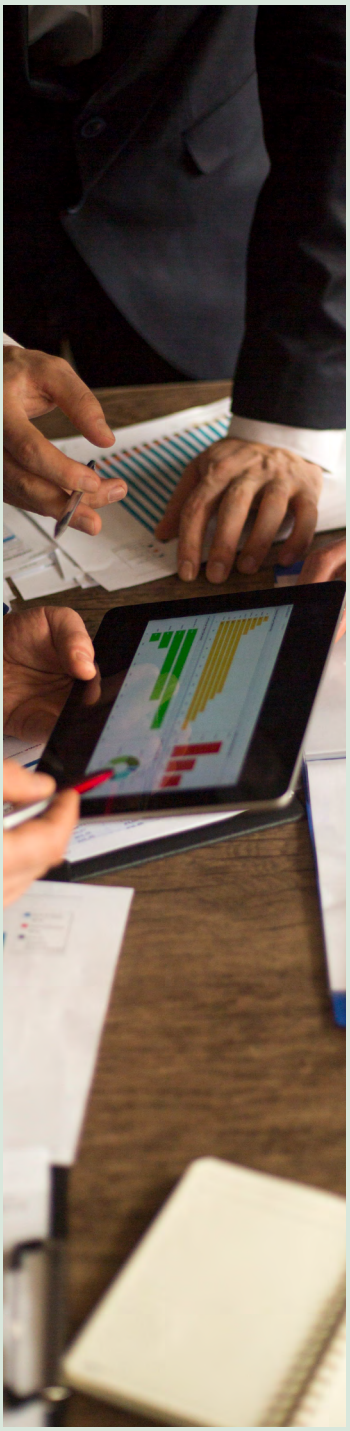
WHITE PAPER



THIRD-PARTY RISKS ARE ON THE RISE: HOW CAN YOU PROTECT YOUR FINANCIAL SERVICES ENTERPRISE?

metricstream

Infosys®
Navigate your next

Introduction

Financial services institutions (FSIs) worldwide are increasingly relying on low-cost third-party service providers to deliver business-critical services. Many have set up global in-house centers (GICs) or captive subsidiaries in low cost, often remote, locations to take advantage of diverse talent pools and skill sets.

While these shifts are valuable to the bottom-line, they have also caused an increase in third-party risks across the industry. So, it isn't surprising that financial regulators are paying closer attention to organizations' third-party governance programs.

This paper created jointly by MetricStream, and Infosys provides a glimpse into why third-party risk management is becoming increasingly relevant to FSIs, especially in a post-Covid era. It also examines where traditional risk management programs are insufficient, and how you can effectively safeguard your financial services enterprise.

How COVID-19 exposed the holes in Third-Party Risk Management

When the pandemic hit, FSIs struggled to adapt. Most had to rethink their protocols, rebuild their processes, and reallocate resources to new business areas – all within a few days or weeks.

These conditions extended to third parties as well. The sudden shift to a remote working model left third-party employees more susceptible to cyberattacks without the hardened firewalls and security protections that office systems afforded.

Around the same time, record numbers of American employees were quitting their jobs in what became known as The Great Resignation. To fill the resulting labor gaps, many businesses hired independent contractors. Some consciously began building hybrid teams of full-time employees, freelancers, and consultants. This helped them reduce costs and scale teams as needed. But with more third parties came increased risks.

The risks are real

In June 2021, millions of Australians were unable to bank online[1] after a major blackout at a technology vendor hit multiple financial services giants, causing websites to crash and digital services to be cut for over an hour. The same year, a major investment bank reported a data breach[2] after attackers hacked into the Accellion FTA server of a third-party vendor, stealing personal information belonging to the bank's customers.

The biggest takeaway from incidents like these is that third-party risk management can no longer be an after-thought – it must become a strategic priority. Organizations need to be investing in resources, capabilities, technology, and reporting to monitor their extended enterprises.

As the risks in these ecosystems evolve, so must our controls and frameworks. In a post-pandemic world, an agile and robust third-party risk management program can make all the difference to organizational success, resilience, and even survival.

The Regulators Are Watching

Regulators worldwide are taking a closer look at how companies manage their third parties. The General Data Protection Regulation (GDPR - EU), Health Insurance Portability and Accountability Act (HIPAA - US), Personal Data Protection Act (PDPA - Singapore), and proposed Digital Operational Resilience Act (DORA - EU) are just some of the regulations that outline specific requirements for third-party risk management – that too, for data security and privacy alone.

In the financial services industry, additional third-party governance requirements are issued by the likes of the Office of the Comptroller of the Currency (OCC - US), the Consumer Financial Protection Bureau (CFPB - US), and the Financial Conduct Authority (UK). Other regulations like the Foreign Corrupt Practices Act (FCPA - US) and the UK Bribery Act (UK) cut across industries.

We are also seeing more of a regulatory focus on environmental, social, and governance (ESG) practices, not just in organizations but in their third-party ecosystems as well. For instance, the Supply Chain Due Diligence Act in Germany[3] will require companies to identify, assess, and minimize the risks of human rights violations and environmental abuses across their supply chains.

As regulatory scrutiny increases, fines for violations are touching hundreds of millions of dollars. The underlying message is that FSIs can no longer wash their hands off the actions of their third parties. The same level of due diligence, risk monitoring, and controls that they implement within their own organizations must be extended to third parties as well.

The Old Way vs a Better Way

Old isn't necessarily gold when it comes to third-party risk management. Controls and best practices that held good even five years ago may neither be effective nor efficient today. That's because the nature of third-party relationships has changed and so has the complexity of global third-party ecosystems.

Recent scandals at Credit Suisse were attributed to due diligence failures.[4] This scandal exposed not only failures in the bank but also their third-party risk management system.

Traditional third-party risk management processes tend to be:

Siloed	Reactive	Myopic	Manual
Different departments within the same enterprise manage risks in different ways.	Ongoing risk monitoring isn't prioritized and limited to initial due diligence only. Risks are identified only during third-party onboarding.	Focused only on direct third-party relationships, without considering the risk impact of fourth parties, or the interconnectedness of risks.	Time-consuming and resource intensive.

To top things off, older third-party risk management approaches often have the following drawbacks:

Lack of a 360⁰ Vision

Teams don't have a single view of third-party risk exposure. This delays decision-making and action.

Inconsistent taxonomies

Risk terminologies vary across the enterprise, hampering communication and reporting.

Unstructured Processes

Low-risk third parties aren't monitored. Supply chain disruptions and changing risks aren't considered.

Lack of accountability

Teams fail to acknowledge a security vulnerability or risk of an attack

So what is a better way of assessing and monitoring third-party risk? In our experience with leading organizations, here's what matters:

- Third-party risk management is made a strategic priority.
- Teams have a 360⁰ real-time view of third-party and fourth-party risks.
- Best practices are implemented in line with industry standard risk assessment and due diligence frameworks.
- Risks are continuously assessed.
- Clear lines of risk responsibility and accountability are established.

Best Practices to Up Your Third-Party Risk Management Game

The aim of a third-party risk management program is not only to protect your FSI from harmful incidents, but also to build resilience. You should be able to capitalize on the opportunities that third parties provide, while being prepared for all possible disruptions.

Outlined below are some best practices that can help your financial services enterprise achieve a high level of risk maturity:

Get the Basics Right: Set up a Structured Process to Assess Risks Across the Third-Party Lifecycle

Third-party risks can occur anytime, anywhere. Your best defense is a streamlined risk management process that extends from initial third-party screening and onboarding, to offboarding.

Catalogue your third-party risks: You can't manage what you don't know. So, the first step is to identify and document your third-party risks, whether they are compliance, reputational, data privacy, corruption, or sustainability risks.

Understand the source and causes of these risks: Perhaps your vendor's security patches are not up to date, or a service provider doesn't have adequate backup arrangements if their systems go down. Both incidents could impact the security and continuity of your business. By identifying them beforehand, you can proactively prevent or mitigate their impact.

Screen third parties before onboarding: Look beyond traditional financial health scores at other parameters like third-party compliance, security controls, litigation history, and political exposure.

The better you understand your vendors, the more targeted your risk monitoring will be.

Assess and prioritize third parties based on risk likelihood and impact: For instance, if a vendor handles critical financial transactions on your behalf, they may be classified as high risk – and may require more frequent risk assessments. Multiple methods can be used to assess risk – including vendor self-assessments, surveys, and external ratings. You can also use a framework like the Shared Assessments Third-Party Risk Management Framework, ISO 27001, or NIST 800-161 to provide a roadmap for risk assessments. The choice of framework would depend on your compliance requirements, risk appetite, and scope of third-party use.

Establish comprehensive agreements with third parties: Use contracts to define how your third parties will be expected to manage various risks. Be especially clear about privacy and security requirements.

These processes may seem laborious but getting the basics right can go a long way towards safeguarding your financial services enterprise.

Keep your eye on the ball: Continuously monitor the risks

Risks are constantly evolving, so it is important to stay vigilant. Initial third-party due diligence assessments or annual risk evaluations will only give you a point-in-time view of risks. In between these assessments, a lot can go wrong. That is why continuous risk monitoring is essential. This can help by regularly updating you about changing risk thresholds, new risks, and security concerns.

Monitor your third parties: Conduct risk assessments frequently and augment the findings with intelligence from external sources. Dow Jones, D&B, BitSight, Security Scorecard, and others provide trusted data on third-party parameters like financial health, bribery, corruption, and security ratings. These insights can help you deepen your own understanding of third-party risks, and proactively identify red flags.

Keep vendor profiles updated: Consider setting up a portal that consolidates all third-party information, including a list of products and services provided, contracts, risk ratings, and certifications. This centralized database makes it easier for stakeholders to search and find the third-party data they need. It can also be used by third parties to upload and update their profiles.

Develop a remediation plan: Document third-party issues or vulnerabilities spotted during a risk assessment. Categorize the issues based on their criticality and create an action plan to address them. Establish clear deadlines and responsibilities. Then, work closely with third parties to resolve the issue.

The goal of these practices is to stay one step ahead of risks. That way, your financial services enterprise can remain agile, and pivot swiftly when a third-party disruption occurs.

Only 40% of executives from various industries, including financial services, say they thoroughly understand the risk of data breaches through third parties. Nearly a quarter have little or no understanding at all about these risks.[5]

Go Deep: Cultivate a Holistic and Granular View of Third- and Fourth-Party Risks

To manage your third parties, you need to know who they are and how they fit into your ecosystem. Yet, very few FSIs, have visibility into the full map of interdependencies across all tiers in their supply chain.

Risk visibility is usually hampered when data is scattered across business units and systems. So, the solution would be to break down these silos and consolidate third-party information into a single source of truth. This gives stakeholders a unified risk view that then enables them to make more informed decisions.

However, a single source of truth is only as effective as the data it holds. So, make sure to organize your information well. Map your third-party ecosystem to the corresponding products, services, assets, and business units, as well as risks, regulatory requirements, policies, controls, and testing processes. With this integrated data model, stakeholders can quickly understand the risks associated with third parties, along with the areas of high susceptibility. A well-mapped risk universe also helps you identify how various risks are interconnected.

When constructing your third-party universe, look beyond your direct suppliers. Establish a line of sight to your supplier's vendors, subcontractors, and service providers wherever possible. You could do that by contractually binding your third parties to seek your approval whenever they want to use a fourth party's services. You could also join hands with your third parties to assess and monitor sub-contractors. The objective is to improve visibility into your entire third-party ecosystem. So, even if a bottleneck or disruption occurs deep in your network, you can quickly trace and resolve the root cause.

Third-party risk management is ultimately just one part of a larger program that encompasses third-party compliance, performance management, auditing, due diligence, and issue management. Integrating all these processes on one unified platform and linking them to your enterprise risk management (ERM) framework, can help you build a truly holistic view of risk.

Watch Out for Third-Party Security Risks: They are More Important Now Than Ever

Cyber attackers don't always launch a frontal assault on a network. Sometimes, one targeted intrusion in vendor systems is all they need to compromise hundreds of thousands of customer accounts.

During the pandemic, cybersecurity risks escalated as third-party employees began accessing sensitive data from their homes and other locations that weren't protected by enterprise firewalls. FSIs quickly realized that most of the third-party security controls they had assessed pre-pandemic weren't necessarily valid or effective anymore. They needed to be re-assessed, and third-party security profiles needed to be updated to reflect the new threat landscape.

Today, It is important to determine where your third-party's employees are accessing and processing data. If It is from their homes, examine how well employee activities are being monitored. Are their systems properly configured with firewalls, anti-malware, and intrusion prevention software? Have they received sufficient training on security awareness? Is the data backed up securely?

The idea is to determine if your third parties have bolstered their security posture since the pandemic. To assess their risks, you can use a variety of methods - be it questionnaires, partner references, or even an external third-party risk assessment service.

97% of financial services professionals say that cyber risk affecting third parties is a "critical" or "important" issue.[6]

Choose an approach or a combination of them that will give you a true picture of your third party's security risk profile. Preparing for risks before they occur can help you reduce the impact of an attack and get ahead of the issues before they spiral out of control.

Equip Your Organization with the Right Tools

Let's face it. Third-party risk management can be tough. Even if you have just a few vendors or suppliers, you need to stay ahead of multiple risks. That's hard to do when your risk assessments are manual. Fortunately, there are tools and technologies that can automate risk monitoring, making it faster and simpler. Some tools come with pre-defined questionnaires to assess risks.

There are also platforms that support the end-to-end third-party risk management cycle – from initial due diligence and onboarding to ongoing risk monitoring and reporting. Plus, they unify all third-party information and risk data in one place, so that users have a complete view of third-party risks at their fingertips to make quick, informed decisions.

Analytics are another useful tool. They help integrate disparate pieces of third-party data from internal and external sources, connecting the dots to provide a holistic picture of risk.

The more agile systems give your front-line teams easy-to-use, intuitive tools — ideally mobile. So, users can report third-party risks and observations which might not be immediately obvious to second-line functions.

How can the Infosys MetricStream Partnership help?

The Infosys Third Party Risk Management as a Service powered by MetricStream can help you streamline, integrate, and automate third-party risk management. The service provides a holistic and real-time view of your extended enterprise, including third-party vendors and suppliers, as well as fourth-party sub-contractors.

With this offering, you can:

- Consolidate all third-party data in a single source of truth for optimal visibility
- Simplify third-party data intake across departments through a user-friendly portal
- Validate third-party information based on globally sourced content automatically
- Prevent adverse incidents with consistent third-party risk and compliance assessments
- Assess and track third-party KPIs
- Capture third-party business continuity plans
- Streamline onsite third-party audits or online audit assessments
- Gain a sound understanding of third-party risks with powerful reports, analytics, and business intelligence
- Incorporate authoritative intelligence from external sources to deepen risk visibility

Looking Ahead

As Financial Services Enterprises grapple with new regulations, a rapidly growing third-party ecosystem, changing operating models, and increasing cyber threats, Third-party risk management will remain a key strategic priority.

We expect a greater focus on integrated and collaborative approaches to third-party risk monitoring. Multiple risk types will need to be tracked – cybersecurity, anti-bribery, and ESG. Many of these risks extend deep into the vendor ecosystem, making it imperative to account for not just third parties, but also fourth parties, fifth parties, and beyond.

In a rapidly shifting world, organizations need agile and forward-looking third-party programs that can incorporate continuous monitoring and early risk warnings to stay ahead of risks.

Finally, intelligent automation will be key. There is a lot of data and process complexity to be able to handle third-party risks manually. FSIs will incline towards leveraging the power of predictive risk analytics, AI, and other technologies to improve both risk management productivity and decision-making.

Ultimately, resilience is what matters the most. We all want our organizations to anticipate, respond to, and bounce back quickly from business disruptions. Core to that ability is robust third-party governance. FSIs that can proactively monitor third-party risks, prevent incidents, and enable a coordinated risk response and mitigation effort will be stronger and better positioned to thrive in the new normal.

About the Authors

Navdeep Gill

Heading GRC Practice under Financial Services Domain Consulting Group.

She has over 15 years of industry experience leading several large and complex IT consulting, process re-engineering, system integration, business transformation programs across marquee clients globally. Over the years, she has built teams and multiple COEs to address business needs across the industry domain.

Pat McParland

Director of Product Marketing at MetricStream.

She is responsible for creating product messaging, product go-to-market plans, and analyzing market trends for MetricStream's compliance and third-party risk product lines. Pat has more than 25 years of financial data and technology marketing experience at Fortune 1000 brands as well as startups and has led product and marketing teams at Dow Jones and Dun & Bradstreet. She has a BA from the College of William and Mary and lives in Summit, New Jersey.

References

1. Banks back online after Akamai outage linked to CBA, Westpac, ANZ internet banking disruptions; June 17, 2021, SMH
2. Morgan Stanley announces breach of customer SSNs through Accellion FTA vulnerability, July 09, Zdnet.com
3. Germany: New Law Obligates Companies to Establish Due Diligence Procedures in Global Supply Chains to Safeguard Human Rights and the Environment, July 22, 2021, Library Congress
4. A timeline of the Credit Suisse scandals, Feb 22,2021, The week
5. How well do you know the risks posed by your third parties and supply chain? 2022, PwC
6. Third-party cyber risk for financial services: Blind spots, emerging issues & best practices, April 2019; Bitsight

For more information, contact askus@infosys.com

Infosys®
Navigate your next