PIFS

Program on International Financial Systems

Regulation of Governance & Risk Management:

The Intersection of Banking & Technology

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

Dennis Campbell, Professor of Business Administration, Harvard Business School

John Gulliver, Executive Director, Program on International Financial Systems

JULY 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.

Regulation of Governance & Risk Management: The Intersection of Banking & Technology

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

Dennis Campbell, Professor of Business Administration
Harvard Business School

John Gulliver, Executive Director
Program on International Financial Systems

Contents

Executive Summary

In this paper, we evaluate the regulatory structure for risk management at U.S. banking institutions as compared to technology companies. We also evaluate the appropriate regulatory structure for cloud service providers to U.S. banking institutions, as banking institutions are increasing their reliance on cloud service providers for their data needs and effective risk management regulation can safely facilitate that transition.

Part I of our paper provides a comprehensive review of the regulation of corporate governance and risk management at U.S. banking institutions with a focus on how the regulatory structure is tailored to address the business activities of U.S. banks. We find that the regulation of risk management processes by U.S. banking institutions is highly prescriptive and that U.S. banking regulators have centralized key risk management responsibilities with the board of directors and senior management.

Part II of our paper reviews the regulation of corporate governance and risk management at U.S. technology companies. We find that the regulation of risk management at technology companies is principles-based and does not shift prescriptive responsibilities to technology companies' board of directors.

Part III of our paper considers whether the banking approach to the regulation of risk management or the technology approach to the regulation of risk management is better suited for cloud service providers to U.S. banks. In doing so, we consider key differences between the risks faced by U.S. banking institutions as compared to cloud service providers. We conclude that a principles-based and decentralized approach to the regulation and supervision of cloud service providers and other technology services providers to U.S. banking institutions would better address the risks inherent in such services and facilitate continued adoption of cloud services by U.S. banking institutions.

Part I: Corporate Governance and Risk Management at U.S. Banks and U.S. BHCs

In Part I we begin by providing a brief history of the regulation and supervision of U.S. banks with a focus on the oversight of risk management policies and procedures. We then provide an overview of the legal and regulatory requirements for risk management that apply to U.S. banks and U.S. bank holding companies with a focus on the role of the board of directors. Next, we review the role of banking regulators in supervising banks' and bank holding companies' compliance with risk management requirements. We provide a case study of the recent regulatory and supervisory actions related to risk management at Citibank that demonstrates the highly prescriptive and central role of the board of directors in overseeing risk management at U.S. banking institutions. Finally, we review certain policy issues with the existing centralized and prescriptive approach to risk management at U.S. banking institutions.

a. Historical Background

Following the Great Depression, banks were highly restricted, by both federal and state law, in terms of the activities that they could engage in and where they could operate.[1] However, in the late 1980s, Federal Reserve interpretations of the Glass-Steagall Act and the Bank Holding Company Act allowed bank holding companies to deal in and underwrite a wide variety of securities.[2] Likewise beginning in the 1980s, the Office of the Comptroller of the Currency ("OCC") issued a series of interpretive letters of the National Bank Act of 1863 that allowed banks to trade and deal in derivatives.[3] And in 1994, the Riegle-Neal Act enabled banks to open branches across state lines by repealing restrictions on interstate branching.[4] Five years later, the Gramm-Leach-Bliley Act repealed Glass-Steagall's limits on combining commercial and investment banking.[5]

Following these legal and regulatory changes, the scope of activities and size of U.S. banking organizations grew substantially. Bank supervision also shifted from a regime of oversight that relied predominantly on an examination of individual transactions to oversight that focused on a bank's policies and processes for risk management. Although the shift was largely driven by the need to supervise a much wider range of activities,[6] it was also a response to failures of supervisory oversight that had resulted in the wave of

---

[1] Glass-Steagall Act, ch. 89, 48 Stat. 162 (1933); McFadden Act, Pub. L. No. 639, 69th Congress, H.R. 2 (1927). *See generally* Bernard Shull, T*he Separation of Banking and Commerce in the United States: An Examination of Principal Issues*, 8(3) FINANCIAL MARKETS, INSTITUTIONS, & INSTRUMENTS 1 (Aug. 1999).

[2] Bernard Shull, T*he Separation of Banking and Commerce in the United States: An Examination of Principal Issues*, 8(3) FINANCIAL MARKETS, INSTITUTIONS, & INSTRUMENTS 1 (Aug. 1999).

[3] Saule T. Omarova, *The Quiet Metamorphosis: How Derivatives Changed the "Business of Banking",* CORNELL LAW FACULTY PUBLICATIONS (2009).

[4] *Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994*, PUB. L. NO. 103-328; 108 STAT. 2338 (1994).

[5] *Gramm-Leach-Bliley Act*, PUB. L. NO. 106-102, 113 STAT. 1338 (1999).

[6] *See* FEDERAL RESERVE SYSTEM, *Remarks by Chairman Alan Greenspan* (Feb. 21, 1997), https://www.federalreserve.gov/boarddocs/speeches/1997/19970221.htm. *See also* FEDERAL RESERVE SYSTEM, *Testimony of Chairman Alan Greenspan* (March 19, 1997), https://www.federalreserve.gov/boarddocs/testimony/1997/19970319.htm.

savings and loans failures in the late-1980s and early-1990s.[7] Speaking in 1996, then-Fed Chair Alan Greenspan, noted that "the Federal Reserve and other bank supervisors are placing growing importance on a bank's risk management *process*. … Rather than evaluate a high percentage of a bank's loans and investment products by *reviewing individual transactions*, we will increasingly seek to ensure that the management process itself is sound, and that adequate policies and controls exist."[8]

b. *Legal and Regulatory Duties of Directors and Management at U.S. Banks and U.S. BHCs*

As part of the shift in bank supervisory focus from reviewing individual transactions to the risk management process, bank regulators assigned an important risk management role to the board of directors and senior management.[9] In this section, we will review the responsibilities for risk management that apply to senior management and boards of directors at U.S. banks and U.S. bank holding companies.

i. Risk Management Responsibilities of Directors and Management at U.S. Banks

The OCC regulates risk management at nationally chartered U.S. banks and requires senior management to establish a risk governance framework and the board of directors to oversee the design and implementation of the risk management framework. The OCC's risk management framework is based on a "three lines of defense" structure: first, so-called "front line units" for managing risk that generally consist of mid-level employees that are engaged in operating activities, such as lending and trading; second, independent risk management—those within the bank that have responsibility for identifying, monitoring or controlling risks but are not otherwise engaged in operating activities; and third, the bank's internal audit function, which is responsible for monitoring the bank's internal controls and independent risk management activities.[10]

In addition to the risk management framework, the boards of directors and management of banks are also assigned specific responsibilities for certain substantive areas of risk, including liquidity risk, market risk, operational risk and compliance risk.

---

[7] OCC, *Testimony of Eugene A. Ludwig, Comptroller of the Currency, Before the House Subcommittee on Financial Institutions and Consumer Credit* (Dec. 5, 1995), https://www.occ.treas.gov/news-issuances/congressional-testimony/1995/pub-test-1995-133-written.pdf.

[8] FEDERAL RESERVE SYSTEM, *Remarks by Chairman Alan Greenspan* (Nov. 18, 1996), https://www.federalreserve.gov/boarddocs/speeches/1996/19961118.htm.

[9] For a comprehensive collection of these requirements, see Annex A, U.S. Bank Regulatory Related Matters to be Addressed by the Board or Board Committee Pursuant to Statute, Regulation or Agency Guidance, The Clearing House (May 2016).

[10] See Thomas J. Curry, Comptroller of the Currency, Testimony before U.S. Senate Comm. on Banking, Hous., and Urban Affairs (June 6, 2012); Department of the Treasury, Office of the Comptroller of the Currency, OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations, 79 Fed. Reg. 54518 (Sep. 11, 2014) (the guidelines cover all banks with total consolidated assets equal to or greater than $50 billion, as well as certain banks that do not meet that asset threshold).

1. *Liquidity Risk*

The OCC expects the board of directors to establish a bank's tolerance for liquidity risk—the risk that the bank will have difficulty meeting its short-term financial obligations. The OCC also requires boards to approve policies related to liquidity risk management and review liquidity policies and procedures at least annually.[11] This approval extends to the assumptions used by management in measuring liquidity risk and cash flow projections.[12] The board and senior management must also review the assumptions used to assess the liquidity risk of assets that may be difficult to convert into cash (such as complex financial instruments and less-marketable loan portfolios), liabilities and off-balance sheet positions.[13]

2. *Market risks*

Directors and senior management are similarly subject to a host of bank-specific requirements with respect to market risks—the risk of losses on investments in capital markets. Guidance from the Federal Financial Institutions Examination Council (the "**FFIEC**") mandates that the board and senior management review at least annually the appropriateness of investment strategies, policies, procedures and limits.[14] More detailed guidance promulgated by the OCC directs bank directors to, among other things, review the bank's investment portfolio to confirm that its risk level remain acceptable,[15] determine that the bank uses financial derivatives only for approved purposes,[16] review the bank's key behavioral and pricing assumptions,[17] and approve and enforce policies to control foreign currency risks.[18]

3. *Operational risk*

Federal bank regulators have also imposed, through regulation and guidance, special requirements on directors and senior management related to a variety of operational risks—the risk of security breaches, service interruptions or financial losses caused by internal failures or external events. For instance, the Federal Reserve, OCC, and FDIC require bank boards to approve and monitor a program designed to detect, prevent and mitigate identity theft.[19] Under these same rules, the board or senior management must be involved in the development and administration of the program.[20] Senior management and the board of directors are similarly responsible for overseeing the development and

---

[11] Commercial Bank Examination Manual, Section 4020.1 (Federal Reserve Board); Detecting Red Flags in Board Reports – A Guide for Directors (OCC); Risk Management Manual of Examination Policies, Section 6.1 (FDIC); Interagency Policy Statement on Funding and Liquidity Risk Management (FFIEC).
[12] Risk Management Manual of Examination Policies, Section 6.1 (FDIC).
[13] Id.
[14] FFIEC Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities.
[15] Detecting Red Flags in Board Reports – A Guide for Directors (OCC).
[16] Id.
[17] Comptroller's Handbook, Interest Rate Risk (OCC).
[18] (Comptroller's Handbook, Investment Securities (OCC).
[19] 12 C.F.R. 222.90 (FRB-regulated banks); 12 C.F.R. 41.90(e)(1) (OCC-regulated banks); 12 C.F.R. 334.90 (FDIC-regulated banks).
[20] Id.

implementation of strategies related to the risk of intrusion into bank computer systems, including risk assessment and mitigation, as well as intrusion response policies and testing processes.[21]

4. Compliance risk

In addition to financial risks and operational risk, federal bank regulators have assigned responsibility to bank boards and senior management in connection with compliance programs. Regulators require a bank's board of directors to set an appropriate "culture of compliance" within the bank, and should review and approve key elements of a bank's compliance risk management program and oversight framework, including the compliance oversight roles and responsibilities of senior management within the bank.[22] Regulators also assign bank boards of directors responsibility for oversight of compliance programs for specific substantive areas of risk. For example, a bank's board of directors must approve and review annually a written program for compliance with the anti-money laundering requirements of the Bank Secrecy Act.[23] The board is also responsible for approving compliance programs to address the extension of credit to bank insiders or affiliates.[24]

5. Additional risk management responsibilities

The foregoing examples are illustrative of the risk management responsibilities imposed on bank boards and management by federal bank regulators. A 2016 review by The Clearing House Association identified hundreds of additional board obligations.[25] These responsibilities range from the development, implementation and approval of significant firm policies to reviewing ongoing business activity and personnel decisions.[26] They include the following responsibilities for the board of directors:

- Reviewing and approving the bank's capital plan annually.[27]
- Establishing and periodically reviewing policies and standards covering who the bank will lend to and at what price, as well as the bank's appraisal and evaluation program for certain types of loans (such as real estate or agricultural loans).[28]

---

[21] OCC 2000-14, Infrastructure Threats – Intrusion Risks (May 15, 2000).
[22] SR 08-08.
[23] 12 C.F.R 208.63(b) (FRB-regulated banks); 12 C.F.R. 21.21 (OCC-regulated banks); 12 C.F.R. 326.8 (FDIC-regulated banks).
[24] 12 C.F.R. 215.4(b) (FRB-regulated banks); 12 C.F.R. 31.2 (OCC-regulated banks); 12 C.F.R. 326.8 (12 C.F.R. 337.3).
[25] The Clearing House, The Role of the Board of Directors in Promoting Effective Governance and Safety and Soundness for Large U.S. Banking Organizations – Appendix A (2016).
[26] They also include relatively trivial responsibilities. Boards of national banks are, for example, required by regulation to review and schedule the bank's banking hours. 12 C.F.R. 7.3000. And the OCC has issued guidance mandating that boards formulate policies and procedures with respect to the purchase of commemorative coins. OCC, BC-58(Rev), Sup. 1 – Sale of Commemorative Coins (December 28, 1983).
[27] 12 C.F.R. § 225.8; FRB, Federal Reserve Supervisory Assessment of Capital Planning and Positions for LISCC Firms and Large and Complex Firms, SR letter 15-18 (December 18, 2015).
[28] 12 C.F.R. Part 208, Appendix C; 12 C.F.R. Part 34, Appendix A to Subpart D; 12 C.F.R. Part 365, Appendix A to Subpart A; FRB Commercial Bank Examination Manual, Section 2140.1.

- Reviewing and approving together with senior management adequate risk-tolerance limits across all established product lines.[29]
- Designating a security officer to develop and administer a security program for each banking office.[30]
- Ensuring that a third party to which a bank outsources collective investment fund management functions performs its functions in a safe and sound manner and in compliance with applicable laws and policy guidance.[31]
- Ensuring that the information provided by management in IT reports is accurate, timely, and sufficiently detailed.[32]

ii. Risk Management Responsibilities of Directors and Management at U.S. BHCs

The Federal Reserve Board (the "**Fed**") regulates bank holding companies ("**BHCs**") and mandates that the board "[e]nsure that the organization's internal audit, corporate compliance, and risk management and internal control functions are effective and independent, with demonstrated influence over business-line decision making."[33] Regulators expect the board to ensure that management information systems are sufficient to enable the board to oversee the institution's core business and critical operations.[34] The framework clarifies that boards are responsible for providing effective corporate governance with support from senior management, including: maintaining a corporate culture that emphasizes compliance with law and regulation, consumer protection, the avoidance of conflicts of interests and management of reputational and legal risks; and assigning senior managers with responsibility for ensuring that compensation arrangements are consistent with the bank's risk appetite.[35]

BHCs with $50 billion or more in consolidated assets must maintain an independent standalone risk committee that has the responsibility for risk management policies and oversight of the company's risk management framework.[36] The risk committee must meet at least quarterly, be chaired by an independent director and have at least one member that has risk management experience with large, complex firms.[37] The Fed also requires a BHC with consolidated assets of $50 billion or more to have a chief risk officer with

[29] Commercial Bank Examination Manual, Section 2030.1
[30] 12 C.F.R. §§ 21.2, 326.2, 208.61(b).
[31] OCC, Risk Management Elements: Collective Investment Funds and Outsourced Arrangements, Bulletin 2011-11 (March 29, 2011).
[32] OCC Director's Book, p. 39.
[33] Id at 5.
[34] Id.
[35] Id at 2.
[36] 12 C.F.R. §§ 252.21-252.22, 252.33. Dodd-Frank initially mandated that bank holding companies with $10 billion in consolidated assets have a risk committee; that threshold was raised to $50 billion by the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018. In the Federal Reserve's initial implementation of Regulation YY, the risk committee functions for BHCs with between $10 and $50 billion in consolidated assets could be performed by another committee of the board such as an audit or finance committee. See 79 Fed. Reg. 17,240, 17,250 (March 27, 2014).
[37] 12 C.F.R. §§ 252.21-252.22, § 252.33.

experience with risk exposures of large complex financial firms. The chief risk officer must report directly both to the risk committee of the board and the CEO.[38]

The specific responsibilities applicable to directors and senior management of BHCs are similar to the risk management obligations imposed on directors and senior management of banks with regards to their prescriptiveness for the BHC's financial activities—such as credit risk, liquidity risk, and market risk—as well as operational and compliance risks. For example, the board of a BHC is required to approve annually the BHC's liquidity risk tolerance and periodically review the liquidity risk management strategies, policies and procedures established by senior management.

However, the risk management requirements applicable to directors and senior management of BHCs also reflect the unique risks associated with BHCs—in particular risks arising from the activities of nonbank subsidiaries. For example, the board of a BHC with a nonbank subsidiary that takes positions in financial contracts must approve written policies, procedures and risk limits to ensure the safety and soundness of those activities; establish internal controls and internal audit programs to monitor such activities; and on a monthly basis, either the board, a duly authorized board committee, or auditors must review financial contract positions to ensure compliance with those policies and risk limits.[39]

c. Supervision of Bank Governance and Risk Management at U.S. Banks and U.S. BHCs

i. Supervision at Banks

OCC bank supervisors oversee risk management by the board of directors and senior management at national banks through their examination process.[40] The examination process produces a rating for each bank, using the so-called "CAMELS" rating system. The rating formula includes a component for the capability of the board of directors and management to identify, measure, monitor, and control the risks of the bank's activities and to ensure that the bank has a safe, sound, and efficient operation that is in compliance with applicable laws and regulations.[41] This component is generally regarded as the most important element in a bank's CAMELS rating.[42]

Bank examiners evaluate whether the board and senior management:

- have a clear understanding and working knowledge of the risks inherent in the bank's activities;
- have reviewed and approved policies to limit risks inherent in the bank's significant activities or products and risk-exposure limits;
- make appropriate efforts to remain informed about these risks as financial markets, risk management practices, and the bank's activities evolve;

---

[38] See id.
[39] 12 C.F.R. 225.142.
[40] See 12 U.S.C. § 1820(d); Thomas J. Curry, Comptroller of the Currency, Testimony before U.S. Senate Comm. on Banking, Hous., and Urban Affairs, 17-19 (June 6, 2012)
[41] Commercial Bank Examination Manual at 1-2.
[42] Comptroller's Handbook, Bank Supervision Process, 94 (2007).

- are sufficiently familiar with and use adequate record-keeping and reporting systems to measure and monitor the major sources of risk to the organization. [43]

Supervisory findings are reported to the bank's board of directors or a committee of the board who, in turn, must direct senior management to take corrective action and provide management with appropriate oversight.[44] The banking organization is required to commit to a time frame for corrective action. If corrective action is not taken then the OCC may take a public enforcement action against a bank for risk management or compliance problems.

ii. Supervision at Bank Holding Companies

The Fed examines the board and senior management of BHCs for compliance with their risk management obligations. The supervisory rating system for BHCs is similar to the CAMELS rating system, and also includes a component for risk management.[45] According to the Fed, "[o]ne of the primary areas of focus for consolidated supervision of large complex bank holding companies is the adequacy of governance provided by the board and senior management" for risk management.[46] The failure to maintain a satisfactory rating on the BHC supervisory rating system can have significant regulatory consequences. A BHC that does not have a satisfactory rating, for example, may become subject to restrictions, including limitations on engaging in new financial activities or acquiring new investments.[47]

In Box A on the next page we provide an example of a recent enforcement action taken by bank supervisors against Citigroup (a bank holding company) and Citibank (its bank subsidiary). In October 2020, the federal banking regulators ordered Citigroup and Citibank to fix their risk-management systems, citing "significant ongoing deficiencies." This example further demonstrates the prescriptive and extensive risk management requirements imposed on bank boards and senior management.[48]

[43] Commercial Bank Examination Manual, § 1000.1 at 4.7.
[44] See, e.g., Bank Holding Company Supervision Manual, § 5000.0.9.3.
[45] Bank Holding Company Supervision Manual §§ 1050.1.3.1.1, 4070.0.1.
[46] Id.
[47] The Gramm-Leach-Bliley Act allows a BHC to qualify for "financial holding company" status, which authorizes a BHC and its affiliates to engage in a broader range of financial and investment, if the BHC and each of its depository subsidiaries remains both "well capitalized" and "well managed". 12 U.S.C. § 1841(0)(1) & (9); 12 U.S.C. § 1843(k)(l) & (e)(l) & (2) (2014). A BHC or depository subsidiary that does not have a satisfactory rating will not be deemed to be "well managed" and must enter into an agreement with the Federal Reserve Board, prescribing the actions that the BHC will take to correct the areas of noncompliance. The BHC may also become subject to restrictions, including limitations on engaging in new financial activities or acquiring new financial investments. 12 C.F.R. § 225.83(c) (2016).
[48] See, Office of the Comptroller of the Currency, In the Matter of: Citibank, N.A., AA-EC-2020-64 (Oct. 7, 2020); Board of Governors of the Federal Reserve System, In the Matter of Citigroup Inc., No. 20-019-B-HC (Oct. 7, 2020); David Benoit, *Regulators Fine Citigroup $400 Million Over 'Serious Ongoing Deficiencies'*, Wall Street Journal (Oct. 7, 2020), https://www.wsj.com/articles/federal-reserve-finds-serious-ongoing-deficiencies-at-citigroup-11602103099.

The Citi Consent Orders **Box A**

Risk management deficiencies described in the Citi orders include, among others, a general failure to establish an effective risk governance framework and to adequately identify, measure, monitor and control risks, as well as more specific failures, such as inadequate reporting to the board of directors on the status of data quality and progress in fixing previously identified deficiencies. Regulators also determined that the bank's board and senior management oversight failed to adequately correct deficiencies in risk management, internal controls, and data governance.

The OCC consent order—which applies to Citi's bank subsidiary—imposes a long list of new obligations on the board and senior management. These requirements relate primarily to the development and implementation of plans to address deficiencies in data governance (processes to ensure that data is accurate, consistent, timely and complete), enterprise risk management (strategy to manage risk across all business lines) and internal controls (processes to ensure that risk limits are adhered to).

The consent order requires that the data governance plan include processes to ensure that the board is notified of any significant departure from the requirements of the revised data governance program. The board must either approve the departure or ensure that it is timely remediated.

The consent order also requires that the enterprise risk management plan provide for quantitative and qualitative reports to the board on whether risks are consistent with the board-approved risk appetite, as well as reporting on any significant exceptions to the risk management programs. The bank is also required to improve reporting to the board and senior management to capture significant exposures and include relevant analysis on current and emerging risks.

The board is further required to appoint a compliance committee to oversee and report to the board on compliance with the consent order. More generally, the board has ultimate responsibility for ensuring the timely adoption and implementation of all corrective actions required under the consent order, and to ensure that the bank has sufficient capacity to implement and adhere to the orders.

The consent order issued by the Federal Reserve—which applies to Citigroup, Citi's bank holding company—imposes similar requirements on the board of the BHC. Citigroup's board is required to oversee its compliance with matters identified in the consent order, including: holding senior management accountable for remediating deficiencies identified by regulators; ensuring that senior management improves and maintains effect enterprise-wide risk management; ensuring that incentive compensation for senior management is consistent with risk management objectives; and ensuring effective reporting to the board to facilitate its oversight.

d. Policy Issues with the Current Requirements Applicable to Directors and Management

Critics have argued that the regulatory and supervisory responsibilities imposed on bank directors are too burdensome,[49] as regulators have been too quick to conclude that every new issue of regulatory or supervisory concern requires additional board attention, resulting in an overload on board time, attention and resources. Moreover, in many instances regulatory and supervisory requirements have imposed management-like functions on board members. For example, supervisory guidance indicates that bank boards are expected to review the terms for specific categories of loans, such as agricultural loans, regardless of whether that type of loans represents a significant portion of the bank's loan portfolio.[50] That can draw board members' limited attention away from their core responsibilities as directors, which include guiding the bank's strategic objectives and plans, monitoring its financial performance and condition, selecting and evaluating the performance of the CEO and other senior executives, protecting the independence of the bank's risk management and internal audit functions, and dictating and reinforcing the bank's organizational values and culture.[51]

Bank regulators have acknowledged that the existing prescriptive requirements can impose an excessive burden on directors. In a 2014 speech, then-Federal Reserve Board Governor Dan Tarullo noted that "it has perhaps become a little too reflexive a reaction on the part of regulators to jump from the observation that a regulation is important to the conclusion that the board must certify compliance through its own processes." He went further saying that "[w]e should probably be somewhat more selective in creating the regulatory checklist for board compliance and regular consideration."[52]

---

[49] *See, e.g.*, Paul L. Lee, *Directors' Duty to Monitor: Experience in the Banking Sector – Part I*, THE BANKING LAW JOURNAL (Sept. 2016); Paul L. Lee, *Directors' Duty to Monitor: Experience in the Banking Sector – Part II*, THE BANKING LAW JOURNAL (Oct. 2016).

[50] FRB Commercial Bank Examination Manual, Section 2140.1. Other supervisory guidance suggests that boards are expected to engage in a detailed review of certain bank activities: OCC guidance, for example, states that examiners should determine whether the board has reviewed and approved all loans that are charged off. Comptroller's Handbook: Allowance for Loan and Lease Losses, p. 30.

[51] See 82 Fed. Reg. 37219 (Aug. 9, 2017); The Clearing House, The Role of the Board of Directors in Promoting Effective Governance and Safety and Soundness for Large U.S. Banking Organizations (May 2016).

[52] Daniel K. Tarullo, Corporate Governance and Prudential Regulation, Speech at the Association of American Law Schools 2014 Midyear Meeting 6 (June 9, 2014).

Part II: Corporate Governance and Risk Management at Technology Companies

In Part II, we review risk management and corporate governance regulation and practices at large technology companies. Unlike banking institutions, there are no technology industry-specific legal or regulatory requirements that apply to risk management and corporate governance at technology companies. Instead, the relevant legal and regulatory structure for risk management and corporate governance at technology companies is that which applies to corporations and public companies. We therefore summarize state and federal regulation of risk management and corporate governance at public companies. We then describe voluntary industry standards for risk management and corporate governance, on the basis of which independent auditors assess many technology companies, and review risk management practices at technology companies. We conclude Part II by summarizing the additional regulatory requirements for risk management that apply to technology companies that provide services to banking firms and compare those regulatory requirements with the additional regulatory requirements for risk management that apply to technology companies that provide services to other industries, including health care, educational institutions and the federal government.

a. Legal and Regulatory Requirements for Corporate Governance and Risk Management

State corporate law, federal securities laws and regulations, and stock exchange listing standards impose governance and risk management requirements on a technology company's board and senior management.[53] These include requirements relating to financial disclosure, the auditing process, internal controls over financial reporting, and the composition of the board and its committees, among others.[54]

Under state corporate law, corporate directors are responsible for supervising the affairs of the corporation.[55] In this capacity, directors owe fiduciary duties to the corporation and its shareholders. These fiduciary duties include the duty of care and the duty of loyalty.[56] The duty of care requires directors to exercise reasonable care, prudence and diligence in the management of the corporation. The duty of loyalty requires directors to act in the best interests of the corporation and its shareholders, rather than

---

[53] Holly J Gregory, Rebecca Grapsas and Claire H Holland of Sidley Austin LLP, *Corporate governance and directors' duties in the United States: overview*, THOMPSON REUTERS: PRACTICAL LAW (May 1, 2020), https://uk.practicallaw.thomsonreuters.com/w-011-8693?transitionType=Default&contextData=(sc.Default)&firstPage=true#co_pageContainer.

[54] *See, e.g.*, PERKINS COIE, *Public Company Handbook: Chapter 8: Governance on the "Big Board": NYSE Listing Standards* (last accessed June 22, 2021), https://www.perkinscoie.com/en/chapter-8-governance-on-the-big-board-nyse-listing-standards.html.

[55] Holly J Gregory, Rebecca Grapsas and Claire H Holland of Sidley Austin LLP, *Corporate governance and directors' duties in the United States: overview*, THOMPSON REUTERS: PRACTICAL LAW (May 1, 2020), https://uk.practicallaw.thomsonreuters.com/w-011-8693?transitionType=Default&contextData=(sc.Default)&firstPage=true#co_pageContainer.

[56] Peter A. Atkins Marc S. Gerber Edward B. Micheletti Robert S. Saunders, *Directors' Fiduciary Duties: Back to Delaware Law Basics*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP (Feb. 19, 2020), https://www.skadden.com/insights/publications/2020/02/directors-fiduciary-duties.

their own self-interest. The susceptibility of corporate directors to potential liability for breaching their fiduciary duties is a critical aspect of corporate governance in the United States.

Directors' duty of care includes the obligation to be engaged in the oversight of corporate risks. Delaware courts have taken the lead in formulating the legal standard for directors' risk oversight responsibilities. In *Caremark*,[57] Delaware's Court of Chancery held that directors will only be liable for a failure of board oversight if they exhibit (1) a sustained or systemic failure to exercise oversight, such as a failure to assure the existence of any reporting system; and (2) a conscious failure to monitor or oversee the operations of the corporation based on established reporting systems.[58]

Public companies are subject to additional regulatory requirements that apply to corporate governance and risk management. Under the Sarbanes Oxley Act of 2002, for example, public companies are required to have an audit committee of the board, composed entirely of independent directors, that is directly responsible for the appointment, compensation, and oversight of any accounting firm employed by that company for the purpose of preparing or issuing an audit report.[59] Likewise, the SEC requires companies to disclose in their annual reports: "factors that make an investment in the registrant or offering speculative or risky"; the board's leadership structure and its role in risk oversight; and how their compensation policies and practices, including those of their non-executive officers, relate to risk management and risk-taking incentives.[60]

b. Voluntary Standards for Risk Management at Technology Companies

Many technology companies, along with other corporations, adhere to voluntary industry standards for risk management and corporate governance. However, these frameworks generally do not apply specific risk management responsibilities to the board of directors. Instead, risk management goals and responsibilities are principles-based and applied to senior management.

For example, large technology companies[61] generally adhere to the Committee of Sponsoring Organizations of the Treadway Commission ("**COSO**") framework for enterprise risk management and internal control. COSO was established by an independent private-sector organization jointly sponsored by the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, The Institute of Internal Auditors, and the Institute of Management Accountants (formerly the National Association of Accountants). While COSO covers governance processes, it does so at a relatively high level of generality that gives directors and senior management flexibility to decide on appropriate mechanisms for managing

---

[57] *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del.Ch. 1997).
[58] See id.; *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006).
[59] *Sarbanes-Oxley Act of 2002* § 301, PUB. LAW NO. 107-204 (2002).
[60] Regulation S-K, §§ 229.105, 401, 402 & 407.
[61] GOOGLE CLOUD, *Compliance offerings* (last accessed June 22, 2021), https://cloud.google.com/security/compliance/offerings; AMAZON WEB SERVICES, *AWS Compliance Programs* (last accessed June 22, 2021), https://aws.amazon.com/compliance/programs/; MICROSOFT, *Microsoft compliance offerings* (last accessed June 22, 2021), https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide.

particular risks. The COSO framework for enterprise risk management, for example, describes five different components of an effective risk management process—control environment, risk assessment, information and communication, monitoring activities, and control activities.[62] Each of these components involve corporate governance and culture. But the COSO framework recognizes that these components "can be applied in different ways for different organizations regardless of size, type, or sector."[63]

Large, sophisticated technology companies[64] also aim to comply with widely recognized industry standards for risk management and controls. Several of these standards have been developed by the International Organization for Standardization ("**ISO**"), an independent, international standard-setting body comprising representatives of various national standards organizations.[65] ISO standards set forth requirements and best practices both for risk management and corporate governance.[66] Large, sophisticated technology companies—like Google, Amazon and Microsoft—typically have their compliance with these and other standards, such as the Trust Services Criteria for System and Organization Controls ("**SOC**") reports, certified by independent auditors.[67]

Unlike banking regulations, ISO standards do not impose specific requirements on boards and senior management. Rather they set detailed substantive goals and describe adaptable processes for meeting those goals. For example, ISO 27001, which covers the implementation of information security controls, requires organizations to, among other things, define which information needs to be protected and identify threats to that information; to establish an information security policy and objectives; to develop a plan for responding to and addressing risks; and to conduct regular internal audits.[68] It also outlines controls, such as access controls, associated with various risks, that companies can implement based on their risk exposure and appetite.[69] ISO 27001 does mandate a role for senior management, but offers significant flexibility in how senior management

---

[62] COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, *COSO Internal Control – Integrated Framwork: An Implementation Guide for the Healthcare Provider Industry* (Jan. 2019), https://www.coso.org/Documents/COSO-CROWE-COSO-Internal-Control-Integrated-Framework.pdf.

[63] COSO, Enterprise Risk Management – Integrating with Strategy and Performance, Executive Summary, p. 7 (2017).

[64] GOOGLE CLOUD, *Compliance offerings* (last accessed June 22, 2021), https://cloud.google.com/security/compliance/offerings; AMAZON WEB SERVICES, *AWS Compliance Programs* (last accessed June 22, 2021), https://aws.amazon.com/compliance/programs/; MICROSOFT, *Microsoft compliance offerings* (last accessed June 22, 2021), https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide.

[65] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, *About Us* (2021), https://www.iso.org/about-us.html.

[66] See, e.g., INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, *ISO/IEC 38500:2008 - Corporate governance of information technology* (2008), https://www.iso.org/standard/51639.html; INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, *ISO 31000 – Risk Management* (2021), https://www.iso.org/iso-31000-risk-management.html.

[67] GOOGLE CLOUD, *Compliance offerings* (last accessed June 22, 2021), https://cloud.google.com/security/compliance/offerings; AMAZON WEB SERVICES, *AWS Compliance Programs* (last accessed June 22, 2021), https://aws.amazon.com/compliance/programs/; MICROSOFT, *Microsoft compliance offerings* (last accessed June 22, 2021), https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide.

[68] ISO 27001, clauses 4.3, 5.2, 6.12, 6.2, 9.2.

[69] Id., Annex A, clause A.9.1.1.

meets those requirements. For example, the standard requires a periodic management review, but no specific member of management is required to participate—as long as the roles, responsibilities and authorities of participants are well defined.[70]

c. Risk Management Practices at Technology Companies [71]

Technology companies have broad, company-wide standards for addressing risks arising from, for example, human access to data, but provide flexibility to individual divisions and teams to determine how to apply those standards and practice. As a result, risk management decisions and the design of risk management processes at technology companies are distributed throughout the decision-making hierarchy, rather than concentrated primarily at the level of senior management or the board of directors.[72] For example, decisions about risk management are often made at the level of an entire business unit, at the level of a division, or even at the level of an individual team.

In addition, the largest, most sophisticated technology companies increasingly employ standardized, automated tests to ensure that individual products and services meet broad company-wide standards and design processes to develop new products and services with security and controls built in.[73] The decentralization of risk management by modern technology companies enables greater agility: individual teams do not need to go through as many organizational hurdles before developing a product or, more importantly, addressing vulnerabilities that arise in real time.

d. Existing Application of the Bank Framework to Technology Services Providers

Technology companies that provide services to banking organizations are subject to additional governance and risk management requirements.

Federal bank regulators have statutory authority to supervise third parties that provide services to regulated banks, including technology service providers ("**TSPs**").[74] Bank regulators have issued guidance for banks that outsource technology services to TSPs, and the FFIEC, the interagency body that comprises the five federal banking regulators, has issued guidance on how agencies should supervise TSPs, most recently updated in 2012.[75] In 2020, the FFIEC released a separate statement on the use of cloud computing services in the financial sector, which highlights examples of risk management practices for financial institutions to use cloud computing services in a safe and sound manner.[76]

As in the case of banks, boards of directors at TSPs are directed by the FFIEC guidance to play an important role in risk management. Directors must provide clear guidance regarding acceptable risk exposure levels at the TSP and ensure that appropriate policies, procedures, and practices have been established.[77] Bank examiners

---

[70] Id., clause 9.3.
[71] Discussions with major technology companies and cloud service providers.
[72] Discussions with major technology companies and cloud service providers.
[73] Discussions with major technology companies and cloud service providers.
[74] 12 U.S.C. §§ 1464(d)(7), 1867(c)(1).
[75] FFIEC, Supervision of Technology Providers (Oct. 2012).
[76] FFIEC, *Joint Statement: Security in a Cloud Computing Environment* (2020), https://www.ffiec.gov/press/PDF/FFIEC_Cloud_Computing_Statement.pdf.
[77] Id at A-6.

are also directed to consider the quality of oversight by TSP directors.[78] The FFIEC guidance for bank supervision of TSPs includes an assessment of risk management by a TSP.[79] If a TSP has weak risk management controls that require corrective action, then the banks that it serves are directed to take remedial action.[80] TSPs are to be evaluated by bank examiners on multiple factors, such as:

- the level and quality of oversight and support of the IT activities by the TSP's board of directors and management;
- the ability of a TSP's management to plan for and initiate new activities or products in response to information needs and to address risks that may arise from changing business conditions; and
- the ability of the TSP's management to identify, measure, monitor, and control risks and to address emerging IT needs and solutions.

Despite the existence of the FFIEC guidance, a 2017 report commissioned by the Federal Reserve's Office of the Inspector General found significant gaps in the oversight of TSPs by bank regulators.[81] Most importantly, the report found that banks frequently do not notify regulators of the TSPs that they use.[82] As a result, bank examiners do not engage in significant oversight of some TSPs. Moreover, examiners lack the institutional capacity or expertise to engage in oversight noting that the Fed lacked the ability to attract and retain supervisors with the necessary knowledge and ability to assess and address cybersecurity challenges.[83] It is worth noting that four years have elapsed since this report was released, and given growing regulatory and private sector attention to technology risk management practices, financial institutions perform greater due diligence on TSPs today than they did previously.

e. Requirements Applicable to Technology Companies that Serve Other Industries

Technology companies that serve other industries are also subject to additional risk management and corporate governance requirements. However, none of these additional regimes imposes structural requirements on boards and senior management that are expected from technology companies that provide services to banking organizations.

For instance, technology companies that provide services to healthcare companies may become subject to regulations under the Health Insurance Portability and Accountability Act ("**HIPAA**"), which establishes requirements for the use, disclosure, and

---

[78] 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 (Oct. 2012), https://ithandbook.ffiec.gov/media/153533/10-10-12_-_administrative_guidelines_sup_of_tsps.pdf.
[79] FFIEC, Supervision of Technology Providers (Oct. 2012).
[80] Id at 9.
[81] OIG, Board of Governors of the Federal Reserve System, The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing (2017).
[82] Id at 7.
[83] Id at 12.

safeguarding of individually identifiable health information.[84] These regulations require that healthcare companies—including doctors' offices, hospitals and health insurers—enter into contracts with technology service providers ("**TSPs**") to ensure that protected health information is handled in a manner that complies with HIPAA's security and privacy provisions. Likewise, educational institutions that are subject to the Family Educational Rights and Privacy Act ("**FERPA**"), which protects the privacy of students' education records, must ensure that technology companies that they do business with manage student records and information appropriately.[85] Neither of these regulatory regimes, however, imposes a particular governance structure on technology companies or specific duties on technology company directors or senior management for managing the security and privacy risks in a manner necessary to ensure compliance with HIPAA or FERPA.

Cloud services providers that do business with federal government agencies must have the security of their services validated under the Federal Risk and Authorization Management Program ("**FedRAMP**").[86] FedRAMP employs standards and control models established by the National Institute of Standards and Technology ("**NIST**") for the authorization and ongoing cybersecurity of cloud services.[87] NIST, a non-regulatory agency that is part of the Department of Commerce, develops standards to promote innovation and economic competitiveness. Among other things, NIST has published standards and guidelines to help federal agencies comply with information security requirements. These guidelines include a comprehensive catalog of state-of-the-art security controls for information systems, which can be applied to specific business functions, operation environments, and technologies.[88] The FedRAMP standards, which leverage NIST standards, set out substantive security and control requirements, but they do not impose responsibilities on directors or senior management. As a result, they are adaptable to a variety of different technology service providers of different size and structure.

---

[84] *Health Insurance Portability and Accountability Act of 1996*, PUB. LAW NO. 104-191 (Aug. 21, 1996).
[85] CONGRESSIONAL RESEARCH SERVICE, *The Family Educational Rights and Privacy Act (FERPA): Legal Issues* (May 24, 2021), https://crsreports.congress.gov/product/pdf/R/R46799.
[86] FedRAMP was established, in part, to standardize how different government agencies applied the Federal Information Security Management Act of 2002 to their use of cloud computing.
[87] These standards include Recommended Security Controls for Federal Information Systems, NIST SP 800-53, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST SP 800-37, and Guidelines on Security and Privacy in Public Cloud Computing, NIST 800-144.
[88] NIST SP 800-53.

Part III: Analysis and Recommendations

We now compare the regulation of risk management and corporate governance at U.S. banking institutions with technology companies. In doing so, we consider the key differences in risk faced by banking institutions as compared to technology companies. We conclude that a decentralized principles-based approach to risk management regulation is best suited for cloud service providers to banking institutions.

We recommend that that the FFIEC and federal banking agencies should acknowledge the utility of the principles-based approach by updating the relevant guidance and policy statements as it applies to cloud service providers. For instance, the FFIEC should revise its "Supervision of Technology Service Providers" Booklet,[89] which offers guidance to examiners and financial institutions,[90] to articulate a principles-based approach to supervision alongside the existing risk-based guidance. The FFIEC should also specify these principles in its "Management" Booklet, which addresses board oversight of information technology risks.[91] Likewise, the Fed, FDIC, and OCC should amend their joint "Implementation of Interagency Programs for the Supervision of Technology Service Providers,"[92] which describe the process that the agencies follow to implement the interagency supervisory programs,[93] to similar effect.

As described throughout Part I, the regulatory risk management framework for banks is highly prescriptive, imposing specific and extensive procedural requirements and expectations on boards of directors and senior management. These requirements and expectations envision a top-down approach to risk management, directed by boards and senior management. These frameworks differ from risk management frameworks at technology companies, which as we've described in Part II, require technology companies to satisfy broad risk management goals or address particular substantive risks, but generally do not impose specific procedural requirements or expectations on particular elements of their organizational hierarchy, such as boards or senior management.

The regulation and supervision of cloud service providers to banking institutions is increasingly important, as banking institutions transition their data to cloud service providers. Ultimately, banking regulators and supervisors with authority over technology service providers to U.S. banking institutions will have to determine between two general approaches to risk management regulation. Option one would be to adopt a more centralized and prescriptive approach to the regulation of risk management by cloud service providers, similar to the existing approach for banking institutions. Option two would be to adopt a more decentralized and principles-based approach to the regulation

---

[89] FFIEC, *Supervision of Technology Service Providers* (Oct. 2012), https://ithandbook.ffiec.gov/media/274876/ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf.

[90] FFIEC, *Press Release: Financial Regulators Release Guidance for the Supervision of Technology Service Providers* (Oct. 31, 2012), https://www.ffiec.gov/press/pr103112.htm.

[91] FFIEC, *Information Technology Examination Handbook: Management Booklet*, Section I.A.1 (last accessed June 22, 2021), https://ithandbook.ffiec.gov/it-booklets/management.aspx.

[92] Fed, FDIC, and OCC, *Federal Regulatory Agencies' Administrative Guidelines: Implementation of Interagency Programs for the Supervision of Technology Service Providers* (Oct. 2012), https://ithandbook.ffiec.gov/media/153533/10-10-12_-_administrative_guidelines_sup_of_tsps.pdf.

[93] FFIEC, *Press Release: Financial Regulators Release Guidance for the Supervision of Technology Service Providers* (Oct. 31, 2012), https://www.ffiec.gov/press/pr103112.htm.

of risk management by cloud service providers, similar to the existing approach for technology companies.

We now assess the policy rationale behind each approach to risk management regulation to inform which is best suited for cloud service providers to U.S. banking institutions. We note that our analysis applies more broadly to technology service providers to U.S. banking institutions, but we focus on cloud service providers due to the significant increase in uptake of cloud services by U.S. banking institutions. Our analysis is also informed by field interviews with leading cloud service providers.[94]

a. Bank Failures Pose Systemic Risk, Technology Company Failures Do Not

A first order issue is that the regulatory and supervisory framework for U.S. banking institutions is more extensive and prescriptive than the regulatory regime for risk management at technology companies because the widespread failure of banks could pose systemic risk to the U.S. financial system.[95] Banks have access to government support to mitigate these risks, including deposit insurance from the Federal Deposit Insurance Corporation and the ability to borrow from the Federal Reserve as the lender of last resort.[96] However, deposit insurance and lender of last resort create moral hazard thereby justifying more intrusive regulation of governance and risk management at U.S. banking institutions.

On the other hand, the financial collapse of a major technology company would not pose systemic risk, because like airlines they could continue to operate in bankruptcy. For example, the financial collapse of a cloud service provider to banking institutions would not pose systemic risk because it could continue to operate in bankruptcy, therefore there is not a need for a highly prescriptive approach to risk management regulation at cloud service providers as compared to U.S. banking institutions on the basis of systemic risk.

b. Bank Risks Can be More Readily Aggregated Than Technology Company Risks

Banks face risks, such as credit or liquidity risks, that often aggregate from the activities of disparate legal entities, such branches and desks, to an entity-wide basis. As a result, those risks can be measured in a way that provides a high-level picture of a bank's aggregate credit or liquidity exposure.[97] That broad picture can facilitate risk management decisions by directors and senior management, who sit at the top of the institutional hierarchy.

---

[94] Discussions with major technology companies and cloud service providers.

[95] *See* Hal S. Scott, *Connectedness and Contagion: Protecting the Financial System from Panics*, MIT PRESS (May 2016).

[96] *See* Hal S. Scott, *Connectedness and Contagion: Protecting the Financial System from Panics*, MIT PRESS (May 2016).

[97] *See, e.g.*, Robert A. Jarrow and Stuart M. Turnbull, *The intersection of market and credit risk*, 24 JOURNAL OF BANKING AND FINANCE 271 (2000); Joshua Rosenberg and Til Schuermann, *A general approach to integrated risk management with skewed, fat-tailed risks*, 79(3) JOURNAL OF FINANCIAL ECONOMICS 569 (2006).

On the other hand, the risks faced by technology companies, including cloud service providers, generally do not lend themselves to aggregation in the same way.[98] Unlike banks, where the credit exposure of one desk can amplify, or mitigate, the credit exposure of another desk, technology-related risks—such as cybersecurity risks—posed by one product or service are typically distinct, and do not necessarily affect risks posed by another.[99] As a result, senior management of technology companies, including cloud service providers, use standardized processes to oversee distinct and specific product-related security and operational issues, including reviewing risk management decisions made by lower-level teams; boards generally advise on strategic direction rather than tactical review of product-related issues that do not lend themselves to the same kind of aggregation that is possible with financial risks.[100]

c. Tailoring the Regulation of Risk Management to Technology Companies

Applying the top-down bank risk management framework to cloud service providers or other technology services providers to banking institutions would need to be done in a manner that does not limit the flexibility of lower-level employees to respond quickly to risk management concerns. For example, as described in Part II, resolving a new security vulnerability does not typically require sign-off from senior management or the board of directors at technology companies.[101] Requiring such approval by the board of directors of a technology company, or otherwise imposing prescriptive process-oriented requirements to technology companies, would reduce their ability to respond quickly to security vulnerabilities. Furthermore, imposing risk management responsibilities on boards of directors and senior management would also need to be designed in a manner to avoid slowing the pace of innovation at technology companies. Imposing the banking approach to corporate governance and risk management to technology companies would also face additional practical hurdles, such as a potential lack of risk management expertise on the board of directors at technology companies.

In conclusion, we believe that a decentralized and principles-based approach to the regulation of risk management and corporate governance at cloud service providers and other technology services providers to banking institutions would likely be better-suited to address the risks faced by such technology companies, rather than a centralized and prescriptive approach to risk management regulation and supervision. Consequently, we recommend that federal banking regulators explicitly acknowledge the utility of the principles-based approach by updating their relevant guidance and policy statements.

---

[98] *See* Shraddha A. Pandya, *Cyber-risk aggregation across multi-actor organizations* (Aug. 24, 2017).
[99] See id.
[100] Discussions with major technology companies and cloud service providers.
[101] Regine Slagmulder and Bart Devoldere, Tr*ansforming under deep uncertainty: A strategic perspective on risk management*, 61(5) BUSINESS HORIZONS (July 2018).

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