protiviti®
Global Business Consulting

Identifying and managing the critical risks of third-party providers

"Outsourcing and other third-party relationships can bring multiple benefits to FIs, including: enhanced operational resilience; faster and more tailored financial products and services; cost reduction; greater innovation; and improved internal processes. However, outsourcing and third-party relationships can give rise to new or different risks to FIs and potentially to financial stability that need to be adequately managed."[1]

Prior to the 1990s, a reference to third-party risk management (TPRM) in a financial institution (FI) meant you were talking about oversight of outsourced technology providers — whether they were financially viable, reputable, reliable, and had adequate privacy and information security safeguards. Cybersecurity controls weren't part of these earlier discussions, since the word *cybersecurity* didn't even enter the English lexicon until 1989. Decisions to engage outsourced technology providers were often broadly distributed throughout a FI, and attempts to compile a complete listing of an institution's third-party technology providers were often futile.

Much has changed in three decades. Today, it is commonly understood that third-party providers to FIs include a broad array of technology and other service providers (although the lack of a universal definition does complicate compliance efforts) and that identifying and managing the risks of these providers require a coordinated and continuous effort. And while long-recognised risks remain important, many other risks, such as concentration risk, also require attention. Given the risk landscape and the realisation that large financial institutions may have close to 50,000 suppliers,[2] it is little wonder that TPRM is a global industry and regulatory priority.

[1] *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Discussion Paper*, Financial Stability Board, November 9, 2020, https://www.fsb.org/wp-content/uploads/P091120.pdf.

[2] "Managing When Vendor and Supplier Risk Becomes Your Own," by Hamid Samandari, John Walsh and Emily Yueh, McKinsey & Company, July 1, 2013, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/managing-when-vendor-and-supplier-risk-becomes-your-own.

The "newer" risks of third-party service providers

With financial services companies reporting 703 cyber attack attempts per week in Q4 2021, a 53% increase over the prior year,[3] and the associated costs of remediating a cyber attack, including restoring customer trust, FIs don't need to be reminded of the importance of managing the infosecurity and privacy risks of their third-party relationships. They also don't need to be reminded to consider the financial wherewithal and reputation of the providers they select. But today's environment, with the continued advancement and reliance on technology, a tangled global framework of data privacy and data handling requirements, the lessons learned during the pandemic, and even the state of global politics, has heightened some existing risks and introduced new ones, including the following:

Common Risks of Third-Party Providers

- Privacy and infosecurity
- Data localisation
- Operational resilience
- Delivery
- Substitutability
- Compliance
- Legal/contractual
- ESG
- Geopolitical risk
- Strategic
- Solvency
- Concentration
- Reputation customer impact
- *N*th-party risk management
- Intragroup risk

- **Data localisation —** stringent data localisation rules in some jurisdictions that limit or prohibit the flow of nonpublic data across borders.[4]
- **Operational resilience —** ability of third-party providers to operate under adverse conditions, a risk that was brought to the fore with the pandemic and the stark realisation that some providers would not be able to pivot easily to remote work.
- **Delivery —** unproven sustainability of new market entrants (e.g. fintechs) to provide contracted services.
- **Substitutability —** ease of providing a replacement service provider in a cost-efficient and timely manner, especially in less developed markets, but also in high-tech markets where the number of providers may be limited.
- **ESG —** alignment of third-party environmental, social and governance (ESG) commitments and practices with those of the user of the services.
- **Geopolitical —** possibility that a third-party provider's ability to provide services is interrupted or precluded because of geopolitical tensions.

[3] "Spike in Destructive Attacks, Ransomware Boosts Banks' Cybersecurity Spending in 2022," by Sherry Fairchok, Insider Intelligence, May 3, 2002, https://www.insiderintelligence.com/content/spike-destructive-attacks-ransomware-boosts-banks-cybersecurity-spending-2022.

[4] Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships: Overview of Responses to the Public Consultation, Financial Stability Board, June 14, 2021, https://www.fsb.org/wp-content/uploads/P140621.pdf.

- **Concentration —** limited number of available providers (e.g. with respect to cloud services).
- ***N*th-party risk —** possibility that a downstream provider of a third-party provider may expose an institution to undue risk, including supply chain risk, and/or may jeopardise operational resilience.

There is one basic third-party risk that seems to need continual reinforcement — intragroup risk: the exposures that result when services are provided by a related entity. What happens too often is that FIs minimise the risks of intragroup providers because they are related entities. Some flexibility should be afforded to how some intragroup risks are evaluated (e.g. solvency of an intragroup provider would generally not require the same degree of scrutiny as an independent third party). However, experience has proven that other risks (e.g. delivery and compliance) are material for intragroup providers, particularly though not exclusively when services are provided cross-border, and, as such, these risks need to be evaluated carefully.

Some of these risks reflect the use of third-party technology, data or cloud services by FIs to deliver increasingly technology-savvy and digital-driven services. While the risks of such third-party arrangements are structured similarly, the concentration of a very limited number of vendors, the difficulty of substituting vendors, the inability to negotiate contracts effectively, and the limited rights of access or audit mean some of these risks are very significant and have received a great deal of regulatory attention, as evidenced by recent regulatory pronouncements from across the globe. As discussed further below, regulators in many jurisdictions are heightening attention on critical IT third-party service providers. The Financial Stability Institute (FSI) considers various approaches to achieve this supervision or oversight in the August 2022 issue of *FSI Briefs*, "Safeguarding Operational Resilience: The Macroprudential Perspective."

Regulatory response to TPRM

National regulatory bodies across the globe continue to reinforce their expectations for TPRM. The Financial Stability Board's (FSB's) November 2020 discussion paper, *Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships*, and the comments submitted in response, provide a good overview of the industry's challenges managing a variety of third parties across multiple regulatory regimes. While the regimes share many common expectations, they can differ materially in the way those expectations are presented and enforced. It is a classic 80/20 rule: Eighty percent of the expectations remain consistent across global regulatory bodies, but 20% are uplift requirements, some of which are easier than others for global programs to address. The following discussion provides an overview of the current state of play in a number of major financial markets.

United States

In July 2021, the Office the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC) and the Federal Reserve System issued for comment proposed interagency guidance for third-party risk management. Aiming to align each agency on TPRM, the proposed framework builds on previously released OCC guidance and continues to focus on developing a risk-based approach to TPRM. Although the comment period concluded on September 21, 2021, a final rule has yet to be issued.

The proposed guidance continues to highlight that FIs — specifically, banks in this instance — are responsible for oversight of third parties and for ensuring that the FI is still complying with laws and regulations. The framework also addresses supervisory reviews of third parties that would occur if a regulator determined that an FI did not accurately assess a third party. Cloud outsourcing arrangements have not been specifically addressed by this guidance. However, they have been, and will continue to be, a focus of the U.S. examination process and are addressed in the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbooks.

Canada

In April 2022, the Office of the Superintendent of Financial Institutions (OSFI) issued a consultation on revisions to its Guideline B-10 relating to TPRM expectations. The consultation, which closes in September 2022, proposes enhancing Guideline B-10 to reflect a more comprehensive set of third-party risks within an expanded third-party ecosystem, emphasising governance and risk management programs, and setting outcomes-focused, principles-based expectations for federally regulated financial institutions (FRFIs).

Draft Revised Guideline B-10 applies to a significantly wider variety of third-party arrangements. It proposes to govern not only risks posed by traditional outsourcing arrangements but also those posed by external entities engaged on a commercial or strategic basis, including material subcontractors. The proposed risk-based approach will broaden the risks to be assessed as well as require financial institutions to adopt a life cycle approach to TRPM, commensurate with the level of risk of the arrangement.

United Kingdom

The U.K. regulators have had long-standing requirements regarding material outsourcing arrangements, including notification before entering into them. The Prudential Regulation Authority (PRA) has recently increased the regulatory focus on TPRM and outsourcing. As a means of improving the operational resilience of the financial sector and reducing perceived vulnerabilities due to “reliance” on third parties, the PRA issued Supervisory Statement 2/21 in March 2021.

The statement provides further definition of, and outlines requirements relating to, outsourcing arrangements, expectations for non-outsourcing third-party arrangements (e.g. material or high-risk hardware, software, and other information and communications technology (ICT) products) and third-party arrangements subject to regulatory requirements. Where non-outsourced third parties are deemed to be "material" or "high risk," institutions are expected to implement risk-based controls as robust as those that would apply to outsourcing arrangements with an equivalent level of risk or materiality. The PRA reminds institutions that while third-party arrangements subject to regulatory requirements (e.g. clearing, settlement and custody services) do not meet the definition of outsourcing, they should be subject to appropriate monitoring and risk-based controls.

In July 2022, the PRA and the FCA jointly issued a Discussion Paper laying out the intention to supervise critical third parties (CTPs) (e.g. cloud service providers) in the U.K. directly. The direct oversight aims to overcome limitations in the current regulatory framework on supervisory authorities managing systemic risk posed by CTPs and would include setting minimum resilience standards, testing resilience and coordination with other regulatory bodies globally.

European Union

The European Banking Association's (EBA's) Guidelines on outsourcing arrangements, which came into effect in September 2019, have been the key source of regulatory requirements for European FIs for some time. These guidelines were strengthened in June 2020 by the EBA's Guidelines on ICT and security risk management, which set out further requirements and guidelines relating to the ICT risks that may involve a third party.

Recognising the heightened risks of outsourcing to cloud service providers as cloud adoption becomes an accepted practice in financial services, other European supervisory authorities, including the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA), have issued guidelines on outsourcing to cloud service providers.

In September 2020, the European Commission (EC) published a proposal for a regulation on digital operational resilience for the financial sector, known as the Digital Operational Resilience Act (DORA), as part of its digital finance package (DFP). DORA aims to harmonise the regulation and supervision of digital operational resilience and ICT risk management across the EU financial sector. Once the regulation has been finalised, the oversight framework is expected to have a significant impact on operational resilience and the risk management of third parties, including cloud service providers.

Australia

The Australian Prudential Regulation Authority (APRA)'s long-standing Prudential Standard CPS 231 covers outsourcing arrangements with material third parties and related entities. The standard requires APRA regulated entities to undertake appropriate due diligence, approval, and ongoing monitoring.

In July 2020, APRA's Prudential Standard CPS 234 came into effect. CPS 234 focuses on requirements for managing information security risks that APRA-regulated entities may be exposed to through third-party arrangements. The requirements include contractual rights for assurance and audits of third parties, appropriate monitoring and management of third parties, and senior management reporting and oversight.

In a further development, in July 2022, APRA initiated Discussion Paper 230 on strengthening operational risk management that proposes a new standard to enhance TPRM by extending requirements to all material service providers for critical operations or those that expose APRA-regulated entities to material operational risk. The proposed new standard will consolidate and replace Prudential Standard CPS 231 and Prudential Standard CPS 232, which pertains to business continuity management. The proposed standard provides a contemporary view of the risks arising from sourcing relationships and the expectations to maintain an operationally resilient institution. The final requirements are expected to take effect in 2024.

Hong Kong

In July 2022, the Hong Kong Monetary Authority (HKMA) issued its Regtech Adoption Practice Guide for third-party monitoring and risk management. The purpose of the guide is to provide an overview of the regtech solutions used in third-party monitoring and risk management, outline common challenges observed during implementation, and walk through examples from industry. It shares best practices and ways leading banks are addressing risks arising from third parties, including strategy and operating models, resourcing, governance and organisation, and technology and data.

While the focus is on regtech providers, the principles and examples provide valuable insight to the regulatory expectations of other third-party relationships. The HKMA requires banks to have a clear view of critical business processes and services and identify the role that third parties play in these areas. It reminds them that the approach to risk assessment across various regulatory and governance priorities should be applied consistently and should adhere to regulatory requirements.

Singapore

In January 2021, the Monetary Authority of Singapore (MAS) revised its Technology Risk Management Guidelines, which seek to help FIs establish sound technology risk governance and oversight and maintain cyber resilience. The revised guidelines note that while the use of third parties by FIs may not always be considered outsourcing, third-party relationships require appropriate due diligence prior to contracting, and monitoring on an ongoing basis. The MAS Guidelines on Outsourcing, issued in 2016 and revised in 2018, remain in effect and cover cloud computing.

Recent regulatory pronouncements highlight risks associated with third parties outside the financial services sector (i.e. nonregulated) and noncontractual outsourcing arrangements. Global regulators are increasingly recognising that non-outsourcing third-party arrangements may pose significant operational risk or have a critical impact on operational resilience and require stronger management and oversight. The increasing industry trend to outsource cloud services is driving further regulatory requirements. We can expect to see additional regulatory pronouncements and tightening of requirements and expectations in these areas globally.

A framework for TPRM

Notwithstanding differences in approach, global regulators agree that the use of a third party does not allow an FI to abdicate its responsibility for the performance of a third party. This means that FIs must proactively manage their third-party relationships. A sound risk management framework for third-party arrangements (shown below) details and assigns authority for a number of activities aimed at evidencing that the FI has done and is doing the following:

- Carefully considered the selection of the third party and its alignment with the institution's business needs (**Planning**). This deliberation includes embedding the assessment of third parties within strategy and planning processes and ensuring that product and service innovation encourages working with third parties to create value to customers and manage risks. Where a new third-party relationship is envisaged, a formal business case should be developed, considering the strategic implications and explicit requirements of the third party. Appropriate risk assessment and due diligence (detailed further below), including consideration as part of new product and service approvals and IT change management processes, should be performed prior to contracting. Senior management oversight and approval will be required for significant third-party relationships.

- Conducted a risk assessment and a thorough due diligence on the third party commensurate with the risk it poses to the FI (**Due Diligence and Vendor Selection**). The risk evaluation will include an assessment of the inherent risk (based on services to be provided by the third party), the risk assessment of the third-party arrangements, and an overall residual risk and risk mitigation plan. A detailed evaluation of each third party will be required, focusing on the key risks identified and including considering the use of fourth parties, data flows, and common ownership and networks that may allow data to be shared beyond planned activities. Business stakeholders should also consider criticality to operations and how the third party will impact resiliency planning. An appropriate risk-based due diligence program is the foundation of an effective program for managing third-party risk.

Protiviti's TPRM Framework

- Contracted and established service-level agreements (SLAs) with the third party that clearly establish roles, responsibilities and expectations (**Contract Management**). Establishing contract requirements and successful contract negotiation with the third party are critical to a successful outsourcing relationship and meeting regulatory expectations. Key considerations should include issue- and breach-notification requirements, data security, resiliency plans and oversight, subcontractor and fourth-party requirements, access and audit rights, and compliance with applicable laws, regulations and other business requirements. Exit plans, substitutability and disruption and business-continuity clauses are also critical. Further, FIs will need to ensure that the business transitions successfully to the third party and that the institution's policies and procedures, and its monitoring and reporting protocols and requirements, are all well established and embedded.
- Monitors third-party performance on an ongoing basis and, as necessary, takes steps to terminate and replace the third party (**Monitoring and Management**). Regular and ongoing monitoring, assessment and review of third-party relationships (in line with contract terms, agreed performance thresholds and risk assessments) should be performed in accordance with the FI's TPRM and governance framework. The nature and frequency of review and information requirements will be determined using a risk-based approach. FIs will also have policies and processes for issue management, contract renegotiation or key changes in the relationship, and for managing the risks and process of terminating the third-party relationship.

Governance of the TPRM program is critical to its effectiveness. Today, most FIs, large and small, have a TPRM function or Center of Excellence to manage third-party risks consistently and ensure oversight of the risks across the TPRM program. Large FIs often have a dedicated

second-line team sharing services with a first-line team that supports the day-to-day operation. Small FIs often combine first- and second-line responsibilities. The TPRM function works closely with other risk stakeholders (e.g. compliance, cybersecurity) to ensure that third parties measure up to the expectations of the FI and its regulators. More mature risk frameworks align TPRM programs within the overall risk function to ensure consistency of approach, establish standards, and minimise potential overlaps and gaps.

Questions management should ask

Management and boards of directors of FIs that have a sound TPRM risk management framework, as described above, will receive periodic reporting on the TPRM program. However, management teams that may not feel well informed, or want to challenge their FI's framework, should ask the following questions:

1. Do we understand the regulatory requirements and expectations for TPRM, and, for global FIs, how have we reconciled differences in home and host country requirements as applicable?
2. Do we have sufficient, appropriately trained staff and senior managers who understand the various risks of third parties and can assess and mitigate those risks?
3. Do we have a uniform, enterprise wide, risk-based program for managing third-party relationships?
4. Are we confident that we have identified and, if relevant, categorised all our third-party relationships?
5. Is our third-party due diligence program (onboarding and ongoing) appropriately risk-based?
6. Do we have an effective escalation process for identifying underperforming vendors or vendors that otherwise pose risk?
7. Is operational resilience factored into our third-party relationship arrangements and management?

About Protiviti's TPRM Services

Through our third-party management Center of Excellence, which comprises experts from our Business Performance Improvement, Risk and Compliance, and Security and Privacy practices, Protiviti has assisted financial institutions of all sizes in creating effective programs to manage vendors and third parties. Our TPM engagements have spanned strategy and program assessment; design and implementation/transformation; improvement of individual risk domains, including BCM, IT security, privacy, PCI and compliance; third-party audits (IT security/shared assessments, operations, compliance); technology enablement; and targeted issue remediation and incident response.

Protiviti provides an integrated solution to ensure that the appropriate operational, regulatory, compliance, risk management and IT expertise is provided on every engagement. We offer the depth and agility to configure teams and solutions to meet our clients' third-party and compliance needs.

Contacts

Carol Beaumier
Senior Managing Director
Risk & Compliance
Protiviti — New York
carol.beaumier@protiviti.com

Bernadine Reese
Managing Director
Risk & Compliance
Protiviti — London
bernadine.reese@protiviti.co.uk

Mark Burgess
Managing Director
Risk & Compliance
Protiviti — Sydney
mark.burgess@protiviti.com.au

Brian Kostek
Managing Director
Risk & Compliance
Protiviti — Tampa
brian.kostek@protiviti.com