Software Engineering Institute
Carnegie Mellon University

MANAGING THIRD PARTY RISK IN FINANCIAL SERVICES ORGANIZATIONS: A RESILIENCE-BASED APPROACH

John Haller and Charles M. Wallen

September 2016

Introduction

Outsourcing to third parties and the resulting dependency risks have become a leading consideration for financial services firms, drawing extensive management attention and regulatory scrutiny. This is particularly true for third party risks that arise from the use of information and communication technology (ICT), which may include data breaches, fraud, access to sensitive internal information, reputation impacts, or disclosure of intellectual property. These concerns are exacerbated by a pervasive and dynamic cybersecurity threat landscape. Attackers know that third party suppliers can be a weak link and target them accordingly.

Recent, high profile incidents involving the financial industry highlight the unexpected or unintended consequences that can arise when organizations outsource support and processing activities. This is particularly true for customer-facing services supported by outsourced information technology. Regulators have emphasized careful oversight of third party suppliers and have strongly urged senior management to more directly engage in this area of risk management.

Financial services institutions face a number of hard questions with respect to managing third party risks:

- How can financial services organizations manage risks commensurately with the level of risk and complexity of the third party relationship?
- How can financial services organizations judge how well they are managing third party risk?
- How can financial services organizations cost effectively satisfy the heightened expectations of regulators? (e.g., Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT), Office of the Comptroller of the Currency (OCC) Bulletin 2013-29, and Federal Reserve Board (FRB) guidance). See Appendix 2 for more context on the regulatory environment for financial services.

This white paper describes a resilience-based approach to third party risk management that can help financial services organizations efficiently and effectively answer these questions and address regulatory concerns. A resilience-based approach emphasizes the following key principles:

- focusing on the critical subset of activities and risks that are essential to meeting an organization's objectives
- identifying and managing key cybersecurity requirements

Distribution Statement A: Approved for Public Release; Distribution Is Unlimited

- balancing protection and sustainment investments efficiently
- establishing consistent and predictable cybersecurity processes
- ensuring that those processes are managed end-to-end

Key Challenges in Third Party Risk Management

Loss of control is the most basic and defining challenge in managing third party risks. When organizations rely on third parties—whether suppliers, contractors, consultants, or critical infrastructure providers—they give up a certain amount of control over the assets, people, and processes that they rely on. This is true no matter how strong or well-drafted the contract or agreement may be.

Outsourcing inherently means that the organization depends on external entities that may not share its approach to resilience and cybersecurity or which may have a different level of security capability.

Naturally, third parties also approach resilience according to their own business interests, priorities, and financial situations. In every case, a principle obstacle is that much of the information necessary to make accurate decisions and manage risk resides with the third party. Its failures directly impact the organizations that rely on it.

Third party risk management presents a problem for organizations of any size. For example, smaller firms may not be able to convince larger vendors to meet their requirements or provide adequate information about the supplier's cybersecurity capabilities. Larger firms may have greater resources than smaller ones but frequently must manage relationships with hundreds of vendors. Third party risk management can quickly become unwieldy and very complex. The uncertainty involved in relying on third parties exists across the board.

A key problem for many organizations—especially larger organizations or those offering many services or products—is identifying critical third parties and quantifying their importance. Thousands of third parties may need to be evaluated, requiring a considerable outlay of resources just to track and manage them. For tracking to be effective, the list of suppliers must be periodically updated to reflect important changes. Examples of such changes include the relative importance of the third party, the organization's requirements for the third party, the organizational services and products it supports, contract changes, location changes, administrative changes, and changes in second or third tier suppliers and subcontractors (if that is being tracked).

Third party risk management touches upon and involves many parts of an organization. A basic problem is getting internal stakeholders to understand and participate in this area of risk management. For example, many procurement and purchasing departments still do not focus on evaluating the cybersecurity capabilities of third parties or include relevant requirements and clauses in contracts.

Some institutions manage third party risks using business rules. For instance, they may not permit certain types of data to be hosted or processed outside the organization. One problem with this approach is that it may not provide enough flexibility in applying the latest technologies and innovating in new

Distribution Statement A: Approved for Public Release; Distribution Is Unlimited

ways. Institutions may find themselves dependent on a smaller supplier that is the sole source for a particular item or offers an important competitive advantage, but which may not have robust cybersecurity capabilities.

From a cybersecurity perspective, third party risks frequently involve a set of threats that may exceed the scope of the organization's risk management activities. Some organizations focus too narrowly on risks. For example, when hosting data in the cloud, most organizations ask the vendor for attestations or some evidence of cybersecurity capability. However, information and communications technology supports almost every supplier for a given organization, not just those that are explicitly focused on data processing and storage. The scope and complexity of these dependencies may dictate a more comprehensive cybersecurity risk review than is frequently conducted. In addition, some organizations fail to consider the broader set of external dependencies on critical infrastructure and public services. A more complete view of third party risk considers the full range of external or third parties and can be broadly termed *external dependencies management*.

Financial Sector Challenges and Solutions

All of the third party risk management challenges discussed above are particularly acute for financial services organizations. They are frequent targets for cyber-attacks, they make extensive use of third parties, and they must manage intensive regulatory oversight. The lure of monetary gain from financial firms draws threat actors from around the world. Successful attacks also provide visibility for those who are motivated by non-monetary or political objectives. Attacks can heavily damage the reputations and brands of financial services organizations. Financial services companies are often connected to a wide array of suppliers needed for payments, clearing and settlement, data processing, communications, and so forth. Scrutiny of the risks associated with these supply chains has taken a more central role in operational risk exams. The rigor of legal and regulatory oversight continues to increase.

Recent regulatory guidance mandates that financial services organizations manage risk commensurate with the "risk and complexity of its third party relationships."[1] But what does complexity mean in this context? Is it defined as technological complexity, interdependencies, or the number and variety of threats? Is it riskier for only one supplier to support multiple services? Does this represent an unacceptable concentration of risk?[2] What if concentrating support with one supplier allows the organization to negotiate higher security standards with that vendor? Or is it unacceptably complex and risky for key services to be supported by many third parties? What if relying on multiple external entities yields security benefits through diversity and redundancy?

---

[1] Office of the Comptroller of the Currency. *OCC BULLETIN 2013-29: Third Party Relationships.* October 30, 2013. http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

[2] Board of Governors of the Federal Reserve System, Division of Consumer and Community Affairs, Division of Banking Supervision and Regulation. *Guidance on Managing Outsourcing Risk.* December 5, 2013. Section II, page 1. http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

Distribution Statement A: Approved for Public Release; Distribution Is Unlimited

What the financial industry needs is a systematic approach that provides consistency, efficiency, and predictability in assessing and managing third party risk. A common approach across the industry, or at least one based on the same basic tenets and framework, would facilitate cooperation across institutions and help to ease uncertainty for executive leadership. Without a common approach and language for describing third party risks, organizations may take disparate pathways to addressing dependency risks. Lacking a common approach, collaboration is more difficult and less efficient; it also introduces more uncertainty during exchanges with business partners, stakeholders, and regulators.

For those in highly-regulated industries, such as banking and financial services, new regulatory guidance and oversight require increased risk management focus and investments that are difficult to prioritize (e.g., FFIEC Cybersecurity Assessment Tool, OCC 2013-29, and the FRB's guidance). Approaching the problem through *resilience management* (discussed in the next section) provides efficiencies, simplifies implementation and management, and facilitates compliance with the latest round of regulatory guidance.

A Resilience-Based Roadmap

Resilience is an organization's ability to adapt to and withstand disruptions, be they cyber-attacks, disasters, or simply the constant pace of change. [3] Organizations of all sizes and types face disruptions and must establish practices that make sense for their situation, budget and risk appetite. A core principle of a *resilience-based* approach is efficiency: having an organizationally appropriate level of investment in managing risk and cost.

A resilience-based approach to managing third party risk features the following characteristics:

Focus on Service Priority: Services are core activities that an organization conducts to achieve its mission. Identifying and prioritizing services can help to make decisions about resilience activities. It also assists with activities central to third party risk management, such as prioritizing and assigning tiers to third parties. In a financial institution, services include activities such as account management, loan operations, mortgage processing, ATM operations, and online banking. Many organizations may wish to examine third party risks and conduct improvements across their lines of business. Nevertheless, a thorough understanding of critical services and functions is a key foundational step for managing risk.

Establishing Repeatable Processes: Key processes and practices become consistent and part of the organization's culture and way of doing business—that is, they become institutionalized processes. As a result, they function in a predictable way even during times of disruption and stress with less risk and uncertainty.

---

[3] For more information about resilience, refer to the CERT Resilience Management Model. More information is available at http://www.cert.org/resilience

Institutionalized (or repeatable) processes are created through consistent and thoughtful management and governance activities. Important activities for establishing and governing repeatable capabilities include the following:

- planning the activity for the organization—how will the organization tie together the activities of various departments and components to effectively manage third parties?
- maintaining policies that apply to third party risk management, including standards and guidelines
- ensuring that the right stakeholders are involved
- overseeing the daily execution of third party risk management
- periodically assessing the organization's processes to ensure they are complete and meet the organization's needs
- identifying, collecting and reporting measurements and metrics to ensure the activities are effective and that stakeholders are engaged
- ensuring that third party risk management activities are adhering to plans and policies

Requirements Management: The organization identifies and updates resilience requirements for assets and third party relationships that support its high-priority services. These requirements can include (but are not limited to) traditional information security requirements such as confidentiality, availability, and integrity.

Identifying and updating the requirements that apply to third parties are essential to managing third party risk. This involves communicating and exchanging information with the right internal stakeholders. Appropriate requirements for third parties are largely driven by what is needed to protect and sustain assets used to support high-priority services. For example, the controls and requirements relevant to information privacy or confidentiality may differ from controls focused on system availability.

Requirements may also arise from broader edicts such as regulations and corporate policies. For example, the Gramm-Leach-Bliley Act (GLBA) of 1999 requires the protection of personal information. An internal corporate policy may establish a rule that all data must be encrypted. Such requirements provide the basis for managing a relationship with a supplier.

Balance Protection and Sustainment Activities: A resilient organization appropriately balances protective and sustainment activities for important assets. Protective activities are usually termed "security" and focus on minimizing the exposure of assets to threats. Access management is a typical example of a protective activity. Sustainment activities are usually response activities and focus on sustaining assets after they are exposed to a threat or attack. Incident management and business continuity are typical examples of sustainment activities. Protective and sustainment activities must be part of a coordinated cybersecurity posture. Allowing them to operate independently in siloes can leave important assets insufficiently supported and defended or lead to unnecessary overinvestment in a particular area.

A similar logic applies to establishing an appropriate balance of third party risk management practices and controls. An organization should establish compensating controls and activities whenever it must rely on a third party with limited cybersecurity capabilities. For example, if an organization relies on a

Distribution Statement A: Approved for Public Release; Distribution Is Unlimited

less capable third party, its situational awareness and threat management efforts must consider the risk associated with that third party.

Life Cycle Coverage: Resilient organizations manage services, systems, assets, and third party relationships across their life cycles. To identify improvements that lead to greater efficiency and less risk, managers should assess, govern, and manage the organization's external dependency risks across the complete life cycle of these relationships. Failures at the start of this process—for example, deficiencies in how third parties are selected or evaluated—can have large impacts in the future when conditions change or the organization experiences a disruption.

Third Party Risk Management is a Team Sport

To be effective, third party risk management must get disparate parts of the organization and outside entities to work together. In contrast, traditional information security practice sometimes treats third party risk management as an "add-on" to otherwise siloed security activities. Further complicating the challenge is the tendency to treat dependency risk as a one-off, supplier-by-supplier activity rather than a key strategic component of enterprise risk in conjunction with other critical areas (such as financial and operational risks). An organization must manage a diverse set of risks and, where possible, collaborate with suppliers and other organizations to manage exposures.

Savvy managers engage with key internal and external stakeholders that may include line managers, IT leaders, external business partners and suppliers. Gathering the right requirements and understanding risks are only part of the reason why they engage with these stakeholders. It is also because the capabilities needed to mitigate third party risks are most likely to be spread across the organization and external groups. For example, an inability to find a supplier with the right capabilities may mean that another part of the organization (such as information security) must do more to compensate for this weakness. If an organization relies on a relatively immature supplier, its situational awareness and threat monitoring activities should include a stronger focus on third parties and exchanging information with other organizations.

The Financial Sector repeatedly experiences threats requiring extensive internal and external collaboration to effectively manage dependency risks. The Financial Services Information Sharing and Analysis Center (FS-ISAC) is a non-profit, member-driven organization that enables over 7000 financial firms to proactively share threat and vulnerability intelligence. FS-ISAC works to provide collaborative information and response strategies for its members. A prominent example is the 2012 distributed denial of service (DDOS) attacks that specifically targeted financial organizations. Coordinated efforts to share real-time threat intelligence that helped address this risk—and ultimately, to find and prosecute those who were responsible for the attacks—demonstrated the value of working together to meet today's challenging cyber-risk environment.

The complexity and difficulty of managing third parties means that relying on one part of your organization to manage risk—for instance, contracting or procurement—is not enough. The challenge must be addressed and the risk managed across the organization, preferably by sharing the responsibility.

Distribution Statement A: Approved for Public Release; Distribution Is Unlimited

Adjusting the mix of internal, external, and cooperative security activities can help an organization find the most effective balance to manage its risks and meet its requirements. More specifically, these activities can be defined as

- internal—actions that can be directly controlled by an organization, such as using multiple suppliers and limiting the type of information that external providers are allowed to process
- external—activities the organization requires a supplier to perform, such as encrypting data, monitoring network access, and requiring specific software patch management procedures
- cooperative—activities organizations can do in collaboration with suppliers or partners, such as conducting joint assessments of controls and sharing information about cyber threats

As an organization builds trust with its suppliers and other organizations over time, it is often possible to refine the mix of strategies and develop collaborative approaches to managing risk. For public and shared infrastructure, using cooperative risk management strategies can be one of the most effective means of managing risk. For cyber threats, it is increasingly evident that more information sharing and collaboration are needed to combat the sophisticated attacks being faced by all organizations.

Regardless of how these risks are addressed, doing nothing is a poor strategy. Inaction leads to failed threat management outcomes, inefficiency, and non-compliance.

Conclusion

Outsourcing provides many positive benefits, but it also comes with risks. Expanded use of information technology and global communication create dependencies that require better methods and practices to resolve risk and meet the dynamic needs of organizations. Financial services organizations are particularly affected by this problem, due in part to their high profile role in managing payments and their constant need to innovate. Financial sector regulators are actively putting new layers of regulation in place, much of it focused on third party cybersecurity. Unfortunately, some of this guidance is inconsistent and may involve conflicting approaches. This situation leaves organizations unsure that they have invested in the right things, while they continue to be exposed to a growing threat environment.

Appendix 1 provides a set of initial steps towards improving third party risk management capability. By applying widely accepted practices rooted in resilience-oriented risk management, organizations can reduce risk, improve compliance, and avoid costly disruptions. For example, practices such as tracking key assets, creating plans to manage cyber events, and monitoring technology controls for effectiveness are widely viewed as basic resilience management activities.

The NIST Cybersecurity Framework (CSF)[4] outlines key cyber practices. It is increasingly seen as a valuable way to organize, manage, and articulate practices focused on cybersecurity and third party

[4] Cybersecurity Framework, *NIST Website.* http://www.nist.gov/cyberframework/

Distribution Statement A: Approved for Public Release; Distribution Is Unlimited

risks. Navigating the multitude of overlapping and often confusing "best" practices, standards, and regulations is a constant challenge. For multi-national organizations, this challenge has expanded with a multiplicity of data privacy laws and national initiatives. Organizations are often overwhelmed by uncertainty as to which standards and regulations they must follow. Smaller and less experienced organizations are often frustrated as they attempt to identify a road map to manage their cybersecurity risks. By adopting the language and structure of the CSF, financial services organizations can more effectively and efficiently communicate with their peers and vendors about cybersecurity and resilience. The common language in the CSF can be used by virtually all organizations to identify, assess, and improve organizational cybersecurity capabilities.

These resources can help institutions to answer some of the questions posed by the recent focus on third party risk by the FFIEC, OCC, and FRB:

How can financial services organizations manage risks commensurately with the level of risk and complexity of the third party relationship?

They can do so by understanding the services (and related priorities) that third parties support, consistently defining and updating the requirements associated with those third parties, and ensuring that stakeholders are engaged. The quantity and intricacy of requirements for managing supplier relationships can provide valuable measurement criteria to determine the level of risk and complexity.

How can financial services organizations judge how well they are managing third party risk?

By assessing their processes for managing risk and by benchmarking themselves against peers by using tools based on the NIST CSF and accompanying resilience management methods. The CSF established a common set of leading practices and a widely accepted vernacular for domestic events, which has influenced similar international efforts.[5] The Department of Homeland Security Cyber Resilience Review (CRR)[6] is specifically designed to help organizations implement the CSF and assess themselves against it. Similar assessment tools, such as the External Dependency Management (EDM) Assessment, focus on organizational management of third party risks.[7]

---

[5] Shackelford, Scott; Russell, Scott; & Haut, Jeffrey. Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks. *UC Davis Business Law Journal*, 2016; *Kelley School of Business* Research Paper No. 16-2. http://ssrn.com/abstract=2702039

[6] C[3] Voluntary Program Assessments: Cyber Resilience Review (CRR). *US-CERT Website.* https://www.us-cert.gov/ccubedvp/assessments

[7] Supply Chain Risk Management Solutions. *CERT Website.* https://www.cert.org/resilience/products- services/supply-chain-risk-mgt-solutions.cfm for more information.

Distribution Statement A: Approved for Public Release; Distribution Is Unlimited

How can banks cost effectively satisfy the heightened expectations (e.g., FFIEC Cybersecurity Assessment Tool, 2013 OCC and FRB's guidance) of regulators?

Organizations can establish efficient, risk based strategies built on cybersecurity management approaches and practices that are widely accepted techniques for managing cybersecurity. The Cybersecurity Framework is the most prominent example. Many regulatory agencies in the United States have embraced the CSF,[8,9,10] making it directly applicable and defensible as a way to build compliant cybersecurity risk management strategies. The CSF is foundationally a collaborative approach, which adds to its appeal as a way to communicate and address the relationships and dependencies on other organizations that characterize cybersecurity today.

Ultimately, the use of third party suppliers and outsourcing does not absolve organizations of responsibility for that risk. It is essential that organizations implement pragmatic risk management strategies that they can control. Doing nothing because suppliers are hard to manage is not a viable approach. The most efficient course of action incorporates converged practices, collaboration, and relationship building. This strategy applies for domestic dependencies and arguably may be even more effective internationally, where the challenges of managing third parties is compounded by distance, legal, and cultural variables.

---

[8] Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation. *FFIEC Cybersecurity Assessment Tool for Chief Executive Officers and Boards of Directors.* SR15-9. July 2, 2015. https://www.federalreserve.gov/bankinforeg/srletters/sr1509.pdf. This document ties the FRB, FFIEC, CAT and the CSF together as the means to assess institutions.

[9] Federal Financial Institutions Examination Council. *FFIEC Cybersecurity Assessment Tool User's Guide*. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_User_Guide_June_2015_PDF2_a.pdf. See paragraph 2 for linkage to CSF.

[10] Aguilar, Luis A. Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus. *Speech given at Cyber Risks and the Boardroom Conference.* New York Stock Exchange. New York, NY. June 10, 2014. https://www.sec.gov/News/Speech/Detail/Speech/1370542057946

Appendix 1 Road Map for Managing Resilience and Third Party Risk

Financial services organizations frequently wrestle with where to focus their third party risk efforts. Under the operational resilience approach laid out in this paper, a good initial set of activities to assess and improve third party risk management in an organization includes the following:

- Prioritize the organization's critical services and functions. Ensure that all of the stakeholders relevant to third party risk management understand these priorities.
- Assess the organization's existing third party risk management practices against a standard or similar guidance. Identify areas for improvement.
- Assess and understand how the organization develops resilience requirements for third parties and ensures that these requirements are included in contracts. Involve the right stakeholders and ensure they understand their roles.
- Understand the communication flows between procurement or vendor management, security, IT, and business continuity resources with respect to third parties. Ensure that relevant stakeholders are assigned responsibility for incorporating third party risk management considerations into their planning and activities.
- Evaluate the organization's higher level governance activities that apply to third party risk management. Identify priorities for engaging with senior and higher level leadership.
- Understand how the organization currently measures the effectiveness of third party risk management activities and compliance with relevant policy and procedures. Develop improvements.

A third party risk management program can build upon existing processes in the organization. Not only does this help to contain costs, it can also ensure that information critical to multiple management processes is shared and improve consistency. Key activities that provide traction and efficiencies include the following:

- Use existing organizational information sources (such as contract databases and accounts payable tracking) to identify suppliers.
- Use existing business impact and process flow analyses to assess high value services for third party risks.
- Identify and prioritize dependency risks in conjunction with continuity and incident management planning.

Distribution Statement A: Approved for Public Release; Distribution Is Unlimited

Appendix 2 Financial Sector Third Party Risk—Regulatory Context

Some of the most notable laws and regulations include the Gramm-Leach-Bliley Act (GLBA) of 1999,[11] the Office of the Comptroller of the Currency (OCC) Third Party Relationship and Risk Management bulletin of 2001,[12] and the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbooks.[13] The heightened concerns of US regulators were clearly communicated to the United States financial services community in late 2013 when the OCC and the Federal Reserve Board (FRB) issued more prescriptive guidance.[14,15] The most recent regulatory release was the FFIEC Cybersecurity Assessment Tool (CAT)[16] of June, 2015, which includes a focus on third party risk and an explicit External Dependency Management domain.

---

[11] [2] *S.900 - Gramm-Leach-Bliley Act.* 106th Congress (1999-2000). https://www.congress.gov/bill/106th- congress/senate-bill/900

[12] United States Office of the Comptroller of the Currency. *OCC BULLETIN 2001-47: Third-Party Relationships.* http://ithandbook.ffiec.gov/media/27914/occ-bul_2001_47_third_party_relationships.pdf

[13] *FFIEC IT Examination Handbook InfoBase.* http://ithandbook.ffiec.gov/

[14] Office of the Comptroller of the Currency. *OCC BULLETIN 2013-29: Third Party Relationships.* October 30, 2013. http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

[15] Board of Governors of the Federal Reserve System, Division of Consumer and Community Affairs, Division of Banking Supervision and Regulation. *Guidance on Managing Outsourcing Risk.* December 5, 2013. http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

[16] Cybersecurity Assessment Tool. *FFIEC Website.* https://www.ffiec.gov/cyberassessmenttool.htm

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu | www.cert.org
Email: info@sei.cmu.edu

Copyright 2016 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0004013