Third-Party Risk in a Post-Pandemic World

Third-Party Risk in a Post-Pandemic World

While the COVID-19 pandemic has resulted in unprecedented job loss and economic uncertainty around the world, third-party risk is becoming another important headline for businesses and nonprofits. The economic crisis resulting from the pandemic has exposed a number of issues for historically stable and profitable businesses, ranging from early retirement of key executives to insufficient insurance coverage.

Whether a third-party is part of the supply chain or an outsourced information technology services provider, organizations are increasingly implementing third-party risk management (TPRM) programs to ensure third-parties are not creating additional exposure for them. Successful outsourcing relationships with effective risk management allow the organization to safely procure goods and services and focus on their strategic objectives.

What is TPRM?

TPRM is the process of analyzing and mitigating risks associated with parties outside your organization. These parties can include everyone from contractors providing janitorial services to suppliers of a critical component to your manufacturing process. Risks to third-parties are also risks to your organization. A plan for managing third-party risk protects your organization from unsuspected threats and nasty surprises.

Advantages of TPRM Implementation

Implementing a TPRM program takes time and resources, but the advantages far outweigh any cost to the organization.

- Data Breaches – Data breaches are on the rise with the distraction of COVID-19 and its aftermath. Data breaches can include the use of phishing schemes, denial of service, ransomware or malware, and can cost the organization millions of dollars. Even with cyber insurance coverage, each breach costs organizations thousands of dollars to resolve.

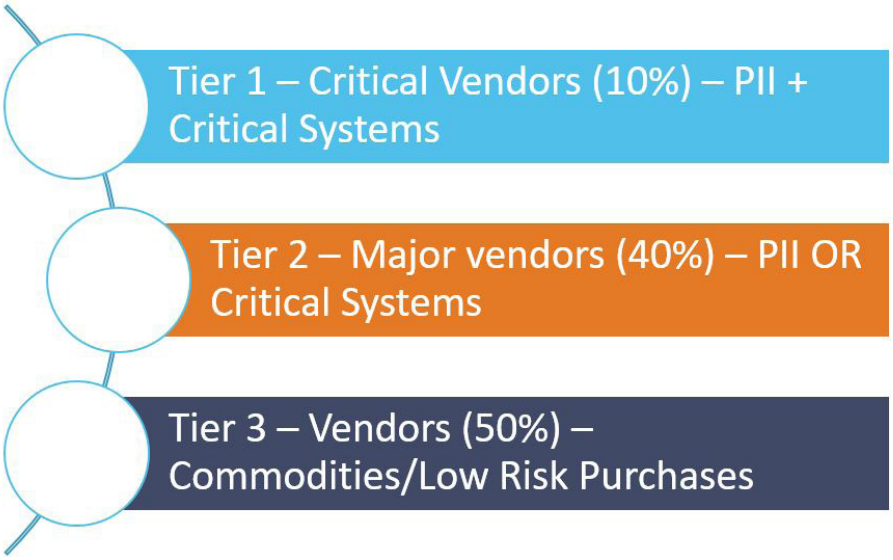
- Operational Failures – What if your beloved outsourced accounting firm (who supported your organization for 20 years) suddenly went out of business? Whether the result of unexpected health problems or even death, who will succeed your longtime accountant who knows everything about your finances? You want to understand your service providers' succession plan before it is too late.

- Vendor Bankruptcy – Your organization depends on a key component in your manufacturing process but that supplier is not answering the phone or replying to emails. With a TPRM program, your organization would know that the company had fallen on hard times and you would have time to identify and procure another supplier for the necessary component. Your manufacturing process stays on-time and within budget.

- Reputational Damage – You read in the news (with everyone else) that your information technology services provider unwittingly helped a foreign country obtain voter registration information. Your organization is connected to this vendor through a legal contract and the relationship made the national headlines. An effective TPRM program would have helped you discovered that the vendor was not maintaining appropriate security measures.

Risk Stratification Guidelines

One of the first steps in any TPRM program is to identify the organization's most critical vendors and perform the necessary due diligence to assess potential risk in that relationship. As part of the onboarding process for a new vendor or supplier, TPRM stipulates that organizations stratify third-parties into risk tiers based on the offered product or service, as well as the third-party's location, countries of operation, and other key factors.



Tier 1 – Critical Vendors (10%) – PII + Critical Systems

Tier 2 – Major vendors (40%) – PII OR Critical Systems

Tier 3 – Vendors (50%) – Commodities/Low Risk Purchases

Risk Assessment

As part of the risk assessment, third-party providers are evaluated in several risk categories. Below are common risk categories and examples of some of the questions used to assess the degree of risk associated with each. Download GRF's Third-Party Risk Management Checklist for more questions from each risk category to consider during your risk assessment.

Example TPRM Risk Categories	**Sample Questions**
Reputation	• Does the third-party's values align with your organization?
Financial projections and review	• Is the third-party solvent? • How many current clients does the third-party have? • How many are significant to the third-party's operation?
Cybersecurity	• Do they maintain baseline security requirements? • Do they have an annual audit performed?
Insurance review	• Does the third-party have insurance, bonding, and business license documentation?
Background checks	• How long has the organization been in business? • Are there negative comments/reviews online about the organization? • Does the third-party outsource any of their services?
Legal review	• Does the third-party have a history of litigation against them or their staff? • Does the third-party operate legally and follow necessary regulatory laws?

Based on the risk assessment, third-parties should be assigned a risk score. This score drives the level of due diligence needed.

Due Diligence for Third-Party Assessment

Due diligence should not just be limited to new third-party providers. It is an ongoing activity, including reviewing, monitoring, and managing communication over the entire vendor lifecycle. As the past few months have taught us, conditions inside and outside of our control can both have a significant effect on operations for any organization. As the buyer of goods and services, you do not want to be surprised when one of your critical vendors cannot deliver on your agreement.

Developing a Third-Party Framework

In general, best practices for any risk management framework include:

Keep in Mind:

The National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) have popular risk management frameworks that can be used together in the assessment process of any third-party risk management program.

- An inventory all third-party vendors your organization has a relationship with (you may need to see who you are paying to find out who they are!);
- An assessment of possible cybersecurity risk exposure from all third-parties;
- Stratifying vendors by tiers by potential risks as described above;
- A system to assess vendors and set a minimum acceptable standards based on the risk assessment guides noted above (as applicable to the specific tiered vendor); and
- Development of contingency plans for when a third-party is deemed below quality or a data breach occurs.

Monitoring and Reporting Process for TPRM

Ongoing monitoring and reporting to your organization's leadership and board of directors will prioritize risk mitigation from your third-parties and facilitate a timely response to risk. To facilitate monitoring and reporting, many organizations employ ongoing analysis and dashboard reporting tools to easily summarize and identify new issues with vendors and suppliers.

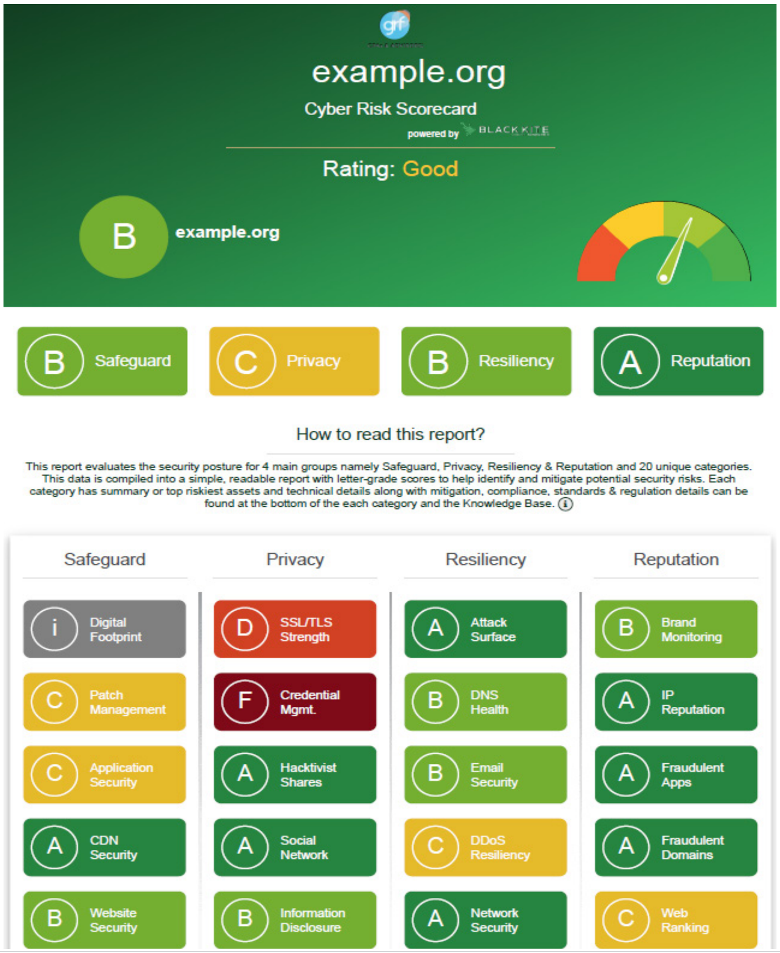
Cybersecurity Assessment & Scorecard

GRF provides clients with a Cybersecurity Assessment & Scorecard that can continuously monitor both the organization and its vendors by providing a "Hacker's View" of vulnerabilities. The GRF Cybersecurity Assessment & Scorecard helps identify possible weakness or vulnerabilities of an organization by evaluating 19 security-related categories and one informational category, as shown below on a continuous basis. Each category provides specific information about an aspect of an organization's cybersecurity posture. The security-related categories are divided into five main groups:

Safeguard: Patch Management, Website & CDN Security
Resiliency: Attack Surface, DNS Health, Email Security, DDoS Resiliency, Network Security
Privacy: Leaked Credentials, Information Disclosure, Hacktivist shares, social network, SSL/TLS strength
Reputation: Brand Monitoring, Web Ranking, IP/Domain Reputation, Fraudulent Domains, Fraudulent Apps
Frameworks: Benchmark against 12 technical frameworks (NIST, ISO, PCI-DSS, GDPR, etc.)

TPRM Benefit:

The GRF Cybersecurity Assessment & Scorecard provides an independent look into your IT environment hosted internally or externally by third-party providers. This assessment will complement their existing efforts by providing a "Hacker's View" revealing potential blind spots. An important part of third-party risk management is holding your third-parties accountable and this has proven to be an excellent cost effective tool as it relates to cyber risk.



How to read this report?

This report evaluates the security posture for 4 main groups namely Safeguard, Privacy, Resiliency & Reputation and 20 unique categories. This data is compiled into a simple, readable report with letter-grade scores to help identify and mitigate potential security risks. Each category has summary or top riskiest assets and technical details along with mitigation, compliance, standards & regulation details can be found at the bottom of the each category and the Knowledge Base. ⓘ

Safeguard	Privacy	Resiliency	Reputation
i Digital Footprint	D SSL/TLS Strength	A Attack Surface	B Brand Monitoring
C Patch Management	F Credential Mgmt.	B DNS Health	A IP Reputation
C Application Security	A Hacktivist Shares	B Email Security	A Fraudulent Apps
A CDN Security	A Social Network	C DDoS Resiliency	A Fraudulent Domains
B Website Security	B Information Disclosure	A Network Security	C Web Ranking

Deliverables:

- Compiled results in a simple, readable report with a letter-grade score to help identify and mitigate potential security risk.
- Summarized technical details along with mitigation, compliance, standards & regulations detail for the top risks items identified.

Summary of TPRM

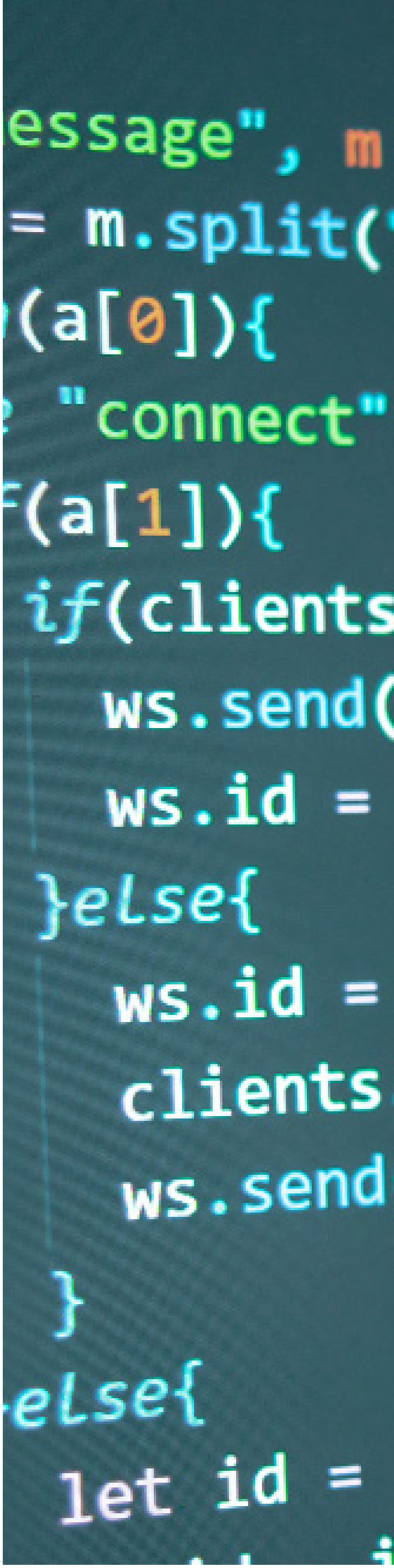
- Pinpoint third-party risks
- Assess your current environment
- Develop a third-party framework based on your organization's context
- Develop risk stratification guidelines to highlight risks by vendor/supplier
- Implement and conduct third-party assessments
- Establish a reporting process

Final Takeaway

Competition is healthy and the best practices that should always govern vendor or supplier selection still apply with TPRM. Use GRF's Third-Party Risk Management Checklist to assist your organization with evaluating a vendor or supplier's qualifications. The questions will help you identify possible risks upfront to make the best possible purchase decision.

GRF's Risk & Advisory Services practice offers guidance for a wide range of business and financial issues to support clients through their most challenging business decisions. Contact Melissa Musser, CPA, CITP, CISA, Principal, Risk & Advisory Services at mmusser@grfcpa.com for more information about TPRM and risk to your organization.

View our Cybersecurity Assessment & Scorecard demonstration here.



Author

Melissa Musser, CPA, CITP, CISA

Principal

mmusser@grfcpa.com
O: 301-951-9090
T: 877-437-4771

About GRF CPAs & Advisors

Our risk experts work with organizations to provide support for complex decision-making over a wide range of business and financial issues.

Services include Enterprise Risk Management (ERM), third-party risk assessment, internal audit, cybersecurity, privacy, fraud support, compliance consulting, and financial systems optimization. For more information on how our experts can support your organization, visit our website at **https://www.grfcpa.com/accounting-services/advisory-services/**.

Headquartered in the Washington, DC metropolitan region serving clients locally, nationally and around the world. GRF CPAs & Advisors is a full-service professional services firm providing clients with audit, accounting,