Our first-ever Extended Enterprise Experience brought together a cross-industry community for a choose your own adventure experience that looked forward to the future of third-party ecosystem management. Through engaging panels, dynamic breakout sessions, and innovative peer collaboration labs, three key themes arose that I believe will continue to resonate in day-to-day business:

The ground is shifting and the time to act is now. Nearly two-thirds of participants indicated staying on top of risks keeps them up at night. Whether it is responding to the pandemic or facing a proliferation of cyberattacks, the fringe-risks of yesterday are now pervasive in business ecosystems. Add to that a dramatic rise in the number—and expectations—of stakeholders, increased regulatory scrutiny, and the sheer speed with which a risk event can cause damage to your reputation, the burning third-party risk management (TPRM) question is no longer “why?,” but “how and how soon?” Carpe Diem.

The world is unpredictable, do not let perfect be the enemy of good. Businesses need to push the envelope in how they identify, collect, and act on risk intelligence. In the next normal, the one with the most information only leads if it translates to real time, actionable insights that drive effective decision making across the organization. An iterative or agile approach to risk intelligence empowers an organization to phase out the point-in-time assessment, be proactive in their risk management, and take the consistent baby-steps necessary to mature from “growth mode” to integrated data-driven insights.

From the use of analytics to drive trending data and insights to tech-enabled event identification, triage, and action to the adoption of innovative risk sensing solutions, the technology backbone of your TPRM initiative is paramount. For many, this will be an orchestrated shift from a patchwork collection of tools to a stackable end-to-end solution that integrates and correlates data, external risk information, and the output from ongoing monitoring activities. A continuous and coordinated effort can help you achieve the overarching objective of placing relevant, real-time data in the hands of those who need it.

I truly look forward to what this next year will bring to the third-party ecosystem risk management journey. Hats off to you all.

Dan Kinsella | Extended Enterprise leader
Deloitte & Touche LLP
dkinsella@deloitte.com
CLOUD FINANCIAL MANAGEMENT

OVERVIEW
There is a growing need for cloud financial management as organizations move more of their business into the cloud – further accelerated over the past year with digital transformation initiatives. Challenges with managing cloud spend include the need for organizational change and a fundamental shift in how information technology (IT) costs are managed.

Adopting a cloud FinOps culture in an organization's cloud strategy can have several priority outcomes that can help control rising expenses while enabling business value and innovation through the cloud.

Principles of cloud financial management:
• Business value of cloud drives decisions
• Ownership of cloud usage is defined and aligned to business owners
• Consumption reporting is available to stakeholders in a timely manner
• Cloud financial negotiations and vendor strategy decisions are centralized

POLL LEARNINGS
• The biggest challenges participants are facing with cloud financial management:
  • 33%: Cost management (e.g., including shifting focus, reporting, chargebacks)
  • 33%: The human element (e.g., experience, resource availability)
  • 33% felt business value of cloud drives decisions was the most challenging FinOps principle to drive at their organization

OPPORTUNITIES
Cloud financial management lifecycle to realize the goals of cloud FinOps:
• Inform: Understand cost drivers, allocate cloud spend effectively, benchmark efficiency
• Optimize: Enable real-time business decisions, monitor, track, and advise on resource and workload efficiencies
• Operate: Continuous improvement of operations to address dynamically changing needs, establishment, and acceptance of cloud FinOps culture
OVERVIEW
Many organizations have been working to upgrade financial management of third-party providers. Yet, management practices may not be equal to the risks presented and there's a tendency to overlook or misinterpret the role financial management can play in optimizing their extended enterprise. As third-party ecosystems become more complex and investments such as cloud continue to expand, a strong foundation of financial management practices will be vital for sustainability.

• Cost pressures are prevalent across industries, and we are seeing a strategic push for more formalized cost recovery and optimization programs
• Balancing financial compliance and strategic relationships can be challenging to navigate, but important to consider when striking the appropriate balance in engaging with cost recovery and optimization programs
• Extended enterprise continues to evolve in new, complex ways and organizations are now tasked with managing third parties in ways that keep pace with business and societal trends

OPPORTUNITIES
Quick win solutions to yield direct cash benefit and future cost savings:
• Up to 30%: Working capital optimization
• Up to 20%: Indirect tax recovery
• Up to 20%: Software asset management
• Up to 5%: Third-party contract compliance
• Up to 5%: Accounts payable analytics
• Up to 2%: Statement of accounts

PEER COLLABORATION | DISCUSSION SUMMARY
What is your organization focused on?
• Reallocating resources to optimize spend/cost recovery
• Clauses in contracts (e.g., discounts, ‘best’ purchase price)
• Monitoring managed service provider relationships
• Buy side/sell side opportunities (revenue leakage)
• Volume spend isn’t always the riskiest area to focus on
• Cloud FinOps (e.g., managing/monitoring spend, billing)
• Spend categories with significant risk (e.g., labor costs, taxes)
• Contracts: Retained recruiting, construction
• Royalties
• Universal rebate structures
• Outsources tech spend
• Media/advertising

POLL LEARNINGS
• More than half of respondents reported their organization experienced a third-party related incident with a financial impact in the past year
• 33% ranked cost recovery and optimization as a priority for their organization today
• Risk intelligence and digital risks are key areas of focus for participating organizations
ENVIRONMENTAL, SOCIAL, AND GOVERNANCE (ESG)

OVERVIEW
Supply chains were traditionally set up for cost and time efficiency—but stakeholder expectations and regulations are changing, demanding a redesign around environmental and social responsibilities. Organizations are paying close attention to ESG risks in their supply chains because of:
• Growing pressure to operate responsibly and integrate sustainability into strategy
• ESG impacts that are outside a company’s own ‘four walls’
• Potential brand, operational, and financial impacts due to failure to manage risks
• High performance on material sustainability/ESG issues may translate into strong returns

Companies can outsource business activities, but not risk. Brand challenges can arise when special interest groups influence consumer behavior; companies fail to deliver sustainable supply chains; negative events go viral. Financial/operational challenges can arise when harmful labor practices result in quality concerns, labor disputes, disruption of deliveries, and regulatory investigations; inadequate preparation for natural disasters halts production; suppliers fail to comply with code-of-conduct requirements, disqualifying them from order placements; and through supplier environmental impacts and footprint.

PEER COLLABORATION | DISCUSSION SUMMARY
What are your biggest challenges?
• Identifying the risks and creating a holistic approach
• Core elements and metrics to guide programs/manage risk
• Who are the best players in the market?
• Plugging ESG into existing programs and processes
• Gathering data from third parties to support ESG efforts
• Identifying key partners/relationships

What is your organization focused on?
• Ethical code of conduct for third parties
• Monitoring requirements and how regularly they are audited
• Measuring ESG/quantifying the value (e.g., supplier diversity)
• Supporting players (e.g., groups/associations, internal)

OPPORTUNITIES
Key enablers to build a sustainable supply chain: Traceability and insight, operational excellence, and industry collaboration. Supply chain resilience can be boosted by:
• Leveraging strategic and technology alliances
• Defining strategic transformation principles and requirements
• Designing and optimizing the physical footprint of your supply chain
• Developing sustainable supply chain operating models
• Implementing third-party management and audit solutions
• Leveraging circular economy and waste management opportunities

POLL LEARNINGS
• When asked to rate the level of preparedness for managing ESG risks and opportunities across the extended enterprise, 45% of respondents reported having implementation/transformation efforts in progress
• More than 50% attributed changes to the ESG landscape to capital markets, corporate action, regulators, customer demands
• 85% expect increasing regulatory pressure around ESG disclosures in the near future – 40% in the next two years, 45% in the next five
MODERNIZING ECOSYSTEM RISK MANAGEMENT

OVERVIEW
Modern third-party risk management is in high demand as many organizations more heavily utilize an ecosystem of third parties. With third-party ecosystems continuing to become more complex, current capabilities are no longer sufficient to manage third-party exposure effectively and commensurate to risk.

Common challenges include:
• Ineffective point-in-time assessments
• Limited ongoing monitoring capabilities
• Lack of adequate strategy and resources
• Evolving threat landscape
• Lack of automation and aggregation of risk

The continuous flow of data from organizations to third-party ecosystems leaves organizations' sensitive data susceptible to risks/threats that are not identifiable within their own cyber risk infrastructure. These include exfiltration, ransomware, denial of service, malware, brand and reputation, and financial viability.

OPPORTUNITIES
An approach that complements traditional third-party risk management programs with ongoing monitoring and oversight, centered around the following principles:
• Elevate to high-value risk management
• Tech-enabled event identification, triage, and action
• Analytics to drive insights based on internal and external data
• Dive deep into data and validate with subject matter advisors/analyst investigations

PEER COLLABORATION | DISCUSSION SUMMARY
What are your biggest challenges?
• Shifting from silos to integrated risk management
• Regulatory/compliance/visibility – down to the fifth party level
• Identifying risk exposure (e.g., technology/software, hardware, infrastructure)
• It’s not ‘if’ but ‘when’ an incident occurs – how do we respond?

What is your organization focused on?
• Scalable technology processes
• Data lakes and integrated systems, applications, databases, etc.
• Operating model/ownership
• Utilizing data for insight into risk profile
• Relying on third-party assessment for the basics

POLL LEARNINGS
• 25% of participants had a vendor fail to notify them about a cyber incident in the last six months
• 47% felt their organization would be most impacted by tech-enabled analytics, correlation, reporting, and illumination platform as a core enabler of TPRM modernization
• 43% are monitoring for risks and vulnerabilities using cybersecurity rating tools, cyber utility shared assessment platforms, threat hunting, security operations center vulnerability solutions, and emerging data flow or network anomaly solutions
PRIVACY

OVERVIEW
While regulatory requirements and consumer expectations for data privacy have continued to increase, many extended enterprise programs are not keeping pace. Opportunities to enhance extended enterprise risk management (EERM) programs through data privacy include:

• Privacy governance: Lack of operational integration between privacy and extended enterprise activities
• Intelligence sharing: Lack of ongoing monitoring on third-party use and sharing of personal information
• Process automation: Lack of shared processes/tools (e.g., Data Loss Prevention (DLP)) to support extended enterprise privacy and data management
• Joint risk management activities: Lack of industry standard third-party contractual expectations to manage data privacy and governance requirements
• Data governance: Lack of integrated approach to data governance and data management with extended enterprise

OPPORTUNITIES
Privacy-by-design can enhance the EERM lifecycle:
• Establish requirements by identifying third-party related data privacy requirements
• Update and maintain an inventory of third parties with whom personal information (PI) is shared and integrate with data inventory/record of processing activities (ROPA)
• Insert contractual clauses to hold third parties accountable for privacy requirements
• Monitor third-party relationships, manage changes to risk profiles as business needs change, and maintain oversight into privacy and data related obligations
• Account for PI management before termination of third-party relationships

PEER COLLABORATION | DISCUSSION SUMMARY
What are your biggest challenges?
• Regulatory/disclosure: Meeting requirements/timelines and streamlining related processes
• Customer and supplier commitments/enforcement
• Standards consistency (e.g., national, global)
• Digital transformation difficulties and implications
• Misalignment/issues with vendors on terms/requirements
• Security vs privacy, cross-functional awareness and collaboration

What is your organization focused on?
• Rationalized requirements approach
• GDPR
• Retaining third-party law firms

POLL LEARNINGS
• Improving privacy risk monitoring and oversight is the top priority for addressing third-party privacy risks
• 50% maintain visibility into personal information shared with third parties through manual third-party inventory tracking, including attributes of data shared
• 63% reported privacy is engaged on an ad-hoc basis when it comes to their extended enterprise programs
• 44% use privacy-enabling technologies for some stages of their EERM program or not at all; only 10% embed fully
SECURE SUPPLY CHAIN

OVERVIEW
Secure supply chain is a broad approach to apply security risk mitigation throughout supply chain ecosystems. Rather than viewing security supply chain risks from a single entity’s perspective, it shifts the view to look at the lifecycle of security across manufacturers and developers, service providers, and consumer personas. Secure supply chain also breaks away from the traditional view of third-party risk management (TPRM), which focuses on the direct supply chain (vendors and suppliers) and looks at the indirect supply chain (all third-party relationships, internal resources, transportation, and logistics).

Principles:
• Product security management
• Secure transportation and logistics
• Product authenticity
• Asset inventory and monitoring
• Remote access and privilege management
• Threat monitoring, correlation, and alerting

OPPORTUNITIES
Prepare for tomorrow’s secure supply chain risks:
• Flag risky purchases based on device type/vendor early in the procurement process
• Provide alerts to the business when a vendor risk is identified
• Detect and respond in near-real time; in-house or through a managed service provider
• Tailored security program based on risk associated with known device types/vendors
• Anomalous activity is flagged Day 0

PEER COLLABORATION | DISCUSSION SUMMARY
What are your biggest challenges?
• Stakeholder engagement
• Governance/strategy/identity
• Monitoring of entities – outsourcing can impact visibility/insight, how far down the line can ownership be enforced?
• Risk assessments (e.g., accelerators, data)
• Regulatory requirements

What is your organization focused on?
• Risk assessments
• Proactive sensing
• NIST 800-161
• Securing fed information systems

POLL LEARNINGS
• 36% of participants reported experiencing a supply chain disruption due to a cyber event in the last 12 months
• 73% anticipate a cyber event will disrupt their supply chain in the next 12 months; with nearly half reporting leadership concern around a ransomware attack specifically
• Unrelated bad actors (e.g., cyber criminals, nation states) were reported as the biggest threat to supply chain cybersecurity
STAKEHOLDER TRUST

OVERVIEW
Customer and stakeholder expectations are evolving, putting trust at the epicenter of many organizations' priorities. Aligning your organizational purpose with the extended enterprise creates trust and identifies value across the ecosystem of stakeholders.

Trust challenges are the prevalent throughout the relationship management cycle:

• **New client diligence**: Customer acceptance in the sales cycle
• **Contract and on-boarding**: Incorporate risk, compliance, and performance requirements in contracts
• **Ongoing relationship management**: Respond to ongoing monitoring and risk management requirements
• **Renew or termination and off-board**: Determine need to terminate and off-board/renew

PEER COLLABORATION | DISCUSSION SUMMARY
What are your biggest challenges?
• Regulatory and stakeholder expectations/requirements
• Internal stakeholders and suppliers – relationships are often transactional in nature, neglect to establish trust
• Cultural issues/lack of awareness
• New FinTech (e.g., lack of risk model, policies)
• SOC 2 reporting

What is your organization focused on?
• Procurement processes/role in third-party management
• Guarding supply chains/manufacturing, moving in house
• Leveraging regulations to compel suppliers to cooperate
• Stakeholders – who, what (e.g., blockchain, information sharing)

OPPORTUNITIES
Organizations may gain better visibility into their third-party ecosystem to improve transparency and trust in today's competitive marketplace by:

• Aligning customer, organization, and supplier values
• Managing costs
• Gaining and retaining trust
• Improving transparency

POLL LEARNINGS
• 50% of participants reported **volume of information request and deciphering the right level of detail** as the greatest challenge in gaining trust and transparency across their ecosystem
• **Conducting due diligence prior to contracting (43%) and responding to ongoing monitoring and risk management requirements (43%)** were reported as the most challenging aspects of the third-party lifecycle
• 50% are considering how to **shift from ‘point-in-time’ assessments to event-driven/‘real time’**
SUPPLY CHAIN RISK REBOOT

OVERVIEW
Supply chain risk has come to the forefront this past year more than ever. Today's environment is not only one of prolonged economic uncertainty, but of heightened risk, blurring the lines between business-as-usual operations and crisis management and response.

Challenges many organizations are facing:
• Inability to determine supply and plan based on demand due to lack of downstream supplier visibility
• Distressed suppliers unable to meet obligations due to liquidity and credit constraints
• Complex, rapidly evolving, and expanding regulatory requirements
• Impact of an unclear political and geopolitical environment on trade and imports/exports
• Inability to respond to newfound customer and stakeholder requests regarding environmental, social, and governance risk

PEER COLLABORATION | DISCUSSION SUMMARY
What are your biggest challenges?
• Sub-supplier tiers and bringing in automation/artificial intelligence
• What makes up risk (e.g., threat, vulnerability, impact)
• Secure supply chain – end-to-end/holistic vs in pieces
• Talent
• Third-party relationships/compliance with requirements

What is your organization focused on?
• Setting standards/minimum requirements
• Identifying supplier risk profiles
• Risk analysis across industries and capabilities
• Risk intelligence, artificial intelligence

OPPORTUNITIES
• Illuminating risk tiers and having knowledge of the ecosystem is no longer a luxury but a necessity
• Risk and controls screening will no longer be a single point-in-time activity, but rather event driven
• Acting on risk via digital platforms that integrate supply networks and provide enhanced visibility is crucial to connect disparate sources to supply chain decision makers

POLL LEARNINGS
• More than half of participants rated awareness and management of supply chain risks as ‘familiar, managing’; only 18% rated ‘very familiar, managing well’
• 56% reported supplier management and risk action and remediation as most critical to success of their supply chain
• 60% indicated extended value chain risks (e.g., third-party suppliers, fourth-party risk, demand/market risks) are the biggest concern for their organization, followed by operational risks (e.g., risks that exists within the organization)
TECHNOLOGY ENABLEMENT

OVERVIEW
With third-party ecosystems continuing to become more complex, now more than ever, current third-party risk management (TPRM) capabilities are challenged to manage third-party exposure effectively and commensurate with the risk they present to the organization.

Today's highly complex environment has exposed the ineffectiveness of TPRM programs:
• Lack of technology coordination: Coordination of technology solutions is needed to optimize collaboration, reduce redundancies, and share data
• Lack of automation and aggregation: Evolving technology landscape presents opportunities to focus on designing and implementing an effective technology strategy
• Limited ongoing monitoring capabilities: Increased complexity and volume is elevating the need for diversification and prioritization in third party oversight
• Point-in-time assessments limitations: Risk sensing capabilities are under-utilized, many oversight activities are generic, and data is not correlated

OPPORTUNITIES
• Integrate TPRM technologies to provide a more effective end-to-end third-party lifecycle and user experience
• Leverage external risk information for advanced risk sensing
• Enable correlation of available information to derive deeper meaning from isolated data points to provide better intelligence to act
• Implement risk sensing and data correlation capabilities to gain visibility into third-party risk beyond point-in-time assessments
• Periodically assess technology for alignment with goals/business requirements

PEER COLLABORATION | DISCUSSION SUMMARY
What are your biggest challenges?
• Understanding the landscape/what's available
• Establishing governance and alignment at the enterprise level
• Third-party processes/controls throughout the lifecycle
• Managing data points across siloed systems

What is your organization focused on?
• Defining ownership and creating a centralized and simplified workflow/operating model
• Leveraging data (e.g., integration, aggregation, data driven workflows/automation of risk, end-to-end risk dashboard)
• Building risk into assessment/decision making criteria for vendors
• Cultural shift via communications and training

POLL LEARNINGS
• 42% of participants rely on off-the-shelf tools for assessments and scoring, with only some third-party intelligence data; 33% are using customized tools for tactical decision making, including access to centralized data
• 41% participants felt the following posed challenges to their TPRM program: Lack of automation, data aggregation, and monitoring capabilities; lack of technology strategy, cross-functional program, and dedicated resources; and evolving third-party landscape and technology solutions

Copyright © 2021 Deloitte Development LLC. All rights reserved
THIRD-PARTY LIFECYCLE MANAGEMENT

OVERVIEW
Dependencies on third parties continues to increase as companies look to innovate drive growth. Managing these relationships remains a challenge and driving toward simplicity and aggregation of information for better decisioning is top of mind for many.

Challenges that are keeping organizations up at night include:
- **Managing performance**: Decentralized data and decision-making, declining/suboptimal operational efficiency and productivity, and ambiguous guidelines for extended enterprise performance monitoring and reporting
- **Staying on top of risks**: Inconsistent risk management practices across the enterprise, complex, evolving risk environment, and immature—or lack of—extended enterprise processes to prevent and/or respond to non-compliance events
- **Seeking financial optimization**: Insufficient access to real-time data to manage costs, lost value/added costs from non-compliance with contract terms and/or suboptimal working capital management and cash-flow cycles
- **Finding partners that align with purpose**: Increasing pressure for environmental/social disclosures and cascading beliefs, policies, and initiatives through the ecosystem

PEER COLLABORATION | DISCUSSION SUMMARY
What are your biggest challenges?
- Ensuring program is simple, clear, drives business value
- Managing growing volume of/visibility into third party ecosystem
- Segmenting/risk profiling suppliers
- Have basics covered; moving up maturity scale is a challenge
- Business continuity planning

What is your organization focused on?
- Continuous monitoring of risk/ecosystem risk assessment
- Performance analytics
- Relationship management within ecosystem
- Social/ESG issues and connection to reputational risk
- Monitoring financial stability of third parties

OPPORTUNITIES
- Elevate to high-value risk management
- Use analytics to drive insights based on data
- Tech-enabled event identification, triage and action
- Identify trending data and investigate with risk owners

POLL LEARNINGS
- 63% of participants reported **staying on top of risks** was keeping them up at night
- 71% reported facing a **third-party related incident** in the past three years
- **Lack of unifying technology/single source of truth** is the biggest challenge faced when engaging with internal stakeholders (58%)
This presentation contains a summary of the common themes expressed by participants during the Extended Enterprise Experience. The notes were taken informally and were based on discussion heard and were not validated or confirmed by Deloitte. Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2021 Deloitte Development LLC. All rights reserved.