Continuous Monitoring of Third Party Vendors: Building Best Practices

A Shared Assessments White Paper

SHARED ASSESSMENTS

Abstract

Continuous risk monitoring is an essential strategic component of a robust third party vendor risk management program in a dynamic operational environment. Continuous monitoring, a subset of ongoing monitoring, moves the risk posture of systems to a level that allows tracking over time, often in real-time, to raise awareness of changing vulnerabilities and processes and provide for more effective decision-making regarding third party risk.

Choosing the right indicators to monitor is also critical for a well-developed program, as ongoing monitoring of ineffective controls provides for an inadequate sense of security. Both regulated and unregulated sectors have definitions regarding third party vendor risk and associated monitoring. For instance:

- Regulators in the US and other countries have issued bulletins regarding the defined roles and responsibilities placed on organizations for due diligence on third party vendors that perform or support essential operations. This focus on third party risk mandates that organizations evaluate and monitor providers throughout the life of the relationship and defines rules surrounding senior management, systems and controls.[1]
- Non-regulated industries commonly employ monitoring for third party risks that include such diverse indicators as third party production line quality, physical access controls and network systems intrusion detection.

The Shared Assessments Best Practices Awareness Group undertook this paper with the following objectives:

1. Provide an introduction to the underlying methodology, tools and definitions, so the stakeholders within a third party risk manager's own organization are better equipped to frame discussions and evaluate what implementing continuous monitoring would look like for their individual organization; and
2. Explore risk areas involved in continuous monitoring and identify cost-effective solutions for implementation.

Organizations that make continuous monitoring a part of their holistic security, lifecycle-based risk management program that is designed in alignment with the organization's overall business objectives would be expected to improve their ability to track and monitor critical third party vendor metrics, improve identification and proactive planning for remediation of issues as they arise and, therefore, reduce the impact of events that do occur.

This initial paper focuses primarily on information security, which lends itself more readily to continuous monitoring, as these processes are already automated. Papers with increased depth on this topic will be published over time for more mature Third Party Risk Management (TPRM) programs. In addition, future papers will examine the emerging movement toward a more integrated ecosystem model, in which threat intelligence and information sharing (e.g., FS-ISAC and others) become key to gaining greater value from long term continuous monitoring.

Issue Landscape

This paper provides an introduction to and definition of ongoing and continuous monitoring for third party risk managers and other stakeholders within an organization. Continuous monitoring is a growing topic of interest in the third party risk management landscape. The need for and value of continuous monitoring are demonstrated in recent surveys of vendor risk management practices. These reports provide insight into opinions regarding efforts to standardize practices, policies and controls to consistently evaluate service providers: :

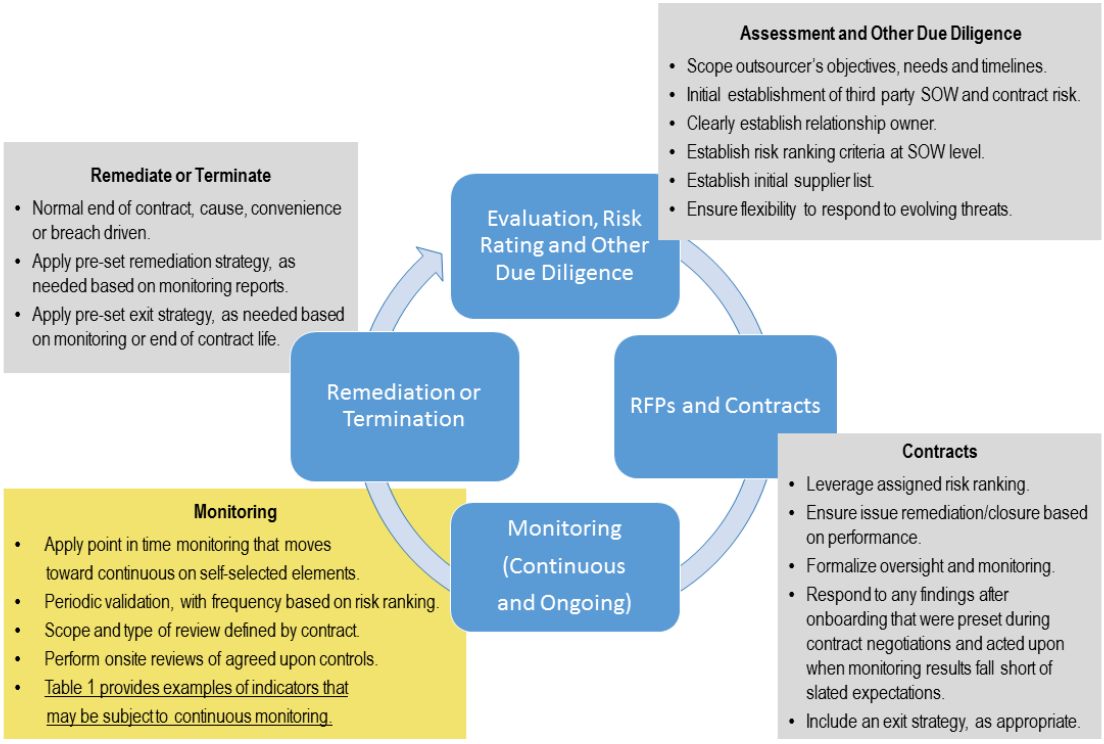
- While 59% of respondents indicated a desire to track/monitor their third parties, just 22% were tracking with monthly or greater frequency.
- 82% of respondents ranked the need to ensure that regulatory compliance requirements are being met as a critical or high priority.
- 65% of respondents predicted major or moderate benefits to their ability to compare security postures among third parties through the tactical advantages gained from utilizing continuous third party monitoring.[2]
- 44% of respondents viewed reliance on subjective data as a challenge in vendor risk managements.
- 38% of respondents identified lack of real-time information about vendor/supplier risk posture as an issue.[3]

1 *SYSC 8.1 General Outsourcing Requirements.* May 2016. United Kingdom's Financial Conduct Authority (FCA); European Union (EU) Regulation 2016/679, better known as the General Data Protection Regulation (GDPR). April 14, 2016. Effective May 2018. EU Parliament; *FFIEC Information Technology Examination Handbook. Appendix J: Strengthening the Resilience of Outsourced Technology Services*. FFIEC. November 2015. [Federal Financial Institutions Examination Council (FFIEC) includes five banking regulators: Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of Currency (OCC), and the Consumer Financial Protection Bureau (CFPB)]. *Third-Party Relationships: Risk Management Guidance*. Office of the Comptroller of the Currency (OCC). OCC Bulletin 2013-29. October 30, 2013; *Third-Party Relationships: Risk Management Principles*. OCC Bulletin 2001-47; OCC Advisory Letter 2000-9; February 2015; *Commission Delegated Regulation (EU) 2015/35*. October 10, 2014. Official Journal of the European Union. January 17, 2015; *AT 9 Outsourcing*. August 15, 2013. Germany's Federal Financial Supervisory Authority (BaFin); *Outsourcing Risk Management*. Monetary Authority of Singapore (MAS), March, 2013.

2 *Continuous Third-Party Security Monitoring Powers: Business Objectives and Vendor Accountability.* BitSight Technologies. January 2015.

3 *Don't Let "Trusted" Vendors Become Cyber-Breach Enablers.* International Data Group (IDG) and BitSight Technologies. May 2016.

Definitions: Continuous monitoring has evolved from traditional auditing and other assessment processes. It is a part of an integrated, disciplined process that involves a strategically designed and implemented risk management framework. Together with the other components of the framework, continuous monitoring supports an enterprise-wide, robust approach to the vendor risk management lifecycle that effectively combines compliance requirements with operational security needs. For the purposes of discussion, within this paper the definition distinguishes continuous monitoring as a subset of all monitoring, including ongoing monitoring. Ongoing monitoring generally lacks the timeliness and level of granular visibility required for proactive response to issues that continuous monitoring can provide. The diagram below depicts the role of continuous monitoring within the third party risk management cycle. Areas for continuous monitoring, as they relate to risk management, appear in the highlighted box in the graphic below. Table 1, at the end of this document, further describes these risk areas.



Continuous monitoring has its own formal definition in some sectors, including financial services, healthcare, defense and utilities, as well as within many industry verticals in the form of generally accepted standards. For example:

- CIO .gov defines continuous monitoring as "a risk management approach to cybersecurity that maintains an accurate picture of an agency's security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implemented prioritized remedies."[4]
- Under the COSO Framework, continuous monitoring is defined as "the process and technology used to detect compliance and risks associated with an organization's environment (financial and operational – which is comprised of people, processes, and systems)."[5]
- NIST defines continuous monitoring generically as "maintaining ongoing awareness to support organizational risk decision-making by maintaining ongoing awareness of information security, vulnerability, and threats to support organizational risk management decisions."[6]

4 *Continuous Monitoring.* CIO Council. April 2016. https://cio.gov/protect/continuousmonitoring/
5 *Internal Control – Integrated Framework: Guidance on Monitoring Internal Control Systems.* Committee of Sponsoring Organizations of the Treadway Commission (COSO). January 2009.
6 Johnson, L. Arnold. *Information Security Continuous Monitoring.* NIST Special Publication 800-137. December 14, 2010.

Monitoring (both ongoing and continuous) is often viewed as being primarily concerned with data security controls. However, increasingly, risk managers recognize that not only is there a need to respond to the shift in regulated industries that requires monitoring to extend beyond cyber security; there is also the need for scoping that includes risk rating during vendor onboarding. Such scoping allows for a clear determination regarding each vendor and what indicators will be assigned to continuous monitoring. Indicators may include financial and operational stability, business and technology resiliency, regulatory compliance and other specific risk categories that could affect the outsourcer's own operations and long term viability. Adequacy of monitoring frequency for any given indicator can be determined by context to ensure that security controls are assessed and reported against each individual organization's specific regulatory environment and risk appetite. Such planning requires communication between risk managers and IT staff to ensure that continuous monitoring metrics are set that are realizable through automated or manual testing.

Continuous Monitoring Goals: Continuous monitoring is an important step away from compliance programs that are implemented using a check-the-box approach. "The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur."[7]

In a dynamic and demanding risk environment, continuous monitoring can provide valuable communications tools and insights that reveal a more comprehensive, real-time or close to real-time picture of the vendor and, therefore, the organizational security posture of that vendor. Strategies for monitoring should be evaluated whenever changes occur to business elements (both internal and external), such as core mission, risk tolerance or business processes, to ensure that controls function appropriately and any new gaps are identified.

The Shared Assessments Best Practices Awareness Group undertook this paper with the following objectives:

1. Improve situational awareness, in order to provide for greater protection of operational, strategic, reputational and resiliency risks through early (real-time) identification of issues as they emerge.
2. Identify issues before they become problematic.
3. Improve response processes and remediation times, as needed.
4. Be part of incident response planning.
5. Be part of vendor onboarding, utilizing pre-determined, organizationally-defined risk categories and monitoring strategies that are tied to the types of risk related to a given vendor.
6. Balance return on investment, including capability and costs of static assessments against ongoing and continuous monitoring costs, relative to potential costs of risk related to each vendor.
7. Provide risk and compliance (dashboard) reporting that is appropriate to the environment, as required to address regulatory requirements and associated reporting, as well as organizational risk, action, management reporting and business resilience reporting issues.

> *"A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static and occasional security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to senior leaders. Senior leaders can use this information to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of their information systems."*
>
> National Institute of Standards and Technology

Operational Processes: To achieve a defense-in-depth level of continuous monitoring capability, all aspects of operations should be involved, including people, processes and technologies. Continuous monitoring requires establishment of responsibility and accountability that involves senior information officers (CISO, CIO, CRO), as well as information system owners, common control providers and business line owners across the organization.[8] This challenges leadership to set clear risk and control priorities and communicate them enterprise-wide, as well as to vendors and other stakeholders. This approach also follows the "*trust, but verify*" model by establishing measures and metrics that are monitored on pre-determined frequencies in addition to the initial vendor assessment performed at time of onboarding.

Table 1, located at the end of this document, describes key indicators that may be susceptible to continuous monitoring and corresponding techniques for tracking those indicators. The techniques use measures for identifying weaknesses in current controls, as well as evaluating current threats and vulnerabilities to critical security functions and information systems. Organizations can use this table to add dimension to their TPRM planning processes to optimize continuous

7 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.* NIST Special Publication 800-37, Revision 1. National Institute of Standards and Technology (NIST). February 2010; *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST Special Publication 800-53, Revision 4. April 2013; *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.* NIST Special Publication 800-137. September 2011.

8 The term common control provider refers to the internal or external organization, group or individual(s) responsible for the overall development and implementation of security controls that provide controls to protect organization information systems using a centrally managed approach. Such controls may be manual or automated.

monitoring of third parties. As a continuous monitoring methodology is developed, the quality of deliverables to be monitored will be determined based on unique factors of each given relationship. The number of vendors may influence the need to determine which vendors are material to business lines in a manner that is tied to risk rating, rather than rating all vendors for continuous monitoring.

Factors that can be useful in developing an effective program include:

- Establishing an inventory of vendors that includes ranking and defines monitoring categories with anticipated monitoring frequencies for each category.
- Determining whether business continuity program elements will be evaluated in real-time. For instance, monitoring the frequency of disaster recovery drills, records of customer complaints to the FTC or other national or international regulatory bodies, such as the new European Data Protection Board, as well as negative press that may indicate financial or reputational stressors that a vendor is facing.[9]
- Determining what 'rules' are or can be used to set a benchmark for meaningful monitoring.
- Defining who owns which processes, noting that ultimately management owns the process, first line owns risk and second line performs the monitoring function.
- Building monitoring and oversight into contracting, with specific definitions for continuous monitoring included in the contract.
- Further areas to consider that may require additional actions:

    1. Data – Determining vendor types, noting how and what each vendor is doing changes the view of what data may require examination; for instance, understanding how the vendor accesses and processes data and how this relates to your organization's overall control posture is important to know.

    2. Analytics around Data – Developing a solid continuous monitoring program is a process, which requires resources, feedback and meaningful analytics that support actionable alerts only on meaningful incidents. As continuous monitoring evolves, automation will be a challenge that industry must meet. As automated systems further reduce manual effort by providing a vehicle for continuous monitoring implementation in information systems, the result can be vastly more detailed and timely information. Some aspects of vendor risk management and third party oversight, such as file processes and security risk issues, those that can be identified by pattern recognition, endpoint profiling and use of threat intelligence, lend themselves to ongoing and continuous monitoring. Other items for ongoing monitoring would include measures of organizational resiliency at the third party level, such as indicators like mergers and acquisitions and other announcements or information that might indicate changes or potential changes to the financial health of the organization. Examining how automation will take place can lead to pertinent and important changes in Service Level Agreements (SLAs).

References for establishing best practices around continuous monitoring can be drawn from a number of sectors and demonstrate how each industry's approach has improved over time to yield more effective information gathering and analysis. For example:

- One challenge historically has been monitoring in the financial securities space, where an abundance of orders made it difficult technologically to distinguish during analysis between events and false positives (such as a legitimate transaction identified as anomalous).
- Recent testimony to US Federal Energy Regulatory Commission (FERC) exemplifies how regulators in a variety of sectors are focusing on supply chain risk management guidelines.[10]

Adopting advances in continuous monitoring practices that are based on such existing examples that can be extended to other verticals will allow risk managers and senior executives to meet organizational due diligence and monitoring goals more efficiently and effectively.

Operational impacts of implementing a continuous monitoring program that provides information which can be analyzed and used to guide decision-making can be significant. As part of ongoing monitoring, continuous monitoring looks at defined aspects of vendor relationships at predetermined frequencies (e.g., real-time, quarterly, etc.), including: determining which vendors are subject to continuous data analysis; what monitoring results are deemed to require immediate attention, action and escalation; and providing a system of preparedness focused on being able to respond effectively.

9 Under the new GDPR, the Article 29 Working Party will transition to become the European Data Protection Board, with more independence and power. Its primary task will be ensuring the consistent application of the new regulation. *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*. Article 29 Working Party. Brussels. Adopted April 13, 2016.

10 *CIP Supply Chain Risk Management* (RM 15-14-000). Statement by Jacob S. Olcott, BitSight Technologies. January 28, 2016.

Timeframes for continuous monitoring may be based on generally accepted practices and could include security engineering and direct data gathering, Security Incident Event Management (SIEM), Security Content Automation Protocol (SCAP), vulnerability scanning, configuration management, Intrusion Detection and Prevention Systems (IDS/IPS), management dashboards and other reporting. A more robust approach can also include tracking for reputational reports, such as news of acquisitions or breaches involving big data and operational metrics and triggers. Types of stress testing can include, but should not be limited to, scenario analysis, model validation and governance, risk, financial and workflow module monitoring. Regarding frequency, legislation allows for what most effectively manages risk. For example, "As long as controls selected and implemented are assessed for effectiveness during the required authorization cycle to demonstrate security due diligence, OMB and FISMA requirements are satisfied."[11]

A common platform firm must:
(1) when relying on a third party for the performance of operational functions which are critical for the performance of regulated activities, listed activities or ancillary services on a continuous and satisfactory basis, ensure that it takes reasonable steps to avoid undue additional operational risk;
(2) not undertake the outsourcing of important operational functions in such a way as to impair materially: (a) the quality of its internal control; and (b) the ability of the appropriate regulator to monitor the firm's compliance with all obligations under the regulatory system and, if different, of a competent authority to monitor the firm's compliance with all obligations under MiFID.

UK Financial Conduct Authority (FCA)

Benefits

A well-designed continuous monitoring program can provide a real-time or close to real-time picture of the state of security both internally and externally at the third party level, allowing an organization to move from reactive, when events occur, to proactive information gathering and analysis. It can also provide reporting that allows an organization to assess the effectiveness of a given set of vendor controls and communicate that information in a timely manner, allowing for remediation based on a pre-planned response, which can lead to improved outcomes when an incident does occur.

Recent surveys reveal that organizations anticipate major or moderate improvements from continuous monitoring of vendors, which include the ability to:

- Compare security postures.
- Screen vendors more effectively based on real-time risk.
- Evaluate infrastructure configurations.
- Reduce the amount of time required for security event identification, remediation and responses.[12]
- Improved working relationships, both in-house and with vendors and other stakeholders.
- The ability to consistently prioritize vendors based on the risk they pose.
- Improvement of the outsourcer's risk posture.[13]

Other benefits of continuous monitoring can be expected to include improved operational and security efficiency that result in:

- Refocused resource use that results in operational optimization, through more efficient and effective monitoring of only the most relevant information sets and elimination of redundancies throughout the risk management system.
- Continuous visibility of issues that drives improved risk prioritization and response to issues.
- Leveraging of common control providers.

As the OCC has stated in guidance over more than a decade: "Proper and complete documentation and reporting is the only way to demonstrate the level of accountability, monitoring and risk management required to manage third-party risk." The OCC further notes that monitoring should be included as part of the onboarding contract process, as: "… without a repeatable, automated process in place that incorporates best practices, organizations cannot create sustainable vendor lifecycle management programs.[14]

11 *Continuous Monitoring: Frequently Asked Questions*. National Institute of Standards & Technology (NIST). June 1, 2010.
12 *Continuous Third-Party Security Monitoring Powers: Business Objectives and Vendor Accountability*. Forrester. January 2015.
13 *Don't Let "Trusted" Vendors Become Cyber-Breach Enablers*. International Data Group (IDG) and BitSight Technologies. May 2016.
14 *Third-Party Relationships: Risk Management Guidance.* Office of the Comptroller of the Currency (OCC). OCC Bulletin 2013-29. October 30, 2013; *Third-Party Relationships: Risk Management Principles.* OCC Bulletin 2001-47; OCC Advisory Letter 2000-9.

Conclusion and Next Steps

The evolving standard of care for continuous monitoring goes beyond a moment-in-time snapshot and is changing to represent real-time or near real-time testing and evaluation of controls in an operational setting. Though there are some emerging best practices and guidance that organizations are providing to each other about what they each do in specific circumstances, ultimately, how and when to perform continuous monitoring is very much a company-by-company decision. Organizations seeking to achieve discernable gains in risk management will find improvement in early identification of issues with vendor security, privacy and other salient factors that can be expected to improve awareness and remediation.

It is crucial for any supply chain security standard to thoroughly address the criticality measure, including any third party that may pose significant risk to operations due to their access to sensitive data, essential nature of services and other criticality test indicators. Appropriate operational support in the form of structure and resources is required for such analysis and for continuous monitoring efforts to become effective. While larger organizations will be able to absorb the high cost of SIEM and threat intelligence software, cost remains a significant concern for smaller organizations.

This paper has discussed the general landscape of continuous monitoring. Additional papers are planned, which will examine in greater depth the implementation of continuous monitoring program design. As continuous monitoring takes greater hold across industries, the techniques and related guidance available for this level of real-time or close to real-time monitoring will increase and the Third Party Risk Management Continuous Monitoring Best Practices Guideline Tool (see Table 1) will be updated accordingly.

About the Shared Assessments Program

The Shared Assessments Program is the trusted source in third party risk management, with resources to effectively manage the critical components of the third party risk management lifecycle. These include: creating efficiencies and lowering costs for all 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 customers. Shared Assessments membership and use of the Shared Assessments Program Tools: The Agreed Upon Procedures (AUP); Standardized Information Gathering (SIG) questionnaire and Vendor Risk Management Maturity Model (VRMMM), offers companies and their service providers a standardized, more efficient and less costly means of conducting rigorous assessments of controls for cybersecurity, IT, privacy, data security and business resiliency. The Shared Assessments Program is managed by The Santa Fe Group (www.santa-fe-group.com), a strategic advisory company based in Santa Fe, New Mexico. For more information on Shared Assessments, please visit http://www.sharedassessments.org.

Thank You to Our Contributors

This is the first of a series of papers on best practices in third party risk monitoring. We'd like to thank the Shared Assessments Best Practices Group volunteer subcommittee members who conducted this effort:

- **Barbara Cochran,** Third Party Risk Assessment Officer, US Bancorp
- **Sridhar Gundrothu,** Lead Solutions Architect Third Party Supplier Security, Genpact USA
- **Jeff Hill,** Product Manager, Prevalent, LLC
- **Gaurav Deep Singh Johar**, AVP, Enterprise Risk and Compliance, Genpact USA
- **Shawn Malone**, Vice President-Business Compliance, Radian Group Inc.
- **Anthony Manley,** Director, Vendor Management, MERSCORP Holdings, Inc.
- **Norman Menz,** CTO and Co-Founder at Prevalent, LLC
- **Jake Olcott,** Vice President Business Development, BitSight Technologies
- **Murali Vijendran**, Enterprise Security Services Leader, Genpact USA
- **Patrick Ward**, Former Senior Vendor Risk Manager, Santander Bank

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

- **Robert Jones,** Senior Advisor
- **Charlie Miller**, Senior Vice President
- **Marya Roddis**, Vice President of Communications

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.

SHARED ASSESSMENTS

Third Party Risk Management Continuous Monitoring Best Practices Guideline Tool *

Table : Key Monitoring Indicators Susceptible to Continuous Monitoring and Corresponding Techniques for Tracking those Indicators

Risk Area	Indicator	Techniques
Operations (or Business Lines) Integrity	• Is there litigation in process that names the organization or its key personnel? • Is there financial data that indicates potential changes in risk vulnerabilities? • Is there evidence of changes to core mission, business processes or enterprise architecture?	• Automated collection of publicly accessible data (news, data collection and reporting agencies, dashboard tool providers, etc.). .
Data Security Operations	• Does the third party meet its agreed upon schedule for security status reporting to the outsourcer (e.g., annual/semi-annual/quarterly)?	• Security Incident Event Management (SIEM) acknowledgment. • SIEM response summary reporting to applicable customer.
Data Security Environment	• Is there evidence of notification provided to the customer for all identified threats, alerts, incidents or breaches, in accordance with contract SLAs (e.g., the presence of remote access tools; data exfiltration; unauthorized malware access or resource abuse, such as: adware malware or malware servers; botnet infections; unsolicited communications; spam propagation; unvetted programs on corporate devices or user behavior events that evidence illegitimate file sharing)? • Are there unauthorized components or other risk vectors present, such as: improperly configured Sender Policy Framework (SPF) configurations; expired Secure Socket Layer (SSL) certificates; missing or altered application security headers; or unnecessary open ports? • Is there evidence of software patches and intrusion detection/virus prevention tool updates being applied, as needed, in a timely manner?	• Automated collection of publicly accessible data (news, data collection and reporting agencies, management dashboard tool providers, etc.). • SIEM response summary reporting to applicable customer. • Security Content Automation Program (SCAP) reports to applicable customer. • Applicable software non-perpetual licenses renewals (automated or manual).
Fourth Parties	• Are all parties that touch sensitive data identified and a risk assessment performed prior to gaining access? This includes all call and data centers, as well as other outsourced service providers. • Documentation of fourth parties that a vendor has changed or newly contracted with since the last assessment report? .	• Fourth party SLAs or contract template(s) that includes requirement of a TPRM program comparable to the vendor's obligation to the outsourcing customer in all risk areas identified as applicable for that vendor. • Automated collection of publicly accessible data (news, data collection and reporting agencies, management dashboard tool providers, etc.) that divulge fourth party relationships, even if the vendor has not divulged those to the outsourcer. • SIEM report documentation demonstrating follow through of reported material event(s).

*Organizations can use this table to add dimension to their TPRM planning processes to optimize continuous monitoring of third parties. This guide focuses on existing techniques that readily lend themselves to continuous monitoring efforts in the operational risk areas identified in this table. The risk areas are primarily concentrated around information security, for which processes are more often automated. This table will be updated over time to include techniques that emerge as technologies catch up with operational needs for continuous monitoring.