SHARED ASSESSMENTS

Framework for Managing Third Party Reputation Risk:

Identifying, Assessing, Reporting, Mitigating, and Monitoring

Framework for Managing Third Party Reputation Risk:

Identifying, Assessing, Reporting, Mitigating, and Monitoring

Table of Contents

SHARED ASSESSMENTS

Executive Summary

Reputation is the currency by which organizations work and survive. An organization that actively builds and maintains a positive reputation gains a competitive advantage and improves its credibility if an event impacts that reputation. A consistently positive tone at the top and proactive reputation management can result in better outcomes for building a favorable reputation and managing negative events.

Reputation risk is the potential that negative publicity regarding an organization's business practices—whether true or not—causes a decline in reputation capital that negatively impacts the customer or investor base, results in costly litigation, or otherwise reduces revenue. All aspects of the third party's contracted services have the potential to impact reputation—such as product quality and safety; quality of cybersecurity hygiene, physical security, privacy, and legal practices; and Environmental, Social, and Governance (ESG), such as fair labor practices.

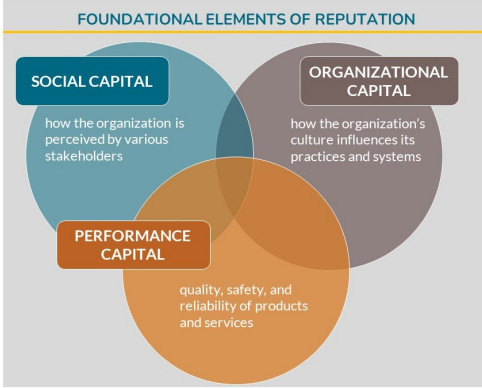
The Reputation Risk Framework principles and practices in this Framework are applicable across all areas of Enterprise Risk Management (ERM) across all organizations and sectors, and can be easily tailored for each individual organization's unique needs and incident management playbooks. Scenario planning and testing event response, reporting and communications, and remediation plans are all basic risk management tenets.

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."

Warren Buffett, legendary business magnate, investor, and philanthropist, chairman and CEO of Berkshire Hathaway

Reputation Capital Can Be Built And Protected

Reputation equates to brand identity and can be impacted positively or negatively through consumer, investor, regulator, or public commentary or reporting through social or other media sources. Naturally, a positive reputation typically provides a competitive advantage that supports market capital, market share and customer retention, and stakeholder confidence. Conversely, negative reputation quickly erodes confidence and can magnify other types of risks in the process.



Capital built through stakeholder relationships—including third parties—is part of the foundation of reputation. The truth for organizations is that they must consider their reputation resilience—their ability to gauge their reputation and recover from reputation impacts—based on a thoughtful, pre-considered plan. Perceptions about reputation change over time. Any gap that emerges between stakeholder expectations and actual performance can result in damage to reputation. Lacking a clear understanding of changes in reputation, the potential impacts of change, and how to manage those impacts only deepens the loss.

Types of Events/Risks that Do the Worst Damage

Reputation risks grew for multinational operations between 2022 and 2023 in the areas of geoeconomic confrontation and interstate conflict with two risks in particular—cybercrime and cyber insecurity, and geoeconomic confrontation—being ranked as likely to be severe over the next two years, as well as over the next decade (World Economic Forum, 2023).

- **Poor company response**, including a failure to take responsibility for an event involving a down chain provider, can itself lead to brand damage beyond the impact of the initial event.

- **Loss of brand confidence** can impact earnings, market share, and the ability to maintain key partnerships. At least 25% of a company's market value is reportedly tied directly to reputation (World Economic Forum, 2023); and 76% of consumers report they would discontinue relations with companies that treat employees, communities, and the environment poorly (PwC, 2022).
- **Data and/or Intellectual Property (IP) breaches and privacy violations** with large fines make the biggest news; however**,** those events rarely exert major long term impacts where sole-source providers are unlikely to lose their customer base; however, their customers (the outsourcers) may in turn suffer significant brand damage in the market and may face significant repercussions, including loss of customer base and/or investors.
- **Crimes committed by rogue employees, agents, third party and other subcontractors** may impact reputation calling integrity into question by running afoul of regulators or law enforcement, including compliance violations (e.g., payments to sanctioned entities, bribery to gain market access, or tax avoidance or violation).

Managing Reputation Using This TRPM Reputation Risk Framework

This framework is built around three key risk management areas—Governance, Due Diligence, and Incident Management and Reporting—and is focused on supply chain and other TPRM-related factors that can result in threats to or loss of reputation. This framework ties into the high level elements of existing risk management programs, and can help build a more robust program for those organizations that do not yet have mature programs.

Companies can track and respond to evolving social priorities and expectations that can impact their reputation by using robust governance and cyber hygiene planning and assessment focused on reputation risk ahead of an event, in combination with ongoing monitoring. Companies can also use this framework construct to identify and act on opportunities to build their reputation capital by making sure:

- Reputation plays a part in third party selection and risk ranking processes.
- Expectations for performance, communication, and messaging are documented and communicated, so staff and third parties are better prepared and can respond effectively when an event occurs.
- Company strategy for reputation management is tied to all lines of defense, providing the ability to work across senior management with an individual pre-assigned company-wide for reputation management.
- Quantifiable, trackable metrics related to organization and third party reputation are established and monitored, such as: changes in third party financial performance; product availability and quality/ performance issues, shifts within geoeconomic risk, or changes within a sector as a whole.
- Scenario planning and testing with as many stakeholders as possible, establishing clear, documented definition of roles and responsibilities in response to situations as they evolve.
- Engaging with groups such as The Responsible Business Alliance and European Financial Reporting Group (EFRAG) that support reputation risk management efforts.

This paper lays the groundwork and helps stimulate thought around managing reputation risk. It provides the opportunity and practical guidance for practitioners, executives, and board members to rally around meaningful organizational reputation risk principles that meet the broad needs of the company and its constituents. While ERM and TPRM programs and practices need to take reputation resilience into account, third parties must also understand how their reputation can impact their ability to do business with the outsourcers and consumers that make up their customers. Improving awareness of and response to reputation issues using clear cut governance, due diligence, and incident response practices allows companies to build stronger reputations over time and recover more readily from negative events.

TPRM REPUTATION RISK FRAMEWORK KEY RISK MANAGEMENT AREAS

- **Governance:** Unify expectations and drive standards across the organization and its third parties by utilizing a formal model that incorporates well-designed, consistently applied policies and processes aligned with the organization's unique needs and risk culture.
- **Due Diligence:** Use quantifiable metrics and tools strategically to detect and track brand sentiment changes including risk assessments, contract and control reviews, financial checks, performance monitoring, issue tracking, and management reporting.
- **Monitoring, Incident Planning and Management, and Reporting:** Planning and response management saves your reputation or sinks it. If an event occurs – when a response is needed – as the outsourcer, own the consequences.

Reputation Risk and Its Impacts

Reputation Capital and TPRM-Related Risks

Reputation is of concern to every risk management practitioner, every executive, and every board member. Yet organizations struggle with defining a common vocabulary or framework. This lack of common vocabulary, as well as the fact that there are many risks that overlap with reputation risk, exacerbate this risk, with possible enterprise-wide impact.

Since reputation is an important component of brand identity, risk practitioners are aware that the time to understand reputation risk and establish and test a plan for responding to risks and incidents such as breaches or service disruptions is *before* an event. Lacking a clear understanding of risk impacts and how to manage them during an event only extends the harm and results in loss of stakeholder confidence. In fact, Gartner reports that for organizations that are able to mount an agile (planned, transparent, and resilience-oriented) response, the time to recover from a disruption is markedly reduced, a factor tied to reputation impacts of any individual disruption event (Gartner, 2021; Dragos, 2023).

From a due diligence and contract management viewpoint, third party related risks that require special consideration include: Geopolitical, Social/Human Rights, and Environmental Concerns; Cyber and Emerging Technology Risks, including IoT and Cloud; Privacy and Data Management Risks; and Artificial Intelligence (AI). These special third party considerations are taken into account in detail in the Shared Assessments TPRM Framework modules (Basics, Due Diligence, Contracts, and Periodic and Continuous Monitoring).

HOW REPUTATION RISK ARISES

Reputation risk arises through other types of risk—including operational risk—and risk-related failures at any level across the enterprise. The company's response to individual events either enhances or diminishes its reputation.

- **Risks around operations, financial resilience, safety, and other domains can result in service disruptions** and failure to meet contract obligations or cyber breaches that can result in privacy or other legal and/or compliance violations.
- **The brand impacts of negative media coverage of those events results in loss of confidence** on the part of investors, consumers, regulators, and other stakeholders that ripples across the supply chain, impacting outsourcing organizations and even entire sectors.
- **This negative change to reputation can result in reduced revenue, regulatory fines, staff turnover and inability to attract quality candidates**, and may adversely affect an organization's ability to maintain existing or establish new business relationships.

Real-World Reputation Risk Examples

The impact on reputation is widely magnified for companies who have not prepared a playbook for incident response, communication, and remediation. For instance, concentration risk can pose reputation risk where the ability to choose a different provider is absent (e.g., banking services, such as MOVEit Cloud or SWIFT; Cloud providers, such as Azure and AWS). Other examples of reputation risk related to third parties include the following.

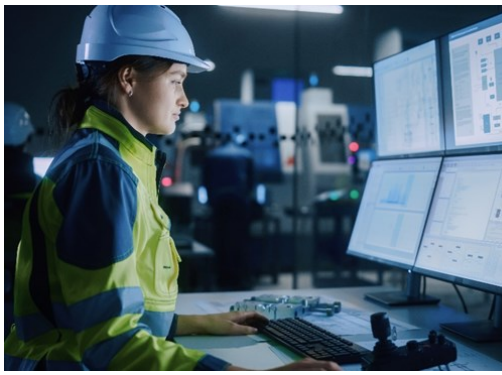
High Risk Domains: Geoeconomic confrontation and interstate conflict rank among senior management in the top five risks for disruption they expect to face in their country in 2023 (World Economic Forum, 2023). Geoeconomic confrontation includes sanctions, trade wars, geopolitical upheaval, and investment screening. Consequently, companies that encounter those challenges face additional reputation risk through third parties located where those disruptions are most likely to occur.

High Risk Sectors: By sector, Manufacturing tops the list for reporting disruptions in its supply chain, followed by Construction, Retail Trade, Wholesale Trade, and Food Services (U.S. Census Bureau, 2023; CEA Calculation; Dragos, 2023). Manufacturing rises to the top again when discussing operational and financial risks, which of course also tie to reputation risk. For example, electric vehicle manufacturers are finding that increased demand is linked to difficulty in sourcing adequate supplies of minerals for batteries, including nickel and lithium. As a result, these manufacturers are working to establish their own sourcing chains that engage directly in mining, which carries risks that can result in increased reputation risk (e.g., financial stability, environmental and labor risks, geolocation risks). This race for key materials results in make-it-or-break-it deals in a notoriously boom-and-bust industry.

Another risk faced by manufacturers is operational technology, which for manufacturers involves sophisticated operations with just-in-time production schedules that increase the need for maximized manufacturing floor up-time. This cycle puts manufacturers, who often play a third party role, in a position to need to be more likely to pay a ransom to return to operations as quickly as possible than other sector stakeholders. Put bluntly, manufacturers are typically large enough to pay substantial ransom, but small enough not to have robust cyber protections at the operational technology level. While this issue is not limited to manufacturing, that sector's importance in the supply chain and need to stay up and running makes them an attractive target. Industry leaders are working to reduce vulnerabilities industry-wide by mitigating the isolation of operational technology (OT) from cyber protections that are already applied to other areas of enterprise technology controls (Dragos, 2023).

KEY CONSIDERATIONS

- Identify potential impacts, so that responsible parties can make informed decisions and better understand potential reputation threats.
- Reputation risk can be hidden and may evolve through a mismatch between what is promised (expectations) and performance.
- Reputation risk is fluid. What matters to stakeholders today may not matter tomorrow. Stay abreast of the reputations of third parties; query stakeholders and stay engaged; and adapt systems, products, and supply chain relationships accordingly.
- Notably, a topic as broad as reputation risk can easily muddy the meaningful difference about how to distinguish between risk and fear or risk and uncertainty.
- Damage to reputation can swiftly unravel years of reputation building, which may be beyond the control of the affected organization(s) to remedy directly.



Reputation Capital Building: Conversely, from a positive real-world management viewpoint, another manufacturing concern—Nucor—stands out for building, securing, and maintaining a positive reputation during its more than 100 year history. They embody a policy of 'integrity and trust to ensure mutual long-term success' in real-life decisions. By actively identifying opportunities to build and sustain reputation capital, they stand out as an example when reputation resilience is discussed in global business forums.

Nucor is known for producing steel, and "central to the concept was the idea of aligning worker interests with management and shareholder interests through an egalitarian meritocracy largely devoid of class distinctions," which has helped the company thrive. By contrast, during the same 34-year period, Bethlehem Steel declined not because of market challenges, but "first and foremost because it was a culture wherein people focused their efforts on negotiating the nuances of an intricate social hierarchy, not on customers, competitors, or changes in the external world." In the end, from 1966 to 1999, Nucor's investors enjoyed a two-hundred fold increase in its investment over the same dollars invested in Bethlehem Steel (Jim Collins, Good to Great, 2001).

Nucor is still making positive news, consistently building its reputation—and that of its partners—most recently by working to produce steel with the lowest possible carbon footprint in a state with outspoken critics of ESG throughout state-level administration (South Carolina Governor's Office, September 28, 2022; Johnson Controls, April 20, 2023). Nucor sees this partnership with Johnson as protecting their operations through sustainable practices, rather than as a political decision; regardless of the push in the state to steer away from business decisions that take ESG into account. The political arguments claim, in part, that ESG reduces shareholder returns. Yet, in 2022 Nucor's efforts boasted $7.61 billion record profits. If a negative event does occur, the strength of Nucor's decades of reputation building would help balance repercussions more than companies that have not taken this care to build and protect their reputation.

Reputation Capital Depletion: The 2010 Deepwater Horizon disaster claimed 11 lives and resulted in the largest oil spill worldwide, with environmental impacts that still exert economic and ecosystem pressure in the Gulf of Mexico today. The fishermen and tourism operators that dominate the region's economy have still not recovered well over a decade after the event. BP received immediate and ongoing backlash from the event, including end consumer boycotts of gasoline at the pump, due in part because the company placed the blame for the accident on its third party offshore oil rig operator, rather than owning the event and its responsibility for this event occurring on its watch.

This one event destroyed any goodwill the company had garnered over the prior 20 years, in which it had built a reputation as a forward thinking player in sustainable practices. To date, they have not been able to fully recover that reputation. Their efforts in sustainable energy are clouded by activist reports of greenwashing and recent announcements backtracking on their much-publicized pledge to cut emissions 35% by 2030. Their stock took immediate hits from the 2010 accident and the company paid then record fines ($4.5 billion) and pled guilty in US federal court to settle related felony counts. The company remains a poster child for what not to do in TPRM and reputation management.

Industry-Wide Impacts: In May 2023, a large regional bank's failure had a cascading impact on the industry as a whole, making it difficult to manage individual company reputation due to their association with the sector. For example, when SVB foundered, Republic Bank got caught up in the industry-level media reporting; and subsequently, and in short order, the impact was seen as a ripple through smaller banks, such as Heartland Trust, even though they did not experience immediate stock loss or failure, as consumers began to take funds out of small banks and move them to larger institutions. This also has created a potential for 'name recognition' reputation risk—if a bank failed, a similarly named bank could be implicated by an implied association—a patent misunderstanding easily propagated through social or other media channels. That unrelated institution could be proactive in distancing itself from the original event; however, their success would not be predictable.

Lack of Market Competition: When major providers maintain a controlling market share or provide a sole service, even a severe reputation hit may not exert a material impact on their market share, their share price, or their business activities. For example, in May 2023, Meta was the subject of U.S. Federal Trade Commission (FTC) action. This was the third time the FTC had taken action against Facebook (Meta's precursor company) for allegedly failing to protect users' privacy. In 2019, Facebook was fined $5 billion in privacy penalty and required to have a third party monitor, install a board privacy expert, and undertake additional systemic governance changes. In the 2023 order, the FTC stated Meta ignored all the agreements the company made during its 2020 privacy order agreement, exhibiting "gross betrayal of public trust."

Emerging Technology and Reputation: The use of generative AI is a final example of third party risk that serves as a warning of the risk to reputation. A sanction and fines were imposed on a firm whose lawyer had submitted a brief that listed six fictitious case citations generated through artificial intelligence, which had not been caught during internal oversight processes at the firm. This legal case could have remained in obscurity except for it being a shining example of "a growing debate about the dangers" of generative AI.

DOUBLE MATERIALITY CONSIDERATION

A double materiality must be assessed for TPRM reputation risk:

- What impact does your company exert on others; and
- What impact do other companies exert on yours?

The metrics used to gauge these risks must be quantifiable and tied to the organization's individual risk appetite and tolerance.

Using a Framework to Mitigate Reputation Risk

Preparedness has become a valuable watchword for corporations, due to the increased reputation risk evident in the 24-hour news cycle and social media that has heightened public and investor awareness of disruptions to an organization's resilience. Many companies, however, miss the point by placing focus on the loss of reputation only after the damage has already occurred.

Placing focus instead on building reputation capital during robust third party due diligence across the lifecycle provides a more mature stance that affords greater resilience for any organization. This norm can be established by unifying expectations and driving standards across the organization and its third parties using a model that incorporates well-designed, consistently applied policies and processes aligned with the organization's unique needs and risk culture.

Regardless of the policies and processes that are established, a solid framework provides defined objectives and goals and establishes a risk posture that can be communicated enterprise-wide and with all third parties. The framework also improves program maturity by supporting a reporting and management oversight model aligned with best practice and appropriate industry and jurisdiction conduct standards. Roles and responsibilities are documented to match framework components. Formal governance and feedback mechanisms are included that are adaptable, keep reputation risk in focus, and allow for monitoring to discover unanticipated or previously unforeseen changes. Reporting processes should ensure sharing of initial and ongoing assessment results at agreed upon regular intervals, with any results that have material impacts being escalated to board level.

REPUTATION RISK DEFINTIONS

Globally across regulations and jurisdictions, reputation risk has historically either been expressly excluded (Basel II) or not been closely defined.

- For instance, UK regulators outline 13 factors firms must consider when selecting their important business services, and includes "*…potential to cause reputational damage to the firm, where this could harm the firm's clients or pose a risk to the soundness, stability, or resilience of the UK financial system or the orderly operation of the financial markets."*

Over time, key principles have tied reputation with other risks.

- UK's Financial Conduct Authority (FCA) and Prudential Regulatory Authority (PRA) SS2/21, and Central Bank of Ireland (CBI) call out risk associated with Important Business Services (IBS) as *"those services that, if disrupted, could cause intolerable harm to a firm's customers or pose a risk to the stability and resilience of the financial system (or financial markets)."*

TPRM Reputation Risk Framework

This framework applies real-world risk-based management principles, demonstrating how an organization can think about, assess, and improve its reputation resilience *before* an event—whether that event's impact may be incidental, material, or long-tail. Governance includes strategy setting and planning. Due diligence and incident management execute on that strategy using specific, hand-selected tactics and tools and establishing pre-vetted and tested processes. Criticality is important in deciding what third (and N^{th} parties) could pose reputation risk, and feedback in response to testing and to learnings from events that occur are used to adapt Governance and Due Diligence.

Governance—Roles and Responsibilities

To be coherent and effective, reputation risk management must be integrated into board and C-suite strategy and planning. To achieve this integration, assigning one individual with sufficient seniority to oversee reputation risk management enterprise-wide is best practice. That individual, with board oversight, conducts operational and growth strategies designed to reduce reputation risk. For example, when managing geolocation risk, organizations that report they are 'extremely concerned' about trade conflicts are managing those risks strategically by: adjusting supply chain and sourcing strategy (40%), shifting growth strategies to alternative territories (25%), shifting production to alternative territories (15%), or delaying foreign direct investment (15%) (Riskonnect, 2023; PwC, 2019).

This individual's role includes setting company objectives and goals; and guiding discussions to establish appropriate related metrics, monitoring, and reporting processes. This role works in concert with risk management functions across the enterprise, including TPRM, procurement, legal, marketing research, communications, HR, corporate affairs, and audit functions. The controls that are put in place work across these functions to ensure information is shared that reveals changes in market conditions and stakeholder perceptions. The examination of reputation indicators is not automatic, even in organizations where there are strong lines of defense and robust TPRM programs in place. Typical lines of defense have been honed in financial services and other highly regulated settings: (1) first line in Line of Business (operational) management; (2) second line in Compliance, Privacy, Information Security, etc. that monitor events inside and outside the view of the first line; (3) third line within audit functions; and (4) a fourth line is recognized as regulators and other key stakeholders as appropriate for the setting.

A concerted focus of reputation risk governance should be placed on supply chain implications. Governance and process development should include discussion of methods for how to approach quantification, controls, and monitoring. Groups such as The Responsible Business Alliance, dedicated to corporate social responsibility in global supply chains, have resources that can support reputation risk management efforts, as does the European Financial Reporting Group (EFRAG), whose mission focuses on financial stability and sustainability reporting standards.

Due Diligence

Strong due diligence processes support a positive reputation across relationships. Supply chain sovereignty depends on a high degree of visibility into N^{th} party suppliers in order to identify critical dependencies and apply a consistent set of principles for monitoring parallel or intentionally redundant processes and other resilience indicators across inbound and outbound supply chains. Due diligence metrics (KPIs and KRIs) should be tied correctly to potential reputation risk in order to effectively gauge impending shifts in perceptions or incidents that will directly affect reputation.

The Metrics section provides guidance on how to select measures that are aligned with the organization's risk appetite and tolerance and how to monitor those metrics. For teams that are updating existing plans or building their first TPRM due diligence and assessment program, significant practical detail and practitioner tools on these topics are available at:

- TPRM Framework – Assessment and Continuous Monitoring Module for incident planning, communications, reporting, and management techniques and tools.
- Shared Assessments Standardized Information Gathering (SIG) provides solid guidance and cross-industry metrics built to be tailored to organization-specific control frameworks and risk appetites.
- Discussion on how to set and document risk appetite can be found in Shared Assessments TPRM Framework – Introduction, Contracts, Due Diligence, and TPRM Basics modules.

Stakeholder Engagement

Reputation depends on being clear about related goals and values and then acting in accordance with those expectations. This can be difficult to achieve across a single organization, much less its third party relationships. Setting contract expectations is key, as is ongoing monitoring of publicly available information that helps identify potentially negative impacts to reputation. Adjust messaging and planning to respond to findings as they evolve and keep key stakeholders informed in a timely manner.

DUE DILIGENCE MUST

- **Include reputation as part in third party selection and risk rating.**
- **Engage appropriate stakeholders**—both internal and external.
- **Include solutions that can be applied to mitigate reputation risks** and reduce their impact.
- **Identify, assess, and monitor quantifiable metrics**—for the organization and its third and identifiable N^{th} parties (screening, analytics, mapping for legal, security, privacy, ESG and other reputation-related risks).
- **Help third parties better prepare for and respond** quickly and effectively to events.
- **Use Playbooks developed specific to the organization** that guide performance of third party reputation risk management.

Input for assessments and metrics planning requires early and ongoing stakeholder feedback during discussions around reputation risk, as well as scenario design, testing, and adaptation. This feedback enhances success in market and stakeholder understanding of their role around if/when a reputation risk event occurs and their place in a response if one is undertaken. This proactive engagement also demonstrates transparency, improves relationship building, and helps to keep an organization focused over time on its stated goals (i.e., the expectations it has set through its in internal and external communications). Roles for staff contact (and/or private company communications/managers) should be readily available on the main (outsourcer) company website and social media pages.

Third parties play the role of both external stakeholder and a key impact point for influencing the outsourcer's reputation. Soliciting feedback helps practitioners understand where resources are best utilized before, during, and after events. For instance, there is no point in stakeholder engagement during an event if the organization is a sole-source provider and the stakeholder cannot provide feedback that would alter the company's response to reputation damage. However, where outsourcers do have access to other products, markets, etc., then surveys, meetings, press releases, and other statements that can be accessed externally can be very important.

Metrics—Quantifying and Assessing TPRM Reputation Risk

Reputation risk management benefits from establishing clear, quantifiable benchmark metrics for third parties before onboarding. Monitoring changes to those metrics across the lifecycle can provide insight into how third parties can contribute to reputation risk—and where transparent enough to identify them, the Nth parties to those relationships that may be critical.

Reputation risk can arise from events that take place across any risk domain enterprise-wide

TPRM Reputation Risk Framework High Level Program Categories *							
Governance, Policies, Standards, Procedures	Operations, Locations, Systems, Sustainability	Vendor Risk Assessment Process	Third Party Contract Development, Adherence & Management	Human Resources, Skills and Expertise	Product Quality	Tools, Measurement and Analysis	Communication and Information Sharing

Examples of Potential Reputation Risks							
Operational or Other Processing Failures, e.g., Supply Chain Disruptions, Distribution Failures, Fraud	Negative Media and Social Media Coverage or Disinformation	Customer Service Outages	Ransomware / Cyber Attack	Environmental Hazards	Greenwashing, Greenhushing (purposeful or unintentional)	Stakeholder Activism	Loss of Intellectual Property, Data Breach

Examples of Potential Reputation Risk Impacts							
Revenue Loss	Regulatory Fines	Talent Loss	Talent Acquisition Difficulty	Loss of Customer Base	Loss of Investor Confidence	Class Action Suits	Loss of Licenses to Operate

Examples of Related Indicators			
Changes in activity (e.g., litigation, regulatory fines, product issues, changes in performance and delivery, customer service incidents, financial performance)	ESG issues, including reports violations of Key Principles (i.e., human rights, labor, corruption)	Measures of shifting geoeconomic risks for critical third parties (e.g., natural disasters, geopolitical or other social disruptions, economic shifts, disruptive changes in technology)	Market shifts indicating changes in stakeholder perceptions within a sector

Table 1: TPRM Reputation Risk Framework Categories, Risk Examples and Impacts, and Related Indicators
* Shared Assessments Vendor Risk Management Maturity Model (VRMMM) https://sharedassessments.org/vrmmm/

Measuring third party reputation risk is challenging since:

1) outsourcers rarely have real-time access to supplier environments; and
2) increasingly complex provider networks have created substantial friction for outsourcers trying to gauge the overall control adequacy and cyber hygiene of their supply chains.

Continuous monitoring and feedback loops reduce that friction by providing the situational awareness necessary for effective reporting and control management as reputation risk evolves. This approach is supported by evolving global regulations that increasingly dictate outsourcers know, manage, and report on their fourth and N^{th} parties. Once clarity is gained through analysis of the results of initial assessment and quantification, better controls for those risks can be devised.

The table below shows selected examples of reputation risk, potential impacts, and related organization and third party indicators that can guide metric selection.

Risk can be demonstrated quantitatively using mathematics and actual or predictive data modeling. Appendix B: Risk Quantification – Approaches and Techniques provides detailed guidance regarding quantifying systemic risk across disciplines in ways that align with measuring reputation risk, since reputation arises through all other types of risk—including operational risk—and risk-related failures at any level across the enterprise. There are many actuarial models for risk management especially in the insurance industry; however, there are also specialized quantitative risk management models for risk management professionals in other areas such as cybersecurity. The FAIR Institute Methodology for quantifying information risk is one example of a number of methods that have gained traction within the third party risk management space.

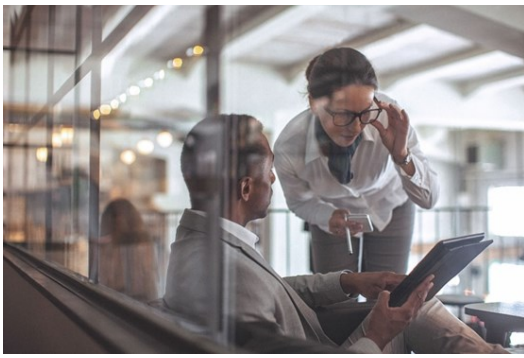
Monitoring, Incident Planning and Management, and Reporting

Once organization-specific metrics have been established, the business of tracking and predicting reputation risk using those metrics can be achieved in part through the use of Risk Assessment Services (RAS). These services utilize publicly available information to compile a risk profile that can provide insight into potential threats prior to onboarding, as well as emerging threats throughout the third party lifecycle.

USEFUL CONSIDERATIONS WHEN BUILDING SCENARIOS AND METRICS

Reputation risk will be higher where geoeconomic risk indicators escalate and a higher volume of third parties (and/or their fourth parties) operate in that area.
Reputation risk will be higher where concentration risk or sole source risk are ranked high.
Reputation risk will be higher where a class of vendors involves a greater volume of the supply chain or source chain.
Reputation risk will be higher when the risk in a number of key risk indicators is high across risk domains.
Reputation risk will be lower where redundancy can be built into the supply chain or sourcing chain.
Reputation risk will be lower where tactics are employed that reduce high risk practices and improve flexibility in supply chains and source chains, such as reshoring, nearshoring, and redundancy.

Changes that monitor investor and financial analysis of individual companies, markets, geopolitical zones, and other risks can be matched to an organization's own risk appetite and tolerance. Pending changes in regulations can be monitored as well to assist in understanding those evolving risks.



In part, it is important to determine how to discover and document:

1) all the parties in the organization's supply chain or source chain;
2) the organization's actual and potential N^{th} party exposure;
3) an understanding of the materiality of those exposures; and
4) curing of issues as they are identified.

Detailed guidance and examples for quantifying and reporting reputation risk are provided in the Appendices. Appendix B: Risk Quantification – Approaches and Techniques; Appendix C: Designing Your Roadmap for the Real-World Using Scenario Planning; and Appendix D: Calculating and Reporting Reputation Risk.

Monitoring

Identifying organization-specific key risk indicators (KRIs) and then matching those to key performance indicators (KPIs) allows an organization to gauge and monitor its reputation risk. Changes in KPIs provide useful insights, including those derived from publicly available reports of financial performance, ESG, quality of services, and non-compliance fines. When compared against enterprise-level KRIs, these metrics reveal shifts in: (1) stability of third parties or sectors; and (2) perception shifts around public/consumer/government, which can drive reputation positively or negatively. Compliance and Risk Governance platforms and RAS are readily available.

Incident Planning and Management

An organization's response to an event is highly determinative of the impact to reputation. The quality of that response is directly tied to the organization's incident planning, testing, communications, and training. Curing previously issues identified during testing or an incident provides a more robust response, as well.

The impact to reputation may be magnified even when the initial severity of the incident may not seem high. For instance, in 2023 Rensselaer Polytechnic Institute's third party maintenance contractor cut power to a freezer compromising 20 years' of solar panel development research, and resulting in legal action against the third party. " The institute's legal team says the company that employed the cleaner failed to adequately train their employee." Yet, it is Rensselaer's name that is in the press, not the contractor's.

Each reputation risk event is unique. Incident response planning involves a focus on wide-ranging potential impacts and messaging needs. External processes including economic, environmental, dependence on third parties, and technology are becoming increasingly impactful. Many companies assume that their crisis/incident planning serves in all circumstances; however, plans not designed to manage reputation risk will not suffice during an incident. The incident management plan must specifically address how communications are deployed, by whom, in what media, what the messaging objectives are, and the frequency based on incident and response type is to be.

A formalized incident management program that is rigorously tested and updated is essential.

- **Monitor and Act on relevant information** about the reputation of the organization and that of key third parties as that information evolves.
- **Determine the major impacts** to establish what actions are appropriate when an event occurs. Previously built positive reputation typically reinforces the brand and can support messaging and response to mitigate future negative impacts.
- **Employ consistent messaging across all channels**, including customer service interactions, social media, press, etc., as deviations make weathering the response appropriately more difficult.
- **Apply quantitative reporting to third party events** that requires the outsourcer's response.

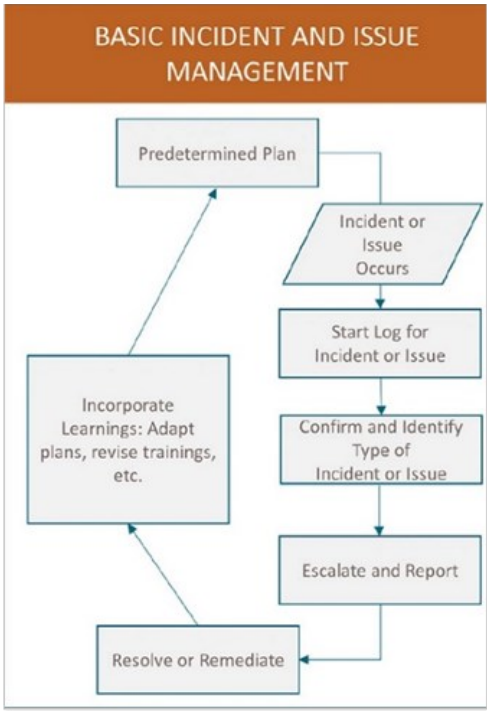
The key to using metrics for incident planning and management lies in creating a unified vision based on real world observations. Scenario planning and testing need to take place that specifically includes testing for reputation risk response. Reputation costs such as the inconvenience of a bank customer transitioning to another provider may be low, as most consumers would accept a credit monitoring offer as a means to mitigate their risk if they are exposed through a third party breach. However, reputation risk for a manufacturer may be high if their customer cannot receive goods in a timely fashion or within a pre-defined recovery time tolerance level because of a ransomware or other attack. Using these types of metrics provides a larger view of the event inputs, throughputs, and outputs during scenario testing. See Appendix C: Designing Your Roadmap for the Real World Using Scenario Planning for additional information on scenario planning and testing.

Trackable Quantifiable Resilience Sustainability Metrics	Examples
Third party and Outsourcer Organizational Indicators	Financial performance, corporate responsibility (ESG), quality of services, and non-compliance fines; and assign a ranking for each of those metrics.
Changes in Activity	Increases/decreases in call center calls, changes to customer base numbers or demographic types, cyber risks (breaches and vulnerabilities).
Geoeconomic Risks for Critical Third Parties	Growth or reductions in operations, sanctions, global and interstate conflicts.
Industry Loss of Confidence	Track industry loss of confidence in an entire industry charting level changes where ripple effects of reputation risk may be demonstrated in a more dramatic way. For example, monitoring rating and other near real-time services, such as Information Sharing and Analysis Centers (ISACs).
Changes within an Industry as a Whole	When the situation is a loss of confidence in the industry this is not the act or admission of any one player, making that perception elusive and difficult to predict. Components of an industry can be viewed, such as increased complaints showing perception changes that the product/service is of low value or is high risk to use.
Apply quantitative reporting when a third party event does occur that impacts the organization	During an event, there are impacts on the outsourcing company that can be tracked, such as cancellations, drops in year-over-year or quarterly revenues, and other typical financial and performance measures).

Table 2: Trackable, Quantifiable Reputation Risk Resilience Sustainability Metrics and Examples

Communications and Reporting

Communicating reputation risk across the organization relies on robust risk quantification techniques to define possible deltas against an organization's unique risk appetite. Good metrics help to prioritize investments in reducing risks. Robust risk quantification techniques infuse reporting with reliable data and provides the basis for informed decision making and mitigation, and provides a solid foundation for preparedness. Gap analysis is used to adjust metrics where initial assessment results vary from testing or real-world event results. Information needs to be shared broadly across various functions, including senior management and board. Reputation risk threats can be missed if this information is not shared in a way that provides ongoing transparency between departments enterprise-wide. For example, Operations may monitor supply chain health for potential disruptions; Communications may monitor media; and Legal/ Compliance may monitor changes to regulations.



Reporting can incorporate risk ranking (or tiering) using a scale for risk and weights for risk type or individual third party. Tying those weights to specific goals aligned to the organization's risk appetite may provide a clearer view of what reputation risk factors exist for that third party relationship.

Reporting should flow top-down and bottom-up. Reports target specific internal audiences (e.g., board, senior management, risk committees, control functions, and business owners), as well as external audiences (as in the case of Sustainability and ESG reporting). Tailored materials include the level of information and detail required for each stakeholder group to fully understand the implications of report results. Share initial and ongoing assessment results at agreed upon regular intervals, with escalation of monitoring results when reputation risk metrics demonstrate a material change (positive or negative).

LEGAL CONSIDERATIONS TIE CLOSELY TO REPUTATION RISK

The U.S. Department of Justice 2023 guidelines for prosecutors provides some boundaries for reporting and communications: *"Is the company's compliance program well designed? Is it being applied earnestly and in good faith? Does the compliance program work in practice? While these questions may be addressed by compliance and risk management executives, other departments such as IT, legal, human resources, and records management can play a key role in the design, implementation, and enforcement of these policies and procedures."*

Conclusion

Using the reputation risk framework outlined in this paper can help companies do a better job of understanding, assessing, building, and managing reputation capital and reputation-related threats that may arise through relationships within their supply chain.

Building and Protecting Reputation: The impacts to reputation that can be posed by third party and other key relationships mean that programs and practices—both outsourcer's and provider's—must account for and be designed to improve reputation resilience. Performing effective due diligence and continuous monitoring throughout the third party lifecycle can help reduce an organization's reputation risk exposure.

Measuring Reputation: The quantitative metric methods, ongoing tracking, and well-planned and executed response included in this framework provide a roadmap for measuring reputation risk, previously considered unquantifiable. This allows companies to adopt a proactive response to reputation management. Detailed guidance and examples for quantifying and reporting reputation risk are provided in the Appendices.

Governing for Reputation Risk Management: To be effective, a positive tone at the top has to be demonstrated and communicated consistently organization wide to reinforce good risk culture. Placing focus first on building reputation capital through robust due diligence utilizing a formalized governance model that includes risk rating in third party selection prior to onboarding and throughout the third party lifecycle, as well as targeted scenario testing and modeling, provides a more mature stance that affords greater resilience for any organization. Applying this same approach enterprise-wide provides even greater benefits to the organization, its investors, customers, and other stakeholders.

Monitoring, Incident Planning and Management, and Reporting: TPRM resources are often focused primarily on documenting controls for individual third parties and analyzing the risks posed by those relationships. It is important to recognize and learn to incorporate reputation risk elements that are material for the organization into reporting, communications, and incident management.

To achieve robust reputation risk management, an organization must have:

- **Risk appetite statements and frameworks help determine what type of risk quantification metrics are appropriate for each stakeholder. These statements and frameworks** improve understanding of significance of risks and how those risks are measured and managed.
- **Access to reliable data that can serve as the basis for a risk analysis**. Historically, this data has been scarce in the third party space. The delisting of public companies purchased by private equity firms exacerbates the difficulty in gaining useful financial information.
- **Ongoing TPRM and ERM program evaluation.** These evaluations are important to ensure that the potential impact of all risk types are understood. Assigned risk management leaders in each department who are responsible for identifying and communicating risks, so the impact of evolving risks can be measured.
- **Playbooks.** Playbooks for each type of event that can occur enable faster, appropriate incident responses. Playbooks should be regularly updated based on scenario testing and real-world events or incidents.
- **Feedback mechanisms.** Feedback mechanisms throughout the organization's risk program and quantification processes are essential to ensure continuous improvement.

Reputation risk is a direct consequence of events that occur from risks across all areas of enterprise risk management. Reputation risk may be heightened through third party relationships, which may include risks that are opaque to the original outsourcer. Organizations that are heavily siloed may have greater challenges in recognizing this type of risk due to a lack of communication across silos. The breadth of risks that can impact reputation risk lays bare the overarching need for Third Party Reputation Risk Management to be a key guide in ERM. By assigning the role for reputation risk management at the C-suite level, existing resources can be leveraged; and information shared across departments, so that metrics can be established, assessed, monitored, and changes observed over time and events can be responded to in an agile and positive way to benefit the organization.

Appendix A: Selected Terms

Complex Supply Chain Management (See also Supply Chain Risk and Supply Chain Risk Management): In an outsourcing context, the strategies, techniques, and processes employed to ensure that each element of an outsourcer's supply chain meets the outsourcer's risk standards and are executed down the entire chain in accordance with overseeing the outsourced critical function is effectively supervised. The management of outsourcing complexity in the supply chain is a subset of complex supply chain management. Complex supply chain as a term applies to all elements required to bring a product or service to market. For instance materials, parts for assembly, assembled parts, final products/services, distribution/ transportation/marketing channels; where a change in any element may impact other elements in the chain. Contractual contexts exist regarding the chains involved and how outsourcers protect themselves from the risks posed. Adapted from EBA Outsourcing Arrangements 2019.

Nth Party Management: An organization's approach to managing risk associated with today's complex outsourcing chains, which increasingly extend beyond third parties. Fourth parties (the outsourcer's third party's third parties) are common today, but regulators have identified as many as 20 organizations in a single financial service outsourcing chain. Outsourcers inherit the risk associated with their expanded supply chain, and mitigating those risks necessitates a far-reaching security strategy that safeguards data and other assets from uncharted risks and vulnerabilities.

Enterprise Risk Management (ERM)
Enterprise Risk Management (ERM) is an integrated and continuous process for managing enterprise risks - including strategic, financial, operational, compliance, and reputational risks - to minimize unexpected performance variance and maximize intrinsic value. This process empowers boards and management to make more informed risk/return decisions by addressing fundamental requirements with respect to governance and policy (including risk appetite), risk analytics, risk management, and monitoring and reporting.

Enterprise Risk Management (ERM) is the culture, capabilities, and practices, integrated with strategy setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value. ERM manages risk through: (1) Recognizing culture; (2) Developing capabilities; (3) Applying practices; (4) Integrating with strategy setting-setting and performance; (5) Managing risk to strategy and business objectives; and (6) Linking to value.
Shared Assessments Guide to Risk Domains introduces and defines other critical and current risk domains: https://sharedassessments.org/risk-domains/.

Environmental, Social, and Corporate Governance (ESG)
Environmental, social, and corporate governance (ESG) is a set of standards designed to measure and improve how a company affects the planet and its people. ESG is important because customers, governments, and other stakeholders increasingly evaluate an organization's performance against these criteria, not just financial results, and socially conscious investors increasingly use ESG criteria to screen potential investments. Collectively, these criteria evaluate a company's stewardship of the planet, its communities, and its people.

Reputation Risk: The risk arising from negative perception on the part of regulators and other stakeholders that can adversely affect an organization's ability to maintain existing, or establish new, business relationships and continued access to sources of funding. Some authorities do not consider reputation risk to be a subcomponent of operational risk. Rather, reputation risk is viewed as being the result of operational failures. Adapted in part from: Basel 30.29. 2020. https://www.bis.org/basel_framework/chapter/SRP/30.htm.

Risk Appetite: a) Risk Appetite: The level and type of risk an organization will take in order to pursue its strategic measurable objectives; b) Risk Appetite Statement: A documented definition of the organization's risk appetite.

Risk Domains: Risk domains are categories or focus areas of defining control areas that help to guide third party risk management (TPRM) programs. Risk domains are used to scope or frame types of controls that should be evaluated during a third party risk assessment. The ever-changing risk and regulatory environment define risk domains. A particular risk may be more relevant to third party risk management based on the nature of the services being outsourced.

Risk can be categorized into four key areas.

- **Governance and Risk Management** include these domains: Compliance Management, Enterprise Risk Management, Environmental, Social, and Governance (ESG), Human Resources Security, Information Assurance, Nth Party Management, Privacy Management
- **Information Protection** includes these risk domains: Access Control, Application Security, Cloud Hosting Services, Endpoint Security, Network Security, Physical and Environmental Security, Server Security
- **IT Operations and Business Resilience** include these risk domains: Asset and Information Management, IT Operations Management, Operational Resilience
- **Security Incident and Threat Management** include these risk domains: Cybersecurity Incident, Management, Threat Management.

Risk Appetite Framework
The core instrument for defining and aligning risk sensitivity and metrics in a specific business context across an organization. The Risk Appetite Framework operates at all levels of an organization (Board, C-Suite, Business Unit, etc.) and must include an effective risk infrastructure that integrates the organization's strategy using key metrics that tie risk to business objectives for driving and evaluating TPRM program effectiveness. The framework should incorporate the roles and responsibilities and the implementation of various risk management tools and documentation of risk policies. Actionable risk tolerance metrics must be included. Adapted from James Lam, 2017.

Risk Management Framework: The Shared Assessments Program's Third Party Risk Management (TPRM) Framework is designed to provide guidance for organizations seeking to develop, optimize and/or manage Third Party Risk by incorporating a wide range of best practices into their risk management program. The Framework also provides guidance about how to implement meaningful incremental improvements in TPRM practice maturity in organizations where resources may be constrained.

Risk Tolerance: A threshold of risk an entity is willing to assume in order to achieve a potential desired result. Tolerance measures the organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives. Risk tolerance can be influenced by legal or regulatory requirements. In this Framework, we use this term with the assumption that risk tolerances can be defined with sufficient precision to be translated into actionable metrics. Note: Risk tolerance can be influenced by legal or regulatory requirements. Retrieved and adapted from CNSSI 4009-2015, NIST SP 800-160 [Superseded], NIST SP 800-32 under Risk Tolerance, NIST SP 800-137 and NISTIR 8183 under Risk Tolerance under Risk Tolerance (2018). https://csrc.nist.gov/glossary/term/risk-tolerance.

For additional TPRM-related terms referenced in this framework, please see:
https://sharedassessments.org/glossary.

Appendix B: Risk Quantification—Approaches and Techniques

Though metrics is considered by many the squishy part of third party reputation risk assessment and monitoring, quantifiable metrics are achievable and trackable.

Understanding the organization's documented risk appetite and associated risk tolerance at the business unit level is a prerequisite to any quantitative analysis of risk. Quantitative risk metrics allow organizations to effectively monitor changes in reputation status of third parties (and where transparent enough to identify them, the N^{th} parties to those relationships that may be critical as well). Quantification can be based on level of business disruption, potential response costs, legal and external personnel, regulatory fines where non-compliance is part of the scenario, consumer services costs (e.g., credit monitoring), and technology recovery costs.

Using static qualitative measures such as point-in-time inherent risk assessment techniques places an organization in a reactive stance. In ideal circumstances, risk quantification combines point-in-time with continuous monitoring techniques providing organizations with the opportunity to adopt a proactive, better informed, position; from which they can more accurately evaluate reputation risk and anticipate the potential impact of events as they evolve.

Reputation risk spans the gamut across multiple domains – physical, cyber, information security, privacy, concentration, regulatory compliance concerns, governance, threat and incident management, and operations management. Better risk quantification has the potential to support third party risk managers, ERM program staff, and senior management who must prioritize and focus limited resources in the most efficient and effective way.

When compared with generalized heat maps that are often based on qualitative approaches, quantification promises a more precise basis for gauging risk and the efficacy of an organization's TPRM program. While frameworks such as National Institute of Standards and Technology (NIST) or International Organization for Standardization (ISO) to guide risk-based policies, these frameworks do not provide sufficient guidance on measurable metrics to estimate the potential probability and impact of reputation risk exposure. The challenge is even greater in third party environments.

Ideally, risk quantification techniques used to identify the potential loss magnitude from internal and third party related exposures should:

- Utilize quantification methods that are materially acceptable, reasonably useable, viable over time, and easily integrated into the organization's processes.
- Focus on factors that should be examined to best align resources and controls to serve the organization's risk practitioners.

Reputation risk may increase through events that include data breach, ethical violation, or failure to deliver—all of which can be made visible during monitoring. Three examples of indicators of reputation risk are:

- **Company actions** (non-compliance, legal, poor-quality product/services, ESG, poor brand representation).
- **Staff/third party action**s (misconduct, service/supply disruptions, breach).
- **External actions** (negative social media, articles, reviews).

Robust monitoring and reporting includes metrics that gauge these types of events and define when, how, and to whom changes are reported when reputation risk is considered high.

Methodologies

In general terms, risk is the likelihood that unplanned events will occur and impact the achievement of strategy and business objectives. Risk is commonly presented either qualitatively or quantitatively. Either measure of risk is a measure of the combination of the extent to which an entity is threatened by a potential circumstance or event on organizational operations (including mission, functions, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat; and the likelihood of that threat occurring (Shared Assessments TPRM Glossary, 2023).

- Qualitative Risk is often used to demonstrate results of a quantitative risk analysis in a more relatable manner, for example, reporting to executive management or the organization's board or governing committee. Risk described qualitatively may be expressed in terms of magnitudes in relation to other similar events or states. For example, a rating of Low, Moderate, or High is a qualitative measure defined according to however an organization defines those magnitudes. Or risk could be described in terms of effect on operational or financial health. Risk can also be qualitatively demonstrated in terms of duration of impact and the magnitude of efforts required to recover normal operations or financial health.
- Quantitative Risk can be demonstrated using mathematics and actual historical data or predictive data modeling assuming the quality of data is acceptable (an ongoing known issue in third party risk management). Numeric quantification of the potential consequences of a risk event provides an objective measure to describe that risk. A common and fundamental measure of risk is the equation: Annual Loss Expectancy (ALE) = Annual Rate of Occurrence (ARO) x Single Loss Expectancy (SLE). Annual Loss Expectancy (ALE) is the estimated amount of annual loss predicted based on historical and predictive factors. Annual Rate of Occurrence (ARO) is the estimated number of times a loss event of a certain kind that occur over a year. Single Loss Expectancy (SLE) is the amount of loss in local currency expected for one occurrence of a loss event.

It is important to remember that the outputs from any statistical approach may well be interpreted differently depending upon organizational priorities and philosophies.

The rate of occurrence of an event within a distribution might be viewed in several ways given a single high quality predictive data set on which an assumption is based. Fundamentally different philosophies that are based on an organization's unique risk tolerance(s), may also yield more variation in risk metrics when switching quantitative approaches that use the same data and underlying risk tolerances.

For example, for a given data set and quantitative approach:

- One organization may be quite happy to base its actions on a "most likely" outcome assuming the data suggests a clear predictive perspective.
- Another firm might choose to act on the basis of a different occurrence likelihood from the same data set, choosing to take action given a "once in a career" event (highly unlikely, but still; possible) occurrence will be seen more frequently.

Understanding risk appetite and associated risk tolerance at the business unit level is therefore a prerequisite to any quantitative analysis of risk.

Precision based models for quantifying specific areas of operational risk to measure risk across disciplines (beyond cyber risk) against complex scenarios are few and far between. The main methodologies currently being employed are techniques developed in the insurance industry for cyber insurance and the FAIR™ Approach. Two examples that may help practitioners in framing discussions around reputation risk are:

- The black box problem in cyber insurance underwriting reflects ratings and generative-AI problems that organizations may face when quantifying reputation risk. Insurance underwriting is based on many factors, such as the industry sector, the size of the company, annual revenue, and other fundamentals, as well as the organization's cybersecurity controls. Actuarial data on the likelihood and impact of cyber events is still insufficient, or of insufficient resolution, for making specific underwriting decisions with high confidence. In any case, the specifics associated with cyber insurance underwriting are not transparent to the outsourcing organization being insured. Adding to this "black box" problem is the growing understanding within the insurance industry that its own scenario-based approach is not always effective in quantifying losses and needs to be strengthened.

- In the Factor Analysis of Information Risk (FAIR) Approach, a move has been made to measure risk using analytic functions that require solid mathematical functions and reliable data inputs (i.e., do not perform math or ordinal scales). This contrasts weighted values, which are subjective qualitative descriptors that are not based on mathematical function. This method has been applied in a wide variety of settings, including third party risk management; and is considered a viable quantitative model for information security and operational risk. (Fair Institute, 2021). Although the FAIR methodology provides a framework that allows the user to set criteria for data collection and analyze risk scenarios from historical data and user input, its utility in the third party space is only as good as its input data, sometimes an issue when dealing with third parties and a bigger concern with complex supply chains.

An organization's risk appetite statement documents at a high level the acceptable level of risk that a board and/or executive management agree is appropriate given the organization's business objectives.[1] The development of a clear and documented organization-level risk appetite statement and the acceptable risk threshold (risk tolerance) metrics that flow from it is typically a top-down and bottom-up iterative process. This process drives program development and processes. [2]

In addition to continuous monitoring and Risk Assessment Services (RAS), robust third party risk assessments include attributes that can be documented and quantified across the range of selected benchmark metrics chosen for the organization. For example, compliance effectiveness is generally evaluated across four areas, listed below. The presence of absence of attributes for that area can be rated on a range or as a plus/minus factor that contributes to an overall score which is then viewed over time.

- **Administrative Policy Compliance:** Written corporate (outsourcer and third party) documents that dictate principles, intent, and policies.
- **Technology Compliance:** All parties should have mechanism(s) to catalog policies, confirm acceptance, testing, and assure adherence, and where needed assure remediation.
- **Regulatory Compliance:** Contract requirements (Service Level Agreements – SLAs) cannot be relied upon solely to satisfy regulatory requirements; while third party providers must be held to the same regulatory standards as their customers, those outsourcers cannot outsource the risk associated with regulatory standards.
- **Contract Compliance:** Procedures should include mechanisms to review existing contracts against compliance requirements. Contract renewal, revisions, issues, and regulatory changes are all triggers for examination of contract compliance.

For additional discussion and information, please see around Third-Party Risk Quantification: Techniques for the Extended Enterprise, available at: https://sharedassessments.org/paper/risk-quantification-techniques-for-the-extended-enterprise/.

Appendix C: Designing Your Roadmap for the Real-World Using Scenario Planning

Field-proven, best practice feasibility guidelines can serve as the basis for modeling scenarios for reputation risk exercises. Examples of how these methods are applied for reporting within a reputation risk setting are included in Appendix D: Calculating and Reporting Reputation Risk.

- Methodologies that model operational risks, such as credit risk, can be leveraged for modeling reputation risk. Forensic information (e.g., expert witness, peer reviewed reports) can help guide model development.
- Custom built models can be used to construct realistic scenarios that include specific use case tracking for each unique setting an organization faces.
- *At minimum, document reasons for selecting parameters in detail in a trackable format to enable proper comparison against scenarios.*

Examining a specific type of threat can yield a reasonable assessment of its impact in real life. However, an individual scenario is just one element of risk. Incorporating many known and unknown scenarios into a risk impact model is a high bar to clear for a risk modeling program. Viewing what senior management needs to know to gauge risk can be helpful. The two main questions are: (1) what can happen?; and (2) what would it cost the organization if that event did occur?

Mathematical distribution curves are favored to express risk and potential loss. This type of curve compares the likelihood of an event occurring with the financial impact of that event. This type of curve is useful in many settings such as natural disasters and other unlikely, but devastating events. It reflects the fact that for many risks, impact is greater for unlikely events, and events that occur more frequently have lower impact.

Building a reliable loss distribution curve depends on the availability of historical data, which is often lacking with operational risk. Threats such as: external (e.g., economic, environmental), process (e.g., dependence on Third Parties, skills gaps) and technology (e.g., cybersecurity, scalability) are becoming progressively more destructive, with increased attack sophistication from nation states and cyber terrorists against critical infrastructures and systems. See Appendix D: Calculating and Reporting Reputation Risk for an example of Loss Distribution S-Curve.

The precision of each quantitative measurement in each area will also differ depending on the amount of information available for that component. Strive for the most accurate representation reasonably possible for that component. The goal is an income margin that can be applied to the analysis. In each of the areas for examination, a cost model will apply. For example, how much attorney time might be required (based on cost and number of hours for litigation); how much would restoration of manufacturing operations cost to help restore reputation (based on down time and cost to restore systems and bring the operations back online); if intellectual property (IP) is lost, what would that cost the organization in theory.

Include as many stakeholders in exercises as can be feasibly achieved. Risk mitigation for reputation risk can be a difficult proposition when the N^{th} or third party event cannot yet be predicted. Engaging with forensics specialists can help to devise scenarios that may otherwise be overlooked. Using a risk rating service to track emerging legal cases and judgments, changes in indicators of financial stability, and other key elements can provide an elastic set of metrics that can be viewed before onboarding and throughout the relationship. This can help gauge any loss of consumer or investor confidence before an event occurs. The level of elasticity impacts how the consumer confidence may result in a financial or market loss associated with a reputation risk event. When evaluating criticality and/or

materiality, the risk loss may be asymmetric to the actual cost (e.g., low probability of occurrence can result in a high reputation loss impact).

At a high level, risk is not a number. It is a probability of loss defined as exceeding a certain financial amount. That range is difficult to define (e.g., typical analysis uses "the % probability of exceeding $x" on average represents a range, not a number). This range has parameters which can be leveraged to evaluate reputation risk. For instance, external processes are becoming increasingly impactful on outsourcers, including economic, environmental, dependence on third parties, and technology so when operational risk events occur, they are likely to have a high impact on reputation. That impact can be estimated based on historical and other predictive factors. For modeling, scenario planning should identify the risk domains that are related to the organization's reputation risk, and carry out both a cost analysis and an analysis relative to the risk tolerance of the organization.

- Identify and assess the company's existing reputation and how third and N^{th} party relationships could potentially impact that reputation).
- Screen, analyze, and map strengths and threats across hand-selected metrics specific to the organization.
- Use scenario analysis in practice by applying heat map scales to quantified data to visually identify trends.
- Use models that examine all key factors that may exert influence on reputation, including factors that impact the ability of the organization to guide or lead communications during an incident.

Appendix D: Calculating and Reporting Reputation Risk

"The ability to effectively perform scenario modeling to predict outcomes is the holy grail of strategic decision making."

Marc Weinberg, Vice President Vendor Risk Management, Commerzbank AG, New York Branch

The following simulation, analysis, and reporting samples provide examples for practitioners for calculating and reporting reputation risk. Reputation risk does not lend itself to deterministic analysis, in which all the necessary data is available to predict an outcome with 100% certainty. A Monte Carlo simulation can be used to gain insight into possible outcome(s) and what the probability may be that any given outcome will occur. All of these reports and the Monte Carlo simulation can be utilized for reputation risk, whether for one vendor, all vendors, a type of vendor, or for evaluating internal reputation risk.

Both internal and external sources of data may be used for the simulation, including data related to loss magnitude, threat events and controls. Loss magnitude and threat event data may be sourced from numerous databases as well as insurance claims and Subject Matter Expert/Risk Owner calibrated estimates.

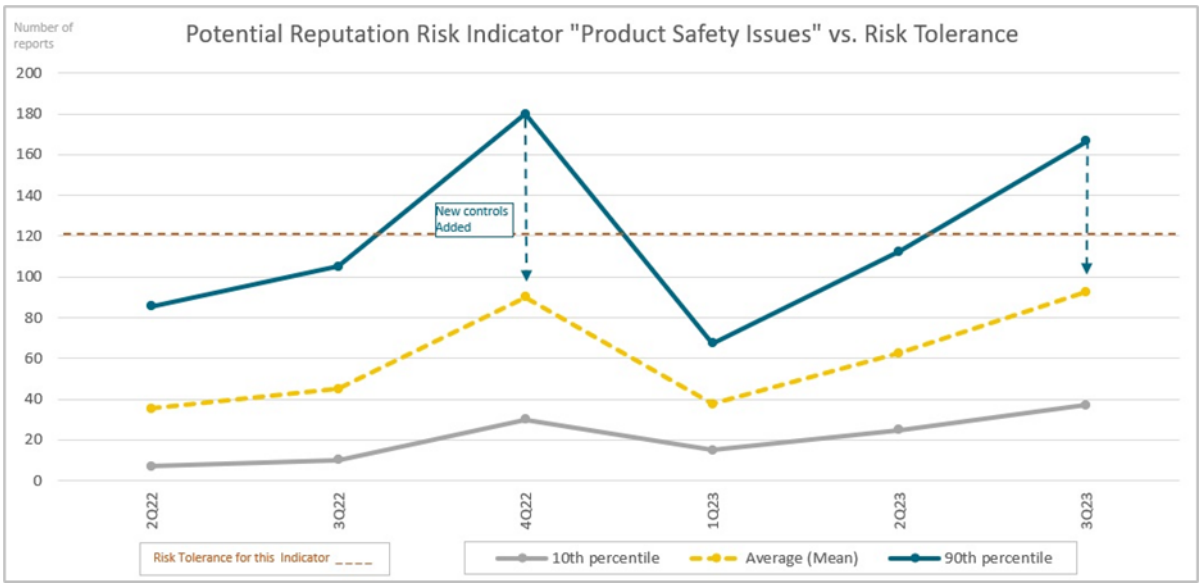


Figure D.1: Reputation Risk by Indicator – Before and After Mitigating Controls Applied [adapted from www.izirisk.com]

Analysis:

- When the Annualized Loss exposure is less than the organization's stated Risk Tolerance, the risk is deemed to be acceptable. Alternatively, when the Annualized Loss Exposure is greater than Risk Tolerance, the risk is deemed to be unacceptable.
- When the risk probability from the simulation is outside acceptable levels, action should be taken promptly to mitigate that risk. If the decision is made to delay or defer action, that is essentially the same as accepting the risk for that time period.
- The 10th and 90th percentiles indicate the confidence range or interval in which the actual loss would contain the predicted value.
- Management decided to mitigate the reputation related "Product Safety Issues" risk by implementing new controls and reducing the input values of Loss Event Frequency (LEF) and Impact. When the simulation is run a second time with these new input values, the mitigation results in a reduction in loss exposure below the organization's Risk Tolerance, as shown by the "New Control Level," for the average and 10th and 90th percentile levels.

Step-By-Step Process
The steps for using a Monte Carlo simulation to calculate reputation risk before and after mitigating controls are applied:

1) **Determine Key Assumptions**—determine whether this will be an internal or external third/Nth party evaluation.
2) **Identify Reputation Risks.**
3) **Define the first simulation run range of inputs with existing controls in place**.
4) **Run first simulation** and analyze results.
5) **Define the second simulation run range of inputs with additional mitigating controls in place.**
6) **Run second simulation** and analyze results.
7) **Repeat as needed** to achieve results within acceptable ranges.
8) **If mitigation is not sufficient to achieve acceptable results, consider other ways to treat risk(s)**—(i.e., selecting different vendor, exiting an existing relationship, applying different supply chain remedies or duplicate sources, etc.)

The Example Risk Analysis Template below indicates the process for running Monte Carlo simulations to generate loss exposure values both prior to and after mitigations. Once the first simulation is performed, one of the following is possible: (a) the risk at the 90th percentile will be below tolerance and no mitigation will be required; or (b) the risk at the 90th percentile will be above tolerance and Management will need to produce additional mitigations and record them in the template. After the second simulation is performed, the risk will be mitigated below tolerance, or Management must consider alternative treatment options.

Example Risk Analysis Template – Monte Carlo Simulation Template					
Inputs 1st Run		Output 1st Run	Input 2nd Run		Output 2nd Run
Identify Reputation Risks	Define Initial Range	Run First Simulation	2nd Run Proposed Mitigations	Define Updated Range	Run 2nd Simulation
→ Ransomware/ Cyberattack → Loss of Intellectual Property/Data Breach → Internal Fraud	Using a 90% confidence interval, determine Loss Event Frequency (LEF), Impact Range, and Distribution Shape (Chart Type)	Plot data in chart for (1) Average; (2) 10th percentile; and (3) 90th percentile.	→ Restrict MS Administrator Domain Access → Improve specific data security controls → Increased separation of duties, and other GAAP controls	Using a 90% confidence interval, determine Loss Event Frequency (LEF), Impact Range, and Distribution Shape (Chart Type) after mitigations	Plot data in chart for (1) Average; (2) 10th percentile; and (3) 90th percentile.

Table D.1: Example Risk Analysis Template

Supporting the Decision: A Return on Mitigation
Mitigation should be put in place to achieve the greatest Return on Mitigation (RoM) whenever Annual Loss Exposure (ALE) is shown to be beyond an organization's stated risk tolerance AND there are positive RoM options as well as sufficient budget available to accomplish this goal. Mitigation should be applied until ALE falls below risk tolerance AND there is no further potential RoM gain and/or no additional budget to effect further change.

$$\text{Return on Mitigation} = \frac{\text{Expected value of risk reduction}}{\text{Expected cost of mitigation}} - 1$$

This formula shows that 'Expected value of risk reduction' represents the difference between the average of the Monte Carlo simulation losses before and after a control is applied. If the reduction in expected losses was to be the same as the anticipated cost, then the RoM would be 0 (i.e., no gain by applying mitigation).

When ALE is above risk tolerance and no positive RoM options exist OR the existing budget is insufficient to effect mitigation, then RoM can be examined to determine:

- Have all possible mitigations have been considered?
- Is the risk tolerance threshold unrealistically low?
- Is it possible to increase the budget or decrease the required RoM.[3]

Example and Explanation of Probability Loss Distribution
Each quarter, a Monte Carlo simulation is run, which calculates the aggregated annualized reputational loss exposure over the next year at all probability levels. This histogram is the source of other reports derived from the model data analysis. Output from the model can be relied on statistically to provide insight that is missing from High/Medium/Low charts and dashboards.

The output is called a probability loss distribution, which is the basis for all other reporting. For purposes of the above chart, three probability levels will be reported:

- 10th Percentile – indicating that there's a 10% chance that the true loss value will be equal to or lower than the predicted value.
- 90th Percentile – indicating that there's a 90% chance that the true loss value will be equal to or lower than the predicted value.
- Average – the statistical mean of all the loss values.

An example of a probability loss distribution histogram is shown in Figure D-2.

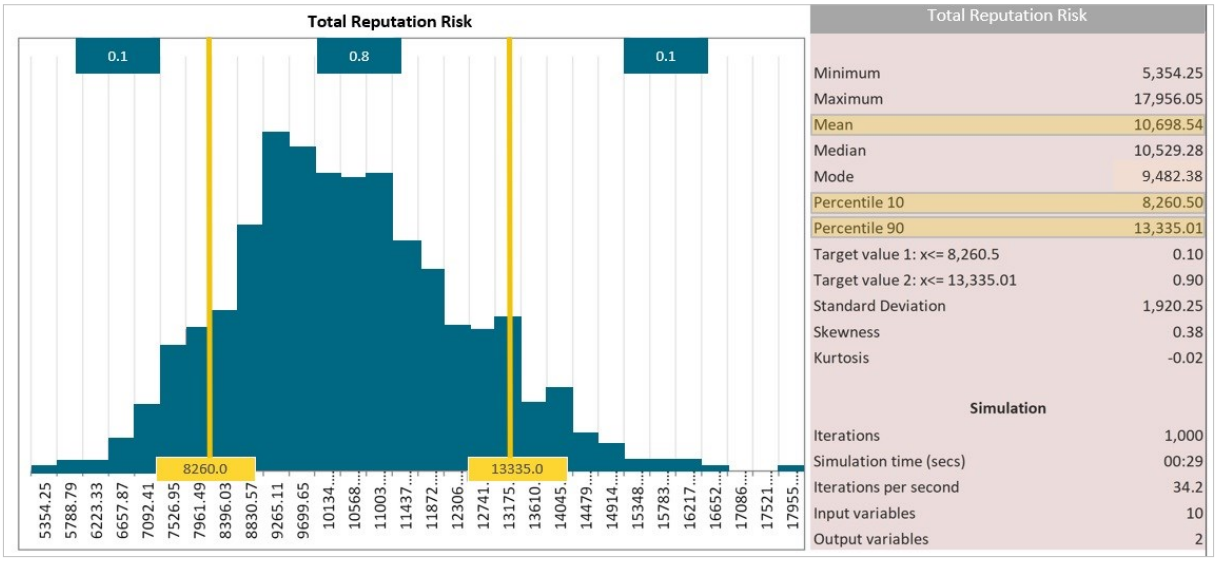


Figure D-2: Probability Loss Distribution (in thousands) [adapted from www.izirisk.com]

- The loss amount at the 10th percentile is $8,260; or there is a 90% chance that the loss amount will be greater than $8,260.
- The loss amount at the 90th percentile is $13,335; or there is a 10% chance that the loss amount will be greater than $13,335.
- The average loss is $10,699.

Other Reports

Bar Charts

Each reputation risk has a probability loss distribution. This output may be used to show, for each reputation risk, the loss exposure at the 10th and 90th percentiles, as well as the average loss. Management may set risk tolerance thresholds for these individual risks, similar to setting risk tolerance thresholds for aggregate risk. The output of this chart may also be used for KRIs, e.g., the number or percentage of individual reputation risks at the 90th percentile exceeding risk tolerance.

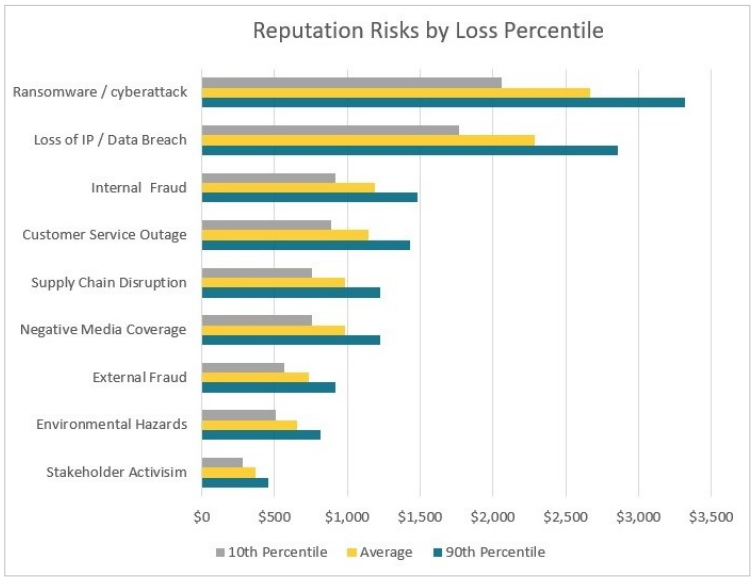
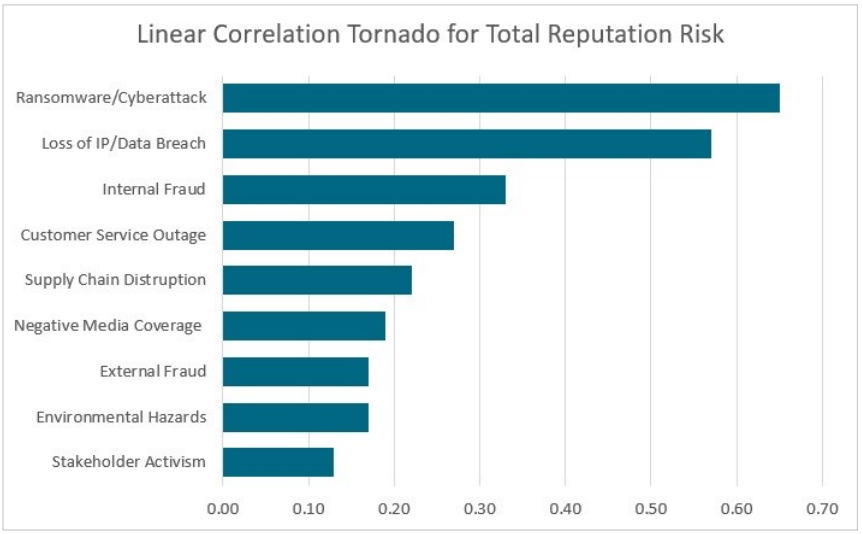


Figure D-3: Probability Loss Distribution by Reputational

Tornado Charts



Correlation Tornado by Input Risks to Total Reputation Risks	Correlation Coefficient
Ransomware/Cyberattack	0.65
Loss of IP/Data Breach	0.57
Internal Fraud	0.33
Customer Service Outage	0.27
Supply Chain Distruption	0.22
Negative Media Coverage	0.19
External Fraud	0.17
Environmental Hazards	0.17
Stakeholder Activism	0.13

Figure D-4: Linear Correlation Tornado for Total Reputation Risk

The correlation tornado, using a correlation coefficient as an index, is used to measure the degree of relationship between two variables if they are quantitative and continuous.

The chart shows in straightforward terms which risks have a greater impact on the total reputation risk. Of the nine risks identified, the two risks that have the greater impact on total reputation risk are: Ransomware/Cyberattack and Loss of Intellectual Property/Data Breach, with their respective correlation coefficients of .65 and .57, respectively.

S-Curve

An S-curve shows the probability of a given cumulative annualized loss amount. It is a direct reflection of a probability loss distribution histogram.

The cumulative loss amounts at the 10%, average, and 90% levels are consistent with the Loss Percentile bar chart for this risk.

S-curves can be produced for individual risks, categories of risks, single or multiple vendors, and the enterprise.

The S-curve shown here indicates that for the risk "Loss of Intellectual Property/Data Breach," there is a 70% probability that cumulative losses will be $2.5 million or less for the coming year. Conversely, there is a 30% probability that cumulative losses will be $2.5 million or more for the coming year.

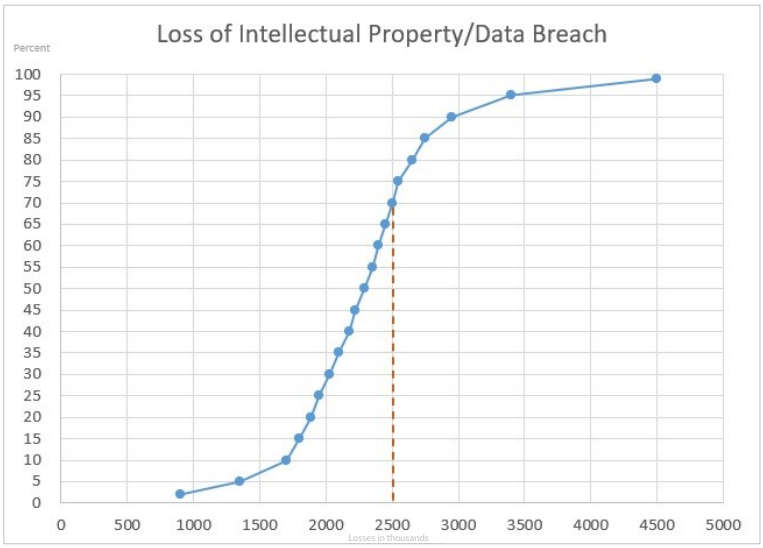


Figure D-5: S-Curve with Losses ($'000) on X-axis

Loss Exceedance Curve

A Loss Exceedance Curve shows the probability of an annualized loss equal to or exceeding a certain amount. The Loss Exceedance Curve is an inverted S-curve, which may be simpler to understand at the Management and Board levels.

Loss Exceedance Curves can be produced for individual risks, categories of risks, single or multiple vendors, or the enterprise. The Loss Exceedance Curve shown here indicates for the risk "Loss of Intellectual Property/Data Breach," there is a 30% probability that losses will be $2.5 million or more for the coming year.

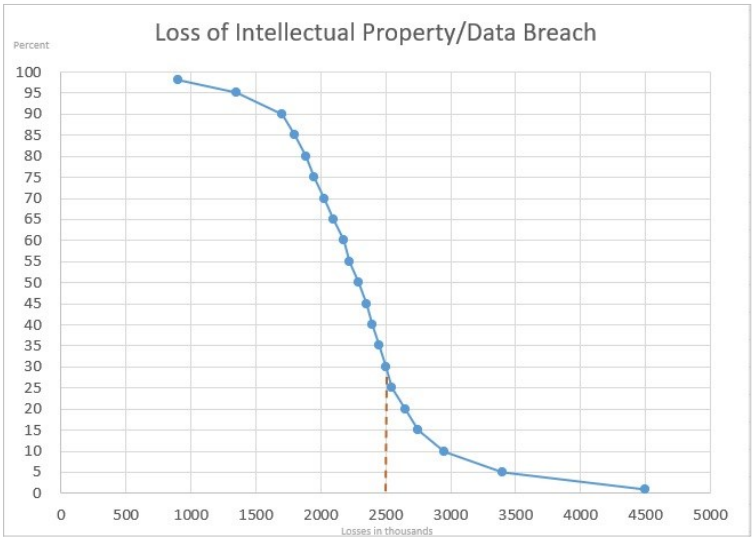


Figure D-6: Inverted Loss Exceedance Curve with losses ($'000) on X-axis

Appendix E: Selected Resources

Shared Assessment Resources

- Adaptive Risk Management for Complex Supply Chains
- Vendor Risk Management Maturity Model (VRMMM)
- Third-Party Risk Quantification: Techniques for the Extended Enterprise
- Guide to Risk Domains
- Nth Party Suppliers – Gaining a Toehold on Down Chain Providers and Nth Party Metrics
- Setting Expectations with Third Parties Blog
- Nth Party Metrics Blog
- Tone at the Top White Paper
- Complex Chain Practitioner Template
- Resources for Complex Supply Chain Risk Management
- Gaining Visibility into Nth Party Governance
- Guide to Risk Domains for Vendor Risk Management
- Shared Assessments Third Party Risk Management Glossary
- Shared Assessments TPRM Framework – Assessment and Continuous Monitoring – Section on Issue and Incident Management
- Shared Assessments TPRM Framework – Introduction, Contracts, Due Diligence, and TPRM Basics modules
- Shared Assessments Standardized Information Gathering (SIG) Questionnaire, Vendor Risk Management Maturity Model (VRMMM), other resources.
- Innovations in Third Party Continuous Monitoring: With a Name Like OODA, How Hard Can It Be?
- A New Roadmap for Third Party IoT Risk Management
- Work from Anywhere Supply Chain Risk Management Blog

Other Reputation Risk-related Management Resources

- Bloomberg, ESG Attacks Prompt Urgent Talks as Insurers Quit Climate Club
- Deloitte, Governance Risk and Compliance, Reputation Risk Blog
- ESG Trackers:
  - Climateactiontracker.org
  - Gain-uaa.nd.edu
- Hazards.fema.gov
- European Financial Reporting Advisory Group
- FAIR Institute Methodology for Quantifying Information Risk
- Journal of Operational Risk Framework Analysis for Reputational Risk
- The Responsible Business Alliance
- The Santa Fe Group Board Risk Committee
- World Economic Forum, 2023 Global Risks Report https://www.weforum.org/reports/global-risks-report-2023
- Protiviti, Quantitative Cyber Risk Management 101: Baselining and Baseline Cycling - Technology Insights Blog
- Izirisk, Open source commentary and examples of histograms, probability loss distributions, and 'Quantitative Project Risk Analysis in Excel

Acknowledgements

We extend our gratitude to the Shared Assessments Program's Global TPRM Best Practices committee members and leaders who contributed to this effort:

- Shamala Boyd, Chief Risk Officer and SVP, Global Customer Success, ControlCase
- Jen Duest, Associate Director, Global TPRM, Business Resilience & Corporate Insurance, Wellington Management Company LLP
- Martin Freeman, Cyber Security and Compliance Managing Director, Calastone; Shared Assessments UK/EU Steering Committee Co-Chair; Global TPRM Best Practices Committee Co-Chair; Member US Steering Committee
- Suzanne Guttschow, Third Party Risk – ERM Professional
- SS Harish, Infosec Compliance Specialist, Akamai Technologies, Inc.
- Matt Jones, Third party Information Security Risk Assessor, Echelon Risk + Cyber
- Shane Jones, AVP, Risk and Performance Management, LPL Financial Services
- Debra Lay, Lead Security Analyst, H&R Block
- Kaelyn Lewis, Vendor Risk Manager, Global Federal Credit Union; Global TPRM Best Practices Committee Co-Chair
- Robyn Marsi, Risk Services and Technology Practice Lead, Lynx Technology Partners, LLC
- Karthikeyan Mathanagopal, Lead Specialist Risk Assurance, Fiserv, Inc.
- David McCrory, Senior Manager, Technology Risk Management and Controls, Ontario Teachers' Pension Plan Board (OTPPB)
- David Medrano, Director, Third Party Risk Management, MorganFranklin Consulting
- Sean Nichols, Senior Manager TPRM, Charles Schwab & Co., Inc.
- Sean O'Brien, Managing Director, DVV Solutions; EMEA Best Practices Steering Committee; Shared Assessments UK/EU Steering Committee Co-Chair; Global TPRM Best Practices Committee Co-Chair
- Eddie Powell, Head of GRC and Privacy, The Constant Company, LLC
- Nicholas Mulvaney, Senior Vendor Security Risk Analyst, Cohesity
- Natasa Simovic, Third Party Risk Analyst, TeleSign Corp
- Pete Tannish, Information Security, Small Business Financial Exchange, LLC (SBFE)
- Marc Weinberg, Vice President Vendor Risk Management, Commerzbank AG, New York Branch

We would also like to acknowledge Shared Assessments Program staff and other subject matter experts who supported this effort:

- Jessica Calzada, Senior Committee Manager
- Bob Jones, Senior Advisor; Staff Lead, Global TPRM Best Practices Committee
- Charlie Miller, Senior Advisor
- Andrew Moyad, CEO
- Gary Roboff, Senior Advisor
- Marya Roddis, SUN Resource Development, Senior Technical Editor

About Shared Assessments

Shared Assessments has been setting the standard in third party risk assessments since 2005. Shared Assessments, which is the trusted source in third party risk assurance, is a member-driven, industry-standard body which defines best practices, develops products, and conducts pace setting research. Shared Assessments Program members work together to build and disseminate best practices and develop related resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments. Additional information on Shared Assessments is available by visiting: http://www.sharedassessments.org. A selection of most recent blog posts, studies, papers and more from our learning center.

Join the dialog with peer companies and learn how you can optimize your compliance programs while building a better understanding of what it takes to create a more risk sensitive environment in your organization.

The Shared Assessments Global TPRM Best Practices Committee examines the challenges organizations face in managing third party risk and identifies existing best and emerging practices. Examples of previously examined topics include complex supply chains, fourth-party management, third party contract development, risk rating, and assessment scoping. The output of this group includes industry briefing and white papers, practitioner guidelines, industry call-to-action pieces, and blogs that enhance TPRM practice. This group coordinates with the Product Development Committees when appropriate.

Endnotes

[1] A risk appetite statement is a documented definition of the organization's risk appetite, typically approved by an organization's governing board or committee. Shared Assessments TPRM Glossary. 2021. https://sharedassessments.org/glossary/.

[2] Shared Assessments TPRM Framework, 2020, https://sharedassessments.org/framework/.

[3] Adapted from: The Failure of Risk Management – Why It's Broken and How to Fix it, Second Edition, 2020, Douglas W. Hubbard, pgs. 72-74, 286