SFG | SHARED ASSESSMENTS

Building Best Practices Briefing Paper

Complex Supply Chains – Gaining Visibility into Nth Party Governance

Executive Summary

Sovereignty in the supply chain is not possible without a high degree of visibility into the Nth parties involved in the outsourcer-provider relationship. Therefore, the need exists to identify critical dependencies across a complex supply chain and then to apply a consistent set of principles for monitoring the processes and controls required for security and resilience across both inbound and outbound supply chains. How to accomplish this remains a perplexing question for practitioners. As third party and supply chain risks converge, increased oversight demands are falling on outsourcers as well as providers.

What's at Risk and How Risks Increase as You Go Up/Down the Supply Chain?

Due diligence information gathering must include processes for Nth parties. Foremost is the need to quantify and map the supply chain so that critical dependencies can be recognized. Without mapping, there is no way to connect the dots across providers and suppliers to allow for proactive versus reactive responses to the implications of those interconnections.

Information has to be compiled, analyzed, and monitored to understand all the interdependencies posed by third, fourth, and Nth parties. Controls at each point must be assessed, and monitored where risk merits that effort. This requires a big picture perspective not currently attainable in many organizations. It also requires a clear understanding of what qualifies as a "material risk" for the outsourcing organization, so that resources are appropriately focused.

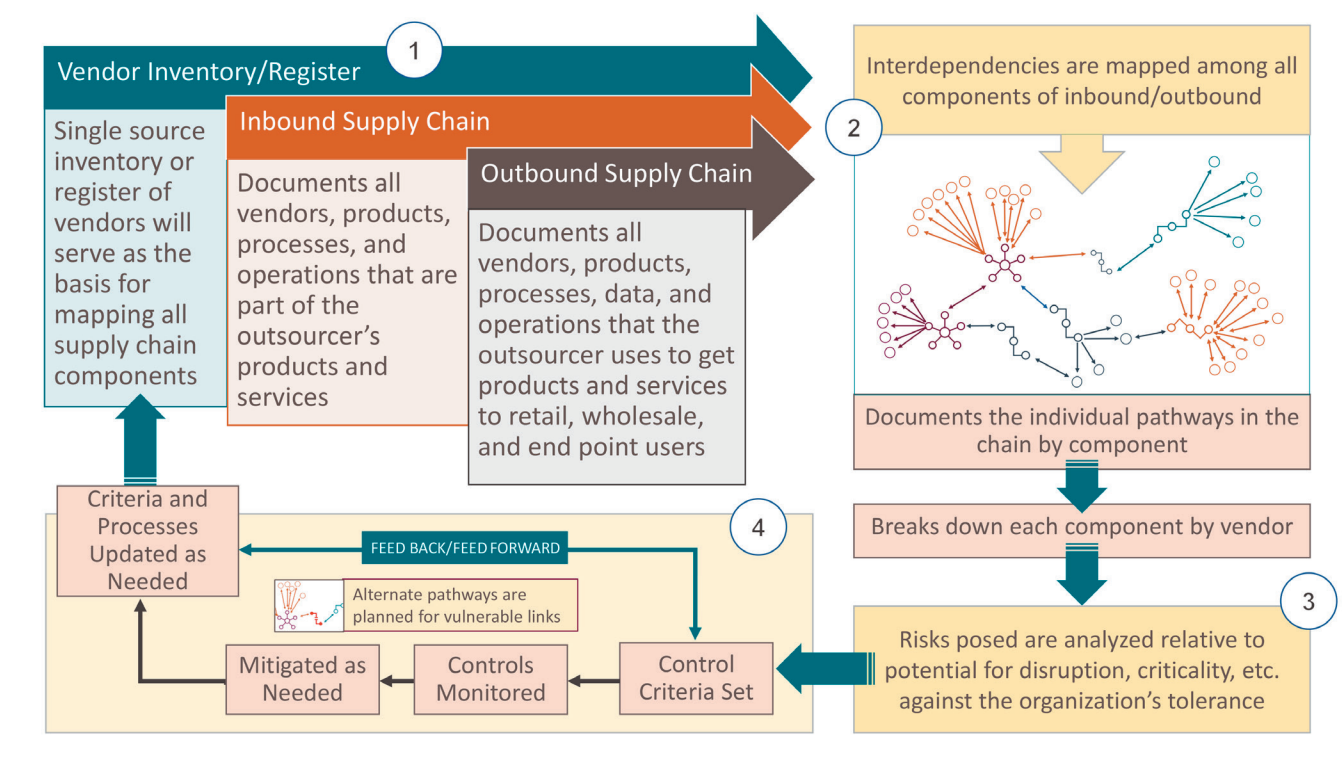
The terms for inbound and outbound supply chains have different meanings depending on the industry. In general, unavailability of inbound pre-product raw materials and/or component parts will have a negative impact on the completion of the final product, and post-production delivery disruptions impact revenue. Mapping should take into consideration which potential inherent risks exist at each stage of its inbound and/or outbound supply chain.

- **The Inbound Supply Chain is the pre-product supply chain** where sourcing of products and services, extends through the design, development, manufacture, distribution, price changes, and delivery of quality products and services to the acquirer. Examples include factory equipment, raw materials and goods, delivery channels, and communications channels.
- **The Outbound Supply Chain is the post-production delivery chain for final products and services.** For all service industries, points that need to be mapped include network connectivity to and use of consumer, Intellectual Property, or other confidential or restricted data that is entrusted to a vendor. Links in the outbound chain that can be disrupted include the hand-off points for sensitive information, business operations that make outsourcer services possible, the outsourcer's third parties, and other parties in the supply chain (the Nth parties).

Disruption in either supply chain can have a direct impact on an outsourcer's reputation. Risks that may impact the ability of an outsourcer to deliver its good and services must be understood, mapped, managed, and mitigated.

Gaining Visibility – Mapping the Supply Chain

To conduct a complete risk analysis across the supply chain requires a targeted information management effort that covers both inbound (supplying the outsourcer's product) and outbound (to the customer) supply chains.



Sequentially (and cyclically) the following need to be established and regularly updated:

1. **A single source inventory/register of vendors** lends itself to the effort of mapping all supply chain in a cyclical fashion.
    a. **Inbound products, processes, and operations inventory.**
    b. **Outbound products, processes, and operations inventory.**
2. **Map of the interdependencies between the inbound and outbound** products, processes, and operations.
    a. **Document the pathways** and interconnections of the chain by component.
    b. **Document individual vendors against the map of interdependencies** to understand the significance of the vendor in the scheme of things, as well as their fourth and Nth parties' significance.
3. **Analyze the risk posed.** Only when all the documentation and mapping are in place can the potential risk really be estimated and understood, controls criteria set, and management of the supply chain really be effective. Where feasible, automate risk analysis; however, always retain the human factor in the process to ensure that decision-making is not solely automated.
4. **Monitor, mitigate, and update criteria/thresholds and relationships as needed.**

This is not a one-size-fits-all process. Third Party Risk Management (TPRM) resources are often focused primarily on documenting vendors and analyzing the risks posed by those individual relationships. To achieve an in-depth information gathering process, with the goal of achieving greater transparency across the supply chain, organizations might examine how a federated model of governance could be used in the enterprise. Identifying where responsibilities currently lie, and then adapting as needed to assign clear roles and responsibilities to assure a more robust level of insight, process development, and execution. In most organizations this process is clearly the responsibility of the control function, but the TPRM practitioners have to have awareness of the controls that need to be mandated at the contract level. TPRM can collaborate enterprise-wide in this way only if they are supported by strong leadership and appropriate resources.

Challenges and Churn Points

Typically, practitioners report that they cannot reach far enough into the chain beyond their third parties and their hosted providers to gain insight into the use of down stream vendors. Data, intellectual property, time, and revenue (due to delay) are the obvious concerns that arise from this lack of transparency.

While regulations are emerging in some jurisdictions that mandate the outsourcer has the right to be apprised of, and reject, a change in a fourth/Nth party before that party is engaged, this requirement is far from universal. Whether a new vendor or an existing one, begin to mandate by contract, scope of work (SOW), data privacy security addendum (DPSA), or other binding documents that the vendor's vendors will have to meet specific control and/or practice standards that are appropriate. The third party would be obligated to ensure that this occurs and will be documented.

Churn Points

The combined impact of these challenges can cause a range of concerns that include privacy issues (such as improper or over-exposure of personally identifiable information), use of unapproved parties, unapproved hosting locations, and even availability issues. Flow needs to be examined across every aspect of the chain, including components, transportation, and assembly IoT (e.g., floor manufacturing robots). Where possible, vendors that manage proprietary information transfer (schematics, other IP) and their downstream providers must be identified as material.

Noise in the System: A tremendous amount of noise can be produced when supply chains and vendors need to be assessed engagement-by-engagement; for service level relevance by business unit (individual unit use and needs), and then monitored and resulting risks mitigated. Adding to the noise is the fact that each point of access is not always connected end-to-end.

Lack of Visibility and Transparency: In addition to the third party inventory/register:

- Visibility *and* transparency beyond the third party (first parameter level) has to be achieved to be able to: (1) follow the data; (2) know if a product has been negatively, and possibly dangerously, impacted; and (3) be proactive in risk management.
- Transparency is largely an issue because without it understanding by both outsourcer and provider suffers.
- Visibility has to be achieved over the ENTIRE landscape (data flow, service, product). Unless enterprise governance includes key processes, the right answers will not be received to direct work effectively and efficiently, much less recover from major disruptions and/or data compromises in an agile manner.

Scope Creep: If a third party has been onboarded and previously assessed for a scope of work, it is possible for the product/solution to morph to a different risk landscape. This scope creep changes the risk posed by that vendor – for better or worse – and has to be recognized when it occurs and managed accordingly in a timely fashion. Internal communications and feedback mechanisms must be in place to show when/if a vendor is being used in a manner different from what was intended. And when/if that has occurred, document what measures have been taken to assure appropriate risk management.

Talent Gaps: Skill sets are a high risk management failure point where TPRM and supply chain risk management converge. There are not enough practitioners with security, privacy, TPRM, and other key training all in one package (including cyber expertise) to fill the need. Contracting out those services provides yet another pathway for Nth party involvement in the supply chain. Use of a third and/or Nth party is not always a viable, acceptable, or allowable. It can be prohibitive to quickly replace this type of high level institutional knowledge, especially where costs must be considered among a multitude of other concerns.

Proactively Improving Visibility (and Reducing Churn)

Practitioners need to closely consider what other concerns need to be considered when they grapple with what risk each provider poses. Retail and healthcare are increasingly moving offshore, placing a huge uptick on assessment requirements. This impacts services, transportation, data, etc. and covers the gamut of control components, which leads to additional challenges. The concerns and proactive measures in the following table should be incorporated into enterprise risk management planning and processes.

RISK CONTEXT	*Contextual assessing is critical.*	Framing context requires the participation of business units organization-wide and across all vendor relationships – as far down chain as possible – to determine and include the controls and contract requirements that are needed to meet each successive outsourcer's risk appetite and requirements throughout the chain. How far to go into the supply chain is dictated by the outsourcer's risk tolerance. That level of risk can only be aligned to the organization's needs by a complete mapping. *Concentration risk must be assessed across both inbound and outbound supply chains.*
EFFICIENCY	*Capitalize on existing resilience planning.*	It is important to understand the organization's existing processes to be able to capitalize on them and not duplicate efforts (e.g., business continuity planning – BCP). From the point of view of resilience planning in Nth party governance, an obvious – yet expensive – solution is to have more than one supplier vetted, prepared, and ready to move into market. This may not be feasible in markets where resilience is less important than the cost of this proposition.
COMMUNICATIONS	*Refresh vendor expectations.*	For any relationship, inherited or otherwise, when current and emerging risk management requirements need to change, that change needs to be mirrored within the assessment process. Where novation (a new contract) or updating existing contract terms is not possible, a red flag may be required to indicate the lack of leverage (and/or cooperation) and document that as a known risk. If enough companies start to notate this as a risk, then visibility is created that can move seemingly unmovable mountains. For example, if enough companies started documenting the inability to audit on larger providers, the potential exists for larger forces to change the balance toward transparency. M&A due diligence should always account for new, and potentially added, risks posed by the inbound and outbound supply chains of the merger/acquisition target. Critical systems, applications, networks, and vendors should all be examined.
ADVOCACY	*Push for industry-wide solutions.*	Push for regulation and advocate for this issue to be drilled down at the fourth/Nth party awareness and need for transparency. Regulations are emerging that support the right to audit/access as a right for outsourcers even when that type of leverage would otherwise have not existed within the outsourcer/vendor relationship. More of these types of discussions are being reported by customers, and vendors are beginning to understand the friction the lack of transparency and adherence to the outsourcer's risk control criteria is causing with their clients. Where customers and regulators mandate these solutions industry-wide, service providers who prove ineffective or ill-suited will experience greater impacts. Possible scenarios that can be exercised to achieve a useful shift in uncomplicating and protecting supply chains include reshoring (to a more favorable setting) and/or bringing tasks back in-house.
VENDOR MONITORING	*Pay attention to vendor intelligence.*	Intelligence gathering has to match your organization's risk appetite and tolerance. Mapping is essential at the down chain level to allow you to carefully determine why you need to do a down chain assessment. You have to know what that assessment can/will reveal, who/what/when/where/how your organization's IP, consumer data, and other critical elements are being managed, and how and by who that information is accessed and used.

GOAL ALIGNMENT	*Pay attention to business intelligence.*	*As with vendor intelligence, an understanding of the project goals of business units enterprise-wide must be achieved and how those goals relate to their vendors and the risks being managed. This understanding requires looping in the other business units that support those units, such as procurement or resilience, IT and security.*
TALENT	*Address skill set gaps.*	Inexperienced risk assessors provide results that are less than optimal. Push for education and soft skills across the organization and ensure that third/fourth/and Nth parties have the right skills to mitigate risk. Every role within ERM/ TPRM has to understand these factors and be able to articulate the issues and solutions (board, C suite, through practitioners, and auditors).

Conclusion

A daisy chain exists of both vulnerabilities and opportunities for strengthening the ecosystem. Lurking among these supplier networks are undefined risks (e.g., the unknowns of the Nth parties). Gaining a holistic view and a tangible grasp of the viability, measurable scope, and practical impacts of the use of Nth parties is essential for robust TPRM. Without this level of assessment, material fourth/Nth parties can wreak havoc. The presence of this type of undefined risk is simply untenable.

Overall, the risk environment is largely reactive across all industries. We've experienced this hard reality in the pandemic setting (just for example, the increased risks presented through Work From Home/Work From Anywhere settings). The pandemic and other socio-economic and environmental impacts are so great that we can no longer afford not to know about fourth/Nth parties and their controls. We are unaware of those connections and relationships until we are impacted – an untenable reactive stance.

To gain a stronger, more proactive and scalable means of improving visibility and transparency, the following considerations can be combined with the recommendation in Table 1 to help gain a more holistic view of the supply chains:

- **Adopt a "Trust, but Verify" approach to risk intelligence** to see what companies are interacting with third parties. It is the outsourcer's responsibility to know what down stream Nth parties are used. Adding a proactive "verify" approach that also incorporates open source intelligence. Add open source and other continuous monitoring to processes going forward if that approach is not already being used.
- **Conduct a higher level of assessment that goes deep** across a wide breadth of services. Use the information gained to build a concrete plan of action that links supply chain risk management to contractual obligations. An inventory diagram needs to go down to levels that adequately depict where the egress/exit points across the chain. All the potential uses/transfer/receipt of data points have to be depicted, acknowledged, and verified. This is another way to identify where Nth parties are present in the supply chain.
- **Evaluate contracts from the product/service/systems level to assure controls are appropriate.** This effort can be hampered if the assessment and early negotiations are not responsive to the specific context in which a vendor is used. For instance, an outsourcer using a vendor for electronic storage of documents/data may not take into account the cloud storage risks posed by that relationship.
- **Remain engaged with business units across the enterprise** to heighten awareness of what is coming up on their radar. Inquire as to what projects they intend to roll out and what vendors they are investigating to be hosting and managing those projects. This provides added value to the third party risk management program to advise and support in their efforts.

The circular nature of supply chains impacts delivery and availability throughout the entire chain. Taking a proactive stance now will provide many opportunities, including being ready to respond to regulatory changes that are beginning to reverberate across industries. Overall, change the company culture to adopt a "Follow the (Service/Product/Data) Flow Perspective." When examining flow, look at several points in the lifecycle – pre-engagement (define vulnerabilities and possibilities); monitoring after onboarding; and when there are termination/offboard moments (for any reason). Be sure to up the stakes for what qualifies a vendor as "high/extreme criticality" wherever that is warranted throughout the chain. Resources can be focused on the outsourcer's most critical vendors.

Practitioner Resources

Two templates are available that can aid practitioners in their Nth party mapping and tracking efforts. These templates may be utilized in any setting, and the templates can be tailored to the needs of the outsourcer.

- The Shared Assessments' Target Data Tracker (TDT) can provide a starting point for organizations. The TDT is a data governance tool that enhances your due diligence artifacts to document and manage third party relationships.
- The Shared Assessments' Assessment Leveraging Tool – The Due Diligence Verification Checklist (Excel template) The checklists are designed for practitioners to house a consolidated record of the control assessments for each third party (and that provider's fourth and Nth parties).

Other practitioner resources include:

- Adaptive Risk Management for Complex Supply Chains briefing paper.
- Using the SCA with other Complementary Types of Assessments to Streamline Due Diligence white paper and practitioner guideline tool.
- Work From Anywhere (WFA) – Upstream Impact of Downstream Lapses blog and guideline tool.
- KRIs for Vendor Performance blog.
- Nth Party Risk Concepts – How Low Should You Limbo? Blog.
- Shared Assessments TPRM Framework – Module 1 TPRM Basics (re: vendor inventories & registers).
- Shared Assessments TPRM Framework – member only access: Module 6 on Due Diligence; Module 7 Contracts.
- Crisis Management and Communications: Prepared Makes Perfect Blog.

Acknowledgments

This is one of series of best practices resources for Third Party Risk Management. We thank the Shared Assessments Best Practices Group volunteer subcommittee members who conducted this effort:

- **Jolanta Broslawik**, Senior Manager - Vendor Technology Risk Mgmt, Charles Schwab & Co., Inc.; Project Member Co-Lead
- **Kaelyn Lewis**, Senior Risk Analyst, Rochdale Paragon (apogee iQ); Project Member Co-Lead
- **Phil Bennett**, Manager, Information Security Metrics and Analytics, Navy Federal Credit Union
- **John Bree**, Chief Evangelist – Supply Wisdom (NeoGroup)
- **Laura DeWert**, Vendor Risk Analyst, BMW Financial Services N.A.
- **Angela Dogan**, Founder & CEO, Davis Dogan Advisory Services, LLC
- **Nasser Fattah**, Cybersecurity and Vendor Risk Management Leader in the Financial and Health Industry
- **Brenda Ferraro**, VP of Third-Party Risk, Prevalent, Inc.
- **Alpa Inamdar**, Head of Third Party Governance Line of Business Administration, BNY Mellon Corporation
- **Emily Irving**, VP RQA, Third Party Risk Management, BlackRock, Inc.
- **Sri Kaza**, Senior Compliance Analyst, State Farm Mutual Automobile Insurance Company
- **Paul Poh**, Managing Partner, Radical Security
- **Michael Riecica**, Director, Security Strategy and Risk, Rockwell Automation, Inc.

We would also like to acknowledge The Santa Fe Group, Shared Assessments Program subject matter experts and other staff who supported this project:

- **Bob Jones**, Senior Advisor
- **Charlie Miller**, Senior Advisor
- **Gary Roboff**, Senior Advisor
- **Marya Roddis**, VP Technical Writing; Editor

About Shared Assessments

The Shared Assessments Program is the trusted leader in Third Party Risk Management, with resources to effectively manage the critical components of the Third Party Risk Management lifecycle.

Program resources are creating efficiencies and lowering costs for all assessment participants; kept current with regulations, industry standards and guidelines and the current threat environment; and adopted globally across a broad range of industries both by service providers and their outsourcers.

Shared Assessments offers opportunities for members to work alongside peers to address global risk management challenges through committees, awareness groups, interest groups and special projects.

For more information on Shared Assessments, please visit: https://www.sharedassessments.org.

About DVV Solutions

Established in 1999, we have become one of the UK's leading providers in the design, implementation and management of Third Party Risk Management (TPRM) and assurance services.

We have a proven model for Third-Party risk reduction and mitigation. Our suite of consultative and managed services improve your ability to manage increasing complexity of third-party and supply chain risks backed by leading risk intelligence and automation platforms.

As a Shared Assessments Program member and registered Assessment Firm we utilize industry standard practices including Standardized Information Gathering (SIG) questionnaires, the Data Privacy Tool Kit and Standardized Control Assessment (SCA) for onsite audits.

For more information on enhancing your third-party risk and cybersecurity assurance:

Call Us: +44 (0)161 476 8700

Contact Us: Complete our Contact Form, or

Learn more about What We Do

Disclosure: The content of this series is not intended to convey or constitute legal advice, is not to be acted on as such, and is not a substitute for obtaining legal advice from a qualified attorney. These materials include the strategic and tactical processes deemed the most generally applicable to and useful for the most parties, both outsourcers and third parties. This material is not intended to be inclusive of every case required by statute or regulation for any specific industry, nor those mandated by any and all industry standards.