those guidelines into line with DORA once it is finalized.[62]

The DORA provisions on managing ICT third-party risk include: (1) key principles governing financial entities' sound management of third-party risk; and (2) a framework for the oversight of ICT third-party service providers ("TPPs") designated as "critical." As described in Part II.B., the key principles set forth in DORA share important similarities with existing supervisory frameworks for outsourcing, including the current outsourcing guidelines published by the ESAs. For example, like existing outsourcing frameworks, DORA's key principles provide that financial entities that outsource technology services retain primary responsibility for ICT risk management, including compliance with, and the discharge of, all obligations under DORA and applicable financial services law.[63] DORA's key principles also state that financial entities' management of ICT third party risk must be implemented in light of the principle of proportionality, as is generally the case under other outsourcing frameworks.[64]

DORA would also establish a new EU-level oversight framework for certain TSPs designated as "critical" by the ESAs. Specifically, the Joint Committee of the ESAs, upon recommendation from a newly established "Oversight Forum" composed of the ESA chairs and senior representatives from national financial authorities, must designate the

---

[61] DORA, *supra* note 1, at p. 14. See also *Joint Advice of the European Supervisory Authorities*: *To the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector* 7–11 (Apr. 10, 2019), https://eba.europa.eu/documents/10180/2551996/JC+2019+26+%28Joint+ESAs+Advice+on+ICT+legislative+improvements%29.pdf/4d2ad5e2-1570-48bd-819a-7cd9b4e8b157.

[62] See ESMA Guidelines on outsourcing to cloud service providers, p. 2 (noting that ESMA is "mindful of the proposal for [DORA]" and "will continue to closely monitor the development of this proposal to provide revised or additional guidance as necessary").

[63] DORA, *supra* note 1, at Article 25(1).

[64] DORA, *supra* note 1, at Article 25(2). Under Art. 25(2), "financial entities' management of ICT third party risk shall be implemented in light of the principle of proportionality, taking into account: (a) the scale, complexity and importance of ICT-related dependencies, (b) the risks arising from contractual arrangements on the use of ICT services concluded with ICT third-party service providers, taking into account the criticality or importance of the respective service, process or function, and to the potential impact on the continuity and quality of financial services and activities, at individual and at group level."

TSPs that are "critical" for financial entities ("CTPPs") according to specified criteria.[65] The criteria include the: (i) systemic impact on the stability, continuity or quality of the provision of financial services if the TSP were to experience a large scale operational failure; (ii) systemic character or importance of the financial entities[66] that rely on the TSP; (iii) reliance of financial entities on the services provided by a particular TSP in relation to critical or important functions of financial entities that ultimately involve that same TSP; (iv) degree of substitutability[67] of the TSP; (v) number of EU member states in which the TSP provides services; and (vi) number of EU member states in which financial entities using the TSP operate.[68]

The Joint Committee of the ESAs must appoint either the EBA, ESMA, or EIOPA as "Lead Overseer" for each CTPP.[69] The Lead Overseer is responsible for the direct monitoring of a CTPP at the EU level to evaluate potential financial sector risks that it could pose, and is vested with broad supervisory authorities to discharge its responsibilities.[70] The ESA that will serve as "Lead Overseer" for a particular CTPP is chosen based on the total value of assets of the financial entities using the CTPP's services.[71]

The CTPP oversight regime represents a significant departure from the current regulatory framework for technology outsourcing by financial institutions in Europe—EU financial regulators currently supervise and impose outsourcing requirements on financial institutions, but do not directly supervise TSPs. Key elements of this novel oversight framework are detailed in Part II.C.

---

[65] DORA, *supra* note 1, at Article 29. The Executive Directors of each ESA and a representative from each of the European Commission, ESRB, ECB and ENISA will also participate in the Oversight Forum as observers. DORA Art. 29(3).

[66] DORA, *supra* note 1, at Article 28(2)(b). The systemic character or importance of the financial entities that rely on the TPP is to be assessed based on: (i) the number of global systemically important institutions (G-SIIs) or other systemically important institutions (O-SIIs) that rely on the TPP and (ii) the interdependence between the G-SIIs or O-SIIs and other financial entities.

[67] DORA, *supra* note 1, at Article 28(2)(d). The degree of substitutability takes into account: "the lack of real alternatives, even partial, due to the limited number of [TPPs] active on a specific market, or the market share of the relevant [TPP], or the technical complexity or sophistication involved, including in relation to any proprietary technology, or the specific features of the [TPP's] organisation or activity; ii) difficulties to partially or fully migrate the relevant data and workloads from the relevant to another [TPP], due to either significant financial costs, time or other type of resources that the migration process may entail, or to increased ICT risks or other operational risks to which the financial entity may be exposed through such migration." *Id*.

[68] DORA, *supra* note 1, at Article 28(2).

[69] DORA, *supra* note 1, at Article 29. The Executive Directors of each ESA and a representative from each of the European Commission, ESRB, ECB and ENISA will also participate in the Oversight Forum as observers. DORA Art. 29(3).

[70] See, e.g., DORA paragraph (62).

[71] DORA, *supra* note 1, at Article 28(1)(b).

b. Similarities to Existing Outsourcing Frameworks

This section focuses on similarities between DORA's key principles for a sound management of ICT third-party risk by financial entities and existing supervisory frameworks governing outsourcing, including outsourcing guidelines published by the ESAs.[72]

1. Outsourcing Prerequisites

Like existing outsourcing frameworks, DORA requires financial entities to undertake a risk assessment and due diligence before entering into a service agreement with a third-party service provider. This assessment and diligence process involves familiar elements such as determining whether the proposed arrangement covers a "critical or important function" and ensuring that the proposed service provider is suitable.[73] And similar to the ESAs' existing outsourcing guidelines, DORA's key principles require financial entities to report new outsourcing arrangements to the applicable regulator.[74]

2. Data Protection and Security

Like existing outsourcing frameworks, DORA's key principles for a sound management of ICT third-party risk address security requirements associated with outsourcing arrangements: they provide that financial entities may only outsource ICT functions to service providers that comply with appropriate security standards.[75] In addition, the proposed rules outline contractual provisions that must be included in a financial entity's outsourcing arrangements; these include requirements that the ICT service provider have in place security measures that satisfy the financial entity's regulatory framework and provisions that address the integrity, security and protection of personal data.[76]

3. Cross-Border Outsourcing

Like existing outsourcing regulations and guidelines, DORA's key principles for the management of ICT third-party risk require financial entities to take into account risks associated with cross-border outsourcing. They provide that before concluding a contract with an ICT service provider in another country, financial entities should consider factors such as the data protection regime in place in that country, the effective enforcement of law, and constraints that may arise with respect to urgent data recovery.[77] They also require contracts for ICT services to specify the locations where functions and services

---

[72] DORA, which is limited to ICT third-party risk, applies more narrowly than the EBA guidelines, which apply to all outsourcing. However, its scope is broader than the ESMA and EIOPA guidelines, since they only apply to cloud outsourcing.
[73] *Id.*, Art. 25(5).
[74] *Id.*, Art. 25(4).
[75] *Id.*, Art. 25(6). Article 25(6) provides that "[f]inancial entities may only enter into contractual arrangements with ICT third-party service providers that comply with high, appropriate and the latest information security standards."
[76] *Id.*, Art. 27(2)(c).
[77] *Id.*, Art. 26(2). See also *id*, Art. 27(2)(g) (requiring contracts with ICT service providers to have in place security measures that guarantee the secure provision of services by the financial entity).

are to be provided, including the storage location, and require notification if any change in location is expected.[78]

4. Business Continuity and Exit Strategies

In addition, the key principles set forth in DORA, like existing supervisory frameworks for outsourcing, require financial entities to plan for service disruptions and other contingencies, including by maintaining the ability to terminate a service arrangement with an ICT service provider without disrupting material functions. The DORA principles require financial entities to ensure that service arrangements are terminated under specific circumstances (for example, when the service provider has "evidenced weaknesses" in the way it ensures the security and integrity of sensitive data);[79] to put in place comprehensive exit strategies to transition functions away from a service provider and maintain business continuity;[80] and to include contractual provisions covering contingency plans, termination rights and exit strategies.[81]

5. Ongoing Monitoring and Risk Management

DORA's ICT third-party risk management principles also emphasize the importance of ongoing monitoring using a risk-based approach.[82] As with the existing outsourcing frameworks, the proposed rules require financial entities to secure access and information rights, including the right to audit the service provider.[83] They also provide that audits should adhere to commonly accepted audit standards and, for outsourcing that involves a high level of technological complexity, a financial entity must ensure that auditors have the appropriate skills and knowledge to effectively assess the service provider.[84]

c. Divergences from Existing Outsourcing Frameworks

This section highlights notable divergences between DORA provisions governing financial entities' management of third-party ICT risk and existing guidance on technology outsourcing, focusing on DORA's provisions concerning the direct oversight of TSPs deemed "critical." As described above, there is no legal or regulatory precedent in Europe for the DORA CTPP oversight framework, which provides for the direct supervision of certain TSPs by EU financial regulators. The proposed direct oversight framework also represents a meaningful departure from the current oversight framework for TSPs in the United States, which involves risk-based—not prescriptive—supervision whose primary

[78] *Id.*, Art. 27(2)(b).
[79] *Id.*, Art. 25(8).
[80] *Id.*, Art. 25(9).
[81] *Id.*, Art. 27(2)(g), (j), (k).
[82] *Id.*, Art. 25(7).
[83] *Id.*, Art. 27(2)(h).
[84] *Id.*, Art. 25(7).

aim is to help client financial institutions comply with applicable legal requirements.[85] Key elements of this novel oversight framework are summarized below.

1. Direct, Ongoing Supervision of CTPPs and Annual Oversight Plans

DORA establishes a robust supervisory framework that subjects each TSP designated as "critical" to direct, ongoing oversight by the ESA designated as its Lead Overseer. Under DORA, a CTPP's Lead Overseer must assess whether the CTPP has sound, comprehensive, and effective rules, mechanisms, procedures, and arrangements in place to manage the ICT risks that it could pose to financial entities.[86] The assessment includes, inter alia, the CTPP's risk management processes, governance arrangements, physical security contributing to ensuring ICT security (e.g., security of data centers), ICT audits, and testing of ICT systems, infrastructure and controls.[87] Based on this assessment, the Lead Overseer must adopt a "clear, detailed and reasoned individual Oversight plan" annually for each CTPP.[88]

The proposed framework for direct supervision of CTPPs represents a significant departure from current supervisory approaches, in two respects. First, to the extent that financial supervisors currently have the authority to conduct inspections or obtain information from TSPs, that authority generally arises indirectly from provisions included in contracts with financial entities—not from independent regulatory authority. In addition, supervisors that have the legal authority, whether embodied in regulation or contract, to oversee TSPs, lack a well-developed framework for exercising it and rarely do so.[89]

2. Information, Investigation, and Inspection Powers

To carry out its supervisory responsibilities, the Lead Overseer is vested with broad powers to request information and documents, including potentially sensitive data, from a CTPP and to conduct investigations and inspections of its business premises.[90]

The Lead Overseer may request or require the CTPP to provide all information that is necessary for the Lead Overseer to discharge its duties under DORA.[91] Information that must be provided includes "all relevant business or operational documents, contracts,

---

[85] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, Administrative Guidelines: Implementation of Interagency Programs for the Supervision of Technology Service Providers 2 (Oct. 2012), https://ithandbook.ffiec.gov/media/153533/10-10-12_-_administrative_guidelines_sup_of_tsps.pdf.
[86] DORA, at Article 30(1).
[87] DORA at Article 30(2).
[88] DORA at Article 30(3).
[89] *See* Basel Committee on Banking Supervision, *Cyber-resilience: Range of practices* 33–34 (BIS Dec. 2018); Juan Carlos Crisanto, Conor Donaldson, Denise Garcia Ocampo and Jermy Prenio, *Regulating and supervising the clouds: emerging prudential approaches for insurance companies*, FSI Insights on policy implementation No. 13, 26–28 (BIS Dec. 2018), https://www.bis.org/fsi/publ/insights13.pdf.
[90] *See* DORA at Article 31(1)(a)-(b); Article 32-34
[91] DORA at Article 32(1).

policies documentation, ICT security audit reports, ICT-related incident reports" and information regarding parties to whom the CTPP has outsourced operational functions.[92]

The Lead Overseer is also authorized to conduct general investigations, assisted by a dedicated examination team for each CTPP. Its powers in connection with investigations include the right to examine and take copies of records, data, procedures and other relevant material; summon representatives of the CTPP for oral or written explanations of facts or documents relevant to the investigation; and collect information, and request records of telephone and data traffic.[93]

In addition, the Lead Overseer and examination team are empowered to access and inspect CTPPs' business properties, including offices and operation centers, and to conduct off-line inspections.[94] While inspecting a CTPP, they may seal the premises and any books or records, to the extent necessary for the inspection.[95] Inspections cover a wide range of the CTPP's property and systems, including all of the networks, devices, data and information that the CTPP uses in providing services to financial entities.[96]

Within three months after an investigation or inspection is completed, the Lead Overseer must adopt recommendations for the CTPP, and immediately communicate these recommendations to the CTPP and to the national financial authorities that regulate its financial entity customers.[97]

Financial regulators in most jurisdictions currently do not have the authority to directly investigate or inspect TSPs. To the extent that they have the right to conduct onsite inspections and obtain information from TSPs, it is only on the basis of limited contractual provisions included in service agreements with financial institutions. Financial regulators that lack that authority typically engage with TSPs on an informal, voluntary basis.[98]

3. Lead Overseer's Power to Issue Substantive Recommendations to CTPPs

DORA empowers the Lead Overseer to "address recommendations" to each CTPP regarding certain substantive issues relating to ICT risks.[99] For example, recommendations may address the use of specific ICT security and quality requirements or processes or the use of conditions and terms under which the CTPP provides services that the Lead Overseer deems relevant to prevent the generation of single points of failure.[100] They may also address the CTPP's planned subcontracting, where the Lead Overseer deems

[92] DORA at Article 32(1).
[93] DORA at Article 33.
[94] DORA at Article 34(1).
[95] DORA at Article 34(2).
[96] *See* DORA at Article 34(4).
[97] DORA at Article 35(4)-(5). The recommendations are adopted after consultation of the Oversight Forum.
[98] *See* Basel Committee on Banking Supervision, *supra* note 33, at 33–34; Crisanto et al., *supra* note 33 at 26–28.
[99] DORA at Article 31(1)(d).
[100] DORA at Article 31(1)(d)(i)-(ii).

that subcontracting could trigger risks to financial stability or for the provision of services by the financial entity client.[101] In addition, the Lead Overseer can recommend that the CTPP refrain entirely from entering into a subcontracting arrangement, if the prospective subcontractor is a TSP established in a third country and the subcontracting concerns a critical or important function of the financial entity.[102]

Within thirty days of receiving the Lead Overseer's recommendations, the CTPP must notify the Lead Overseer as to whether it intends to follow them.[103] The Lead Overseer must then share this information with national financial regulators, which will monitor whether financial entities take into account the risks identified in the recommendations.[104] The national financial regulators can require financial entities to temporarily suspend the use or deployment of a service provided by the CTPP until the risks identified in the recommendations have been addressed.[105] When necessary, they can also require financial entities to terminate related contractual arrangements with the CTPP.[106]

Under current supervisory frameworks, financial regulators do not have authority to issue substantive recommendations directly to TSPs on technical issues like the appropriate level of protection for confidential data. Instead, current guidelines set forth principles relating to issues that financial institutions—not TSPs—must consider when outsourcing to a TSP. Similarly, financial regulators do not have authority to direct substantive recommendations to TSPs about the TSP's planned subcontracting, or to recommend that a TSP refrain from entering into certain subcontracts.

DORA's provisions for follow-up by national financial regulators are in some respects similar to existing ESA guidance. For example, the EBA outsourcing guidelines provide that a national financial regulator should take appropriate action, including by requiring exit from an outsourcing arrangement, when it concludes that a financial institution does not have robust governance arrangements in place or is not complying with regulatory requirements.[107] There are, however, important differences between the proposed authority in DORA and the existing guidelines. The DORA authority focuses on failure of a CTPP to address specific recommendations, not a particular financial institution's overall risk management relationship with a TSP. Moreover, the EBA guidelines heavily qualify the scope of national financial regulators' authority: suspension or termination should only be required if "appropriate", taking into account the financial institution's "need [to] operate on a continue basis", as a last resort if "supervision and enforcement of regulatory requirements cannot be ensured by other measures."[108] The corresponding provisions of DORA lack any similar qualifications.

---

[101] DORA at Article 31(1)(d)(iii).
[102] DORA at Article 31(1)(d)(iv).
[103] DORA at Article 37(1).
[104] DORA at Article 37(1)-(2).
[105] DORA at Article 37(3).
[106] DORA at Article 37(3).
[107] EBA Guidelines, Title, par. 118.
[108] *Id.*

4. Penalties Regime

If a CTPP does not comply with the Lead Overseer's request for information or exercise of its investigation and inspection powers, the Lead Overseer is authorized to impose a financial penalty on the CTPP.[109] The penalty is equal to 1% of the average daily worldwide turnover of the CTPP in the preceding business year, and is imposed on a daily basis until the CTPP comes into compliance, for no more than six months.[110] Penalty payments are enforceable, in accordance with the rules of civil procedure in the EU member state where inspections and access are carried out.[111] Certain due process protections are provided to the CTPP prior to the imposition of the penalty.[112] The ESAs are generally required to publicly disclose any penalties imposed on CTPPs.[113]

Under current supervisory frameworks, financial regulators in the EU and U.S. have limited authority to impose financial penalties on TSPs. As noted above, EU supervisory authorities can only require financial institutions to suspend or terminate their arrangement with a TSP, usually as a last resort, if they find that the arrangement violates a regulatory requirement or is not subject to a robust risk management framework. In the U.S., federal banking agencies have authority to take enforcement action against TSPs in connection with the performance of services for banks, to the same extent as if such services were performed by the bank itself.[114] The threshold for bringing such an enforcement action is relatively high.[115]

5. Financial Entities' Use of Non-EU ICT Third-Party Service Providers

Certain provisions in DORA impose potential limitations on financial entities' use of TSPs located outside of the EU. Under Article 28(9), financial entities are not permitted to "make use of" a TSP established in a third country, which has no business or presence in the EU, if the TSP would be designated as critical if it were established in the EU.[116] In addition, DORA empowers a CTPP's Lead Overseer to recommend that it refrain from

---

[109] DORA at Article 31(4). Article 31(1)(c) empowers the Lead Overseer to request reports from a CTPP that detail the actions taken or remedies implemented in response to the Lead Overseer's recommendations; the Lead Overseer may also assess a penalty to compel compliance with this provision.
[110] DORA at Article 31(5)-(6).
[111] DORA at Article 31(7).
[112] DORA at Article 31(8). For example, the Lead Overseer is required to base its penalty decisions only on findings on which the applicable CTPP has had the opportunity to comment.
[113] DORA at Article 31(8).
[114] 12 U.S.C. § 1867(c); 12 U.S.C. § 1464(d)(7)(D). Federal banking agencies also have authority to take enforcement action against TSPs that are "institution-affiliated parties" of banks under the primary enforcement statute. 12 U.S.C. § 1818(b)(1) (cease-and-desist orders), (i)(2) (civil money penalties); 12 U.S.C. § 1813(u).
[115] Enforcement actions require the agency to show that the TSP engaged in an "unsafe or unsound practice", a violation of law, rule, regulation, final agency order, or a breach of fiduciary duty. The phrase "unsafe or unsound practice" refers specifically to practices that threaten the financial integrity of a bank. *See* Johnson v. OTS, 81 F.3d 195, 204 (D.C. Cir. 1996).
[116] DORA at Article 28(9).

entering into a subcontracting arrangement with a TSP established outside the EU if doing so would implicate a critical or important function of a financial entity client of the CTPP.[117]

These requirements represent a departure from the current approach adopted by EU-level and national financial regulators. Under that approach, the location of a TSP is one risk factor among many that financial institutions must take into account, as part of their risk-based approach to outsourcing, in determining whether to outsource a particular function to the TSP.[118] Similarly, national financial regulators are required to ensure that cross-border outsourcing does not impede their ability to engage in effective supervision, especially of critical or important functions.[119] Neither of these limitations, however, categorically restricts cross-border outsourcing.

[117] DORA at Article 31(1)(d)(iv).
[118] *EBA Guidelines on Outsourcing Arrangements*, Section 13.2, pars. 83-84; Section 12.1, par. 68; *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 4, par. 30(g); Guideline 2, par. 21(a)(vi); *EIOPA Guidelines on outsourcing to cloud service providers*, Guideline 12, par. 49(h); Guideline 8, par. 31(b)(iv).
[119] *EBA Guidelines on Outsourcing Arrangements*, Title V, par. 119; *ESMA Guidelines on outsourcing to cloud service providers*, Guideline 9, par. 47.

Part III: Recommendations for a More Effective DORA

As described in Part II, the European Commission's DORA proposal diverges substantially from existing regulatory and supervisory frameworks for TSPs, such as cloud service providers, that serve financial institutions. Most significantly, the DORA proposal would provide regulators with direct oversight of many of those TSPs, including the authority to issue substantive recommendations, impose penalties and prohibit the use of non-EU TSPs. We are concerned that this significant departure from existing regulatory and supervisory frameworks may discourage financial institutions from adopting new information and communication technologies, including cloud services, that could meaningfully enhance their operational efficiencies. It is unclear that such a step is appropriate to ensure that financial institutions' use of third-party ICT is well-regulated.

DORA's stated goals include: establishing a regulatory framework that is proportionate and risk-based; promoting cross-border regulatory harmonization and coordination; and facilitating innovation in financial services while ensuring operational resilience. The DORA proposal includes measures that will meaningfully promote these goals. But it also contains several provisions that, if adopted, could frustrate the achievement of each of these goals. We therefore recommend that the EU consider certain revisions to the current DORA proposal that would better align DORA with its stated goals and with other regulatory and supervisory frameworks for the use of cloud services by financial institutions. Our recommendations are set forth below.

a. Establishing a Proportionate and Risk-Based Regulatory Framework

The explanatory memorandum that accompanies the DORA proposal emphasizes that the "proposed rules do not go beyond what is necessary in order to achieve the objectives of the proposal."[120] In addition, the memorandum states that the rules are meant to be "tailored to [the] risks and needs" of specific financial entities, based on their "size and business profiles."[121] As noted in Part II, the principle of proportionality is embedded in DORA's key principles governing financial institutions' management of ICT third party risk, which provide that such management shall take into account the "scale, complexity and importance of ICT-related dependencies" as well as "the risks arising from contractual arrangements … with ICT third-party service providers."[122] Another element of the DORA rules that reflects the notion of proportionality is the reservation, in several contexts, of heightened risk management protocols for the outsourcing of "critical and important functions".[123] DORA likewise instructs financial entities to adopt a risk-based approach to determining the frequency and scope of audits and inspections of TSPs.[124]

---

[120] DORA at p.3.
[121] *Id*.
[122] DORA at Art. 25(2).
[123] *See, e.g.,* DORA at Art. 25(3) (requiring a financial entity's management body to review identified risks in respect of outsourcing of critical or important functions).
[124] DORA at Art. 25(7).

The principle of proportionality, however, does not fully inform DORA throughout. In particular, the direct oversight framework prescribed by DORA falls short when measured against the standard of proportionality. DORA provides the Lead Overseer with broad oversight and monitoring authority over designated CTPPs, including to issue prescriptive security and subcontracting recommendations, but does not require the Lead Overseer to exercise that authority in a proportionate and risk-based manner.[125] There does not appear to be any limit, for instance, preventing the Lead Overseer from exercising its oversight authority by issuing such recommendations with respect to any ICT services that a designated CTPP provides to a financial institution, even if that service is not used by the financial institution for a critical or important function. The absence of any such limitation represents a departure from existing guidelines; the EBA outsourcing guidelines, for example, direct national financial regulators to take a "risk-based approach" to assessing financial institutions' management of outsourcing risks.[126] DORA also does not provide CTPPs with a right to be heard in connection with the development of oversight plans, the conduct of examinations or the formulation of follow-up recommendations.[127] A supervisory approach that enables CTPPs to give input on oversight plans would allow for risk monitoring and mitigation measures that are calibrated more efficiently.

Another example of DORA's lack of proportionality relates to the financial penalty for non-compliance with the Lead Overseer's recommendations: DORA grants the Lead Overseer the discretion to impose a daily financial penalty on a CTPP for non-compliance but not to determine the size of the penalty, which is set at a rigid one percent of the CTPP's average daily worldwide turnover. [128] Because the Lead Overseer cannot weigh other factors, such as the severity of the CTPP's failure to comply or even the share of the CTPP's average daily turnover that serves EU financial institutions, the imposition of this penalty is likely to be disproportionate to any specific compliance failure.

We recommend that DORA be revised to more comprehensively incorporate the principle of proportionality, especially with respect to the oversight framework for CTPPs. This recommendation is consistent with the similar recommendation of the individual chairs of the ESAs.[129] Accordingly, the proportionality principle should be incorporated directly and explicitly in the oversight framework for CTPPs, just as it is for financial entities' individual management of ICT third party risk. More specifically, the penalties regime should be revised to clarify that penalties should be imposed by the Lead Overseer in a

---

[125] DORA at Art. 31(1).

[126] *EBA Guidelines on Outsourcing Arrangements*, Title V, par. 114.

[127] In contrast, a federal banking agency in the U.S. that takes enforcement action against a TSP based on an "unsafe or unsound practice" must satisfy certain procedural requirements, including the right to be notified of the basis of the action and to respond on the merits. See 12 U.S.C. § 1818(h). The U.S. banking agencies are also required to establish a process for administrative appeal of any material adverse supervisory determination, which would arguably apply to examination ratings received pursuant to the FFIEC's uniform rating system for TSPs. See 12 U.S.C. § 4806.

[128] DORA at Art. 31(6).

[129] Steven Maijoor (Chair, ESMA), Jose Manuel Campa (Chairperson, EBA) & Gabriel Bernardino (Chair, EIOPA), *Legislative proposal for a regulation on digital operational resilience for the financial sector* (Feb. 9, 2021), https://www.esma.europa.eu/sites/default/files/library/esa_2021_07_letter_dora_oversight.pdf.

manner that it proportionate, not punitive. The Lead Overseer should have discretion to set financial penalties for non-compliance at any amount up to a certain cap—for example, one percent of a CTPP's turnover attributable to its financial services business (not *all* business) in the EU (not globally)—based on the severity of the CTPP's non-compliance.

b. Promoting Cross-Border Regulatory Harmonization and Coordination

Another of DORA's stated aims is to "put in place a detailed and comprehensive framework on digital operational resilience" in order to ameliorate the "overlaps, inconsistencies, duplicative requirements, high administrative and compliance costs" and undetected and unaddressed ICT risks resulting from the proliferation of disparate national regulatory and supervisory approaches.[130] Regulatory harmonization is especially important in the case of financial institutions and TSPs, many of which operate in multiple jurisdictions and who are hampered by duplicative—or in some cases, inconsistent—regulatory or supervisory requirements.[131]

DORA's focus on regulatory harmonization is reflected in its key principles for financial entities' management of third-party risk, which establish a single set of rules governing their service relationship with third-party service providers in order to promote cross-border regulatory harmonization.[132] Similarly, the CTPP oversight framework is rooted in the policy judgment that EU-wide authority is needed to monitor risks stemming from TSPs.[133] Moreover, the oversight framework subordinates national financial regulators to the authority of the ESAs, ensuring that CTPPs will only face a single set of EU requirements: once a CTPP Oversight Plan is finalized, national financial regulators may only take measures concerning CTPPs in agreement with the Lead Overseer.[134] Although intra-European harmonization is the focus of DORA, the proposed rules also contemplate international cooperation between the ESAs and foreign regulatory authorities regarding the review of TSP risk management practices and controls.[135]

While DORA takes significant steps toward regulatory harmonization—especially for the requirements governing financial entities—it falls short in several key areas. For one, the current proposal does not clarify how DORA's provisions on the management of ICT third-party risk interact with relevant outsourcing guidance promulgated by the ESAs. In addition, the proposed allocation of powers between the ESAs and national financial regulators may give rise to regulatory fragmentation: national financial regulators are responsible for execution on and enforcement of the Lead Overseer's recommendations at the financial entity-level and may take divergent approaches in doing so.[136] There are also notable gaps in DORA's approach to harmonization of regulatory and supervisory requirements applicable to TSPs. Although DORA explicitly defines the relationship

[130] DORA at p.1.
[131] DORA at p.2, 14.
[132] DORA at Art. 25.
[133] DORA at p. 18.
[134] DORA at Art. 30(4).
[135] DORA at Art. 39.
[136] DORA at Art. 37(2).

between DORA and general cybersecurity requirements (in particular, the NIS Directive) for financial entities,[137] it is silent on the relationship when it comes to TSPs, including CTPPs. Accordingly, it does not specify how the Lead Overseer responsible for oversight of a CTPP will coordinate that oversight with other supervisory authorities, such as cybersecurity regulators, to which the CTPP is responsible in order to share information and mitigate redundancies.[138]

DORA also could do more to enhance harmonization and coordination with non-EU regulatory and supervisory frameworks, given that many of the financial institutions and TSPs that are subject to DORA also operate outside the EU. As described in more detail in Part II of this report, many elements of DORA's CTPP oversight framework differ significantly from non-EU financial regulators' supervisory regimes with respect to TSPs. These divergences undercut efforts to harmonize supervisory schemes across jurisdictions. Moreover, DORA does not expressly contemplate coordination between the ESAs and CTPPs' non-EU supervisors to mitigate regulatory and supervisory redundancies. Such coordination is especially significant given the possibility that other supervisory authorities might also seek direct oversight authority over major TSPs.

To ensure that DORA's goal of enhancing cross-border harmonization and coordination is met, we recommend that DORA be revised to clarify the relationship between DORA and the ESAs' existing outsourcing guidelines (e.g., specifying explicitly that DORA supersedes current outsourcing guidelines). In addition, the respective roles and powers of the ESAs and national financial regulators within the CTPP oversight framework should be clarified, while underscoring the Lead Overseer's executive position. DORA's oversight framework for CTPPs should also recognize that many CTPPs will also be subject to oversight by both national cybersecurity regulators as well as foreign regulators. DORA should thus clarify how the Lead Overseer will cooperate with its cybersecurity counterparts in order to share information and eliminate redundancies. In addition, DORA should be revised to explicitly endorse cooperation with foreign financial regulatory and supervisory authorities in connection with promoting consensus around shared substantive principles for management of ICT third-party risk and oversight of TSPs, as well as coordinating and sharing supervisory assessments of TSPs that operate in multiple jurisdictions. Such cooperation could benefit regulators by allowing them to leverage the expertise of their supervisory counterparts, reduce redundant compliance obligations for TSPs and provide financial companies with information that can help them assess risks and comply with laws and regulations.

c. Facilitating Innovation While Promoting Operational Resilience

DORA is one of a series of European Commission proposals—including proposals covering regulation of cryptocurrency assets and distributed ledger technology market infrastructure—that are intended to "further enable and support the potential of digital

[137] DORA at Art. 1(2).

[138] Under the European Commission's new NIS 2 Directive proposal, many CTPPs, such as providers of cloud services and data centers, would be considered providers of essential services and subject to supervision of the national cybersecurity regulatory of their primary establishment. *NIS 2 Directive*, Arts. 24-25.

finance in terms of innovation and competition while mitigating the risks arising from it."[139] The DORA proposal, in its preamble, acknowledges that financial institutions' use of ICT services is driven by "their need to adapt to an emerging competitive digital global economy, to boost their business efficiency and to meet consumer demand."[140] Accordingly, DORA aims to strike a balance between enabling financial institutions to leverage ICT services to innovate in order to meet their evolving business needs, and ensuring that they do so in a manner that maintains their operational resilience. In several respects, DORA succeeds in striking that balance. As detailed in Part II, many of the key principles governing financial entities' management of ICT third party risk closely track existing supervisory frameworks, especially the ESAs' existing outsourcing guidelines.[141] This consistency will allow financial entities, as well as TSPs, to take advantage of their existing risk management processes and controls, which they have already deployed effectively to support their operational resilience, to comply with DORA.

However, certain provisions of DORA could, if adopted, impede innovation by imposing significant compliance costs without promoting operational resilience. Indeed, these provisions may actually hamper financial institutions' operational resilience by restricting the use of operational or technological solutions to risk mitigation. For example, DORA subjects subcontracting arrangements of TSPs, particularly CTPPs, to a high level of scrutiny.[142] TSPs, such as cloud service providers, regularly outsource select functions in a manner that allows them to deploy updates and address newly discovered vulnerabilities. Burdensome subcontracting restrictions could disrupt TSPs' business operations (including their non-financial services operations), impeding their agility and innovation while also undermining their operational resilience. In addition, the ability of Lead Overseers to take potentially sensitive information exposes CTPPs and, by extension, the financial companies they serve to significant security risk in connection with security breaches at a Lead Overseer.[143]

Other provisions could also impede innovation without serving any discernable resilience benefit. As noted above, DORA restricts financial entities' use of certain non-EU service providers: financial entities are not permitted to make use of a third-country TSP that has no business or presence in the EU if the TSP would be designated as critical if it were established in the EU.[144] Although we understand that this provision would not apply to large U.S. TSPs that have business and a presence in the EU, such as AWS or Google

---

[139] DORA at p. 0.
[140] DORA at pp. 17-18.
[141] See above Part II.B.
[142] *See, e.g.,* DORA Art. 27(2)(b) (outsourcing contracts must include granular details on the locations where subcontracted functions and services are to be provided and where data is to be processed, including the storage location, and a third-party service provider must notify a financial institution if a change in location is expected); Art. 31(1)(d)(iii)-(iv) (Lead Overseer has power to make recommendations regarding subcontracting arrangements, including that further subcontracting arrangements be refrained from where certain conditions are met).
[143] Art. 33(2)(b). The EBA, one of the authorities that will serve as a Lead Overseer, was recently targeted in a hacking operation. *See* John O'Donnell, *European banking regulator EBA targeted in Microsoft hacking*, Reuters (Mar. 8, 2021), https://www.reuters.com/article/us-microsoft-hack-eba/european-banking-regulator-eba-targeted-in-microsoft-hacking-idUSKBN2B01RP.
[144] DORA Art. 28(9).

Cloud, this restriction limits the availability of TSPs for financial institutions and favors incumbent providers over more innovative competitors. It may also undermine financial institutions' operational resilience: in the case of cloud services, for example, the use of out-of-jurisdiction infrastructure allows financial institutions to distribute copies of applications or data to multiple locations (making them more difficult to target) and route incoming application traffic across geographic regions (making cloud services more resilient to local failure).[145]

Accordingly, we recommend that DORA's restriction on the use of non-EU service providers be eliminated. With respect to DORA's provisions governing subcontracting, we recommend that those be limited to subcontracted functions that are "critical or important" to the operations of a financial institution. And DORA should explicitly allow, in connection with requests for sensitive information or data, for CTPPs and their Lead Overseers to cooperate to find alternative arrangements for a CTPP to provide responsive information that does not involve highly sensitive information or data leaving the CTPP's premises.

[145] PROGRAM ON INTERNATIONAL FINANCIAL SYSTEMS, *Cloud Computing in the Financial Sector: A Global Perspective* at 32-33.

Program on International Financial Systems (PIFS)
134 Mount Auburn Street, Cambridge, MA 02138
www.pifsinternational.org