

## INNOVATIONS IN THIRD PARTY CONTINUOUS MONITORING: WITH A NAME LIKE OODA, HOW HARD CAN IT BE?



## TABLE OF CONTENTS

### TABLE OF CONTENTS

Executive Summary .....	3
Introducing Innovation into Continuous Monitoring .....	4
Continuous Monitoring and TPRM Program Governance .....	4
<i>Figure 1: Continuous Monitoring Processes across the Third Party Lifecycle</i> .....	4
Strategy versus Tactics.....	5
The OODA Loop - Defined.....	5
<i>Figure 2: The Parts of the OODA Loop</i> .....	5
The OODA Loop, Program Governance and Continuous Monitoring.....	6
<i>Table 1: Summary of OODA Loop Use to Guide Third Party Continuous Monitoring</i> .....	6
<i>Table 2: OODA Loop Stages in Static Environments versus Continuous Monitoring Environments</i> .....	7
Summary of the Benefits of Using the OODA Loop.....	8
Conclusion .....	8
Thank You To Our Contributors .....	9
About the Shared Assessments Program.....	9
Appendices .....	10
Appendix 1: Third Party Continuous Risk Management Guideline Tool.....	10
<i>Table 3: Applying the OODA Loop to Third Party Continuous Monitoring Solutions &amp; Governance Strategies</i> .....	10
Appendix 2: Tracking Roles in Continuous Monitoring.....	13
<i>Table 4: Tracking Continuous Monitoring Process Roles and Responsibilities across the TPRM Lifecycle</i> .....	13
Appendix 3: Definition of Key Terms.....	14
Appendix 4: References .....	15
Endnotes .....	17

## BUILDING BEST PRACTICES:

**INNOVATIONS IN THIRD PARTY CONTINUOUS MONITORING:  
WITH A NAME LIKE OODA, HOW HARD CAN IT BE?****Executive Summary**

The dynamic nature of the risk environment means that third party risk professionals are being asked to protect against growing threats with a finite number of resources.<sup>1</sup> In response to the need to be smarter about how we approach third party risk management (TPRM), this paper provides guidance, practical tools and insight into how to leverage an action-oriented emerging best practice to improve third party risk management.

Integrating the innovative best practice “OODA Loop” into continuous monitoring (CM) processes is ideally suited to maximizing TPRM program effectiveness, because the method stresses an action-oriented flexible and unconventional approach to risk management. The phrase “OODA Loop” refers to the “Observe-Orient-Decide-Act” decision cycle that was developed by military strategist and United States Air Force Colonel John Boyd.

The OODA Loop is an extension of systems theory, which defines common principles that govern the behaviour of entities and processes that may be, on the surface, widely different.<sup>2</sup> Boyd was a fighter pilot who revolutionized aerial warfare tactics in the 1950’s by applying the OODA Loop to the combat operations process in military operations.<sup>3</sup> The OODA Loop has already been extended from military settings to business settings and has been proven to allow for better continuous quality improvement (CQI) processes and more effective business governance.<sup>4</sup>

The key benefit of the application of the OODA Loop to continuous monitoring is the ability to improve program maturity for all third party risk teams. The OODA Loop can help teams to identify and act appropriately on monitoring third party risk alerts, know what the alert means, and who to engage to escalate or resolve a problem when it arises.

Using the OODA Loop can:

- 1) *Improve situational awareness* to provide for enhanced mitigation against operational, strategic, reputational, cyber and resiliency risks through early identification of and appropriate action on risk indicators.
- 2) *Improve cost/reward (i.e., return on investment)* by maximizing the impact of near real-time mitigation opportunities that continuous monitoring offers.
- 3) *Potentially reduce compliance costs* through implementation of risk management practices that are defensible to regulatory examiners and other authorities.

Third party risk professionals acknowledge the need for a more holistic, efficient and agile approach to TPRM across the third party relationship lifecycle.<sup>5</sup> Importantly, the OODA Loop model provides such an approach, as it contains both feedback and feed-forward processes, a combination that does not generally exist in other risk management models.<sup>6</sup> Feed-forward processes complement the more commonly applied feedback loop; and in combination these processes provide a stronger model for TPRM program improvements.<sup>7</sup> Feedback relies solely on cause and effect to improve system processes. Feed-forward loops provide guidance that allows third party professionals to utilize pre-determined choices in the event of a disruption without having to wait for confirmation or approval at key decision points. This feed-forward approach lets the third party professional work through a problem without having to worry about making a ‘bad’ decision that could have catastrophic consequences for operations, reputation and organizational resiliency. In these ways, integrating the OODA Loop model into existing TPRM programs can make a risk program more agile.

## Introducing Innovation into Continuous Monitoring

### Continuous Monitoring and TPRM Program Governance

Continuous monitoring<sup>8</sup> evolved from traditional risk and control assessment activities and has rapidly become a critical component of organizational third party enterprise risk and governance strategies.<sup>9</sup> Although the recent growth in continuous monitoring activities has been largely driven by cyber risk threats, the benefits of continuous monitoring are very broad and extend to almost all areas of TPRM program governance. Boards and C-level executives are re-examining their organization's risk appetite<sup>10</sup> and TPRM program effectiveness to better support their strategic business goals and to meet evolving requirements, in which including continuous monitoring in TPRM programs has started to emerge in regulations across the globe.<sup>11,12,13</sup>

TPRM program governance processes that are aligned with regulations and industry best practices include:

- Monitoring of third party performance and controls that utilizes pre-determined, organizationally-defined risk categories and strategies that are unique to the risks related to a third party, including monitoring of a third party's third parties (i.e., fourth parties, fifth parties...).
- Effective use of ongoing assessment and monitoring techniques to identify third party control weaknesses, once onboarded.

- The continuous monitoring solution being tied to review and escalation procedures that are appropriate to the risk presented by the third party relationship and the specific control requirements of the outsourcing organization.
- Prompt response to and management of any third party control issues or opportunities as they arise.
- Effective use of assessment results and decision making regarding such issues as whether to select a third party or use a second provider to mitigate risk, and for building effective management and exit strategies.

This move toward integrating continuous monitoring into third party oversight can help identify opportunities to mitigate an organization's operational risk<sup>14</sup> exposure from third parties. For example, continuous monitoring can identify in real or near real-time:

- The third party's ability to support the outsourcer's adherence to regulatory requirements or otherwise generate additional compliance risk.
- Changes in the third party's processes, personnel and/or technology that could inhibit execution of key organizational processes.

A guide to how continuous monitoring processes can be incorporated program-wide across the third party relationship is described in Figure 1.

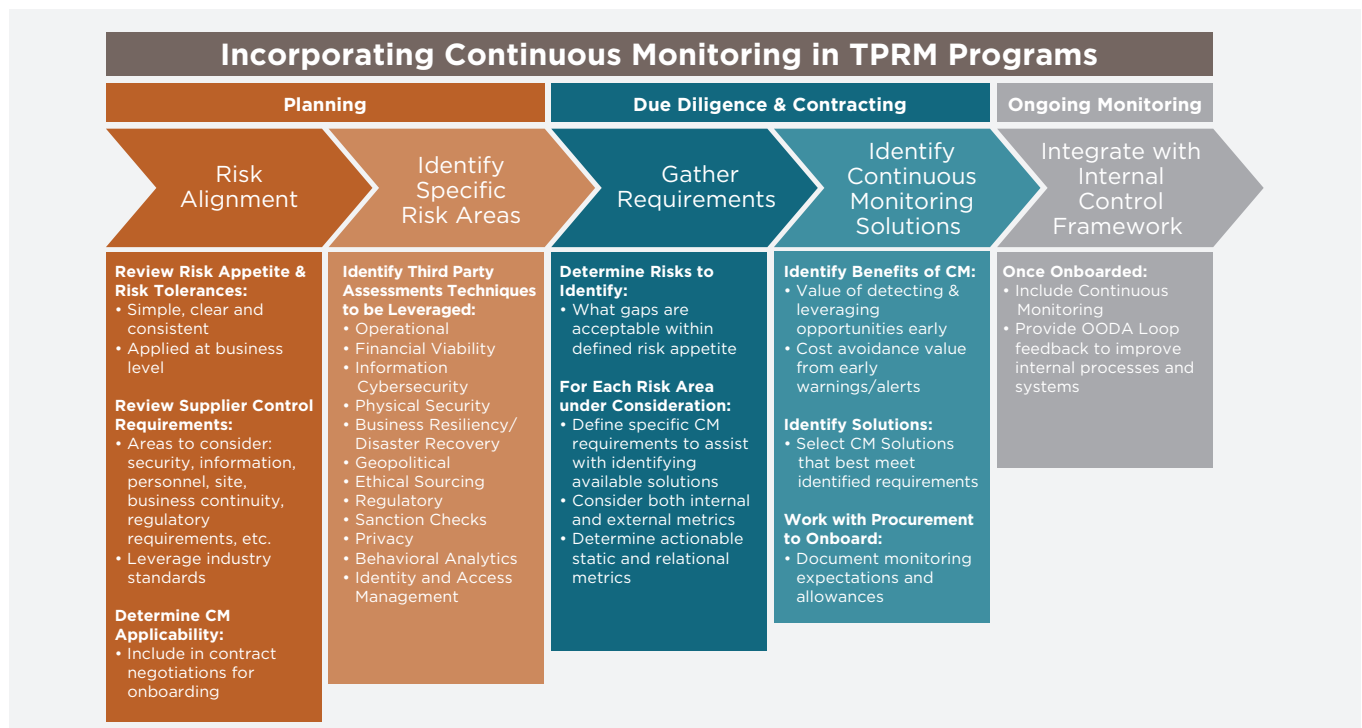


Figure 1: Continuous Monitoring Processes across the Third Party Lifecycle<sup>15</sup>



## Strategy versus Tactics

Continuous monitoring is a critical tactical solution integrated into the TPRM program strategy. There is a common misunderstanding surrounding the difference between strategy and tactics, often leading to techniques and reporting metrics being selected that may not meet an organization's strategic third party risk management goals.

- Strategy defines the organization's risk management goals; the tactics are the means by which those goals are achieved.
- Strategy encompasses the overarching plan; tactics are the operational tasks and processes carried out to support and implement the overarching strategy.
- Strategy and tactics work together, and tactics may be changed based on cause, effect, results and how closely the tactics align to and support the strategy.

Typically, incident response and management within TPRM programs are tactically-focused around a specific event. As a result, third party professionals are not leveraging lessons learned from these events and determining how to apply continuous improvement opportunities to TPRM processes program-wide.

## The OODA Loop - Defined

The OODA Loop is an optimal process for implementing continuous monitoring efficiently across the enterprise. The OODA Loop is a four-stage basis of any decision making process which gives a non-linear, proactive approach for problem solving in real life situations, including continuous monitoring.<sup>16</sup> As seen in Figure 2, the four stages can be seen relative to the parts of third party continuous monitoring (as noted in Figure 1): (1) definition of risk appetite, third party ranking, incident response planning; (2) assessment and monitoring; (3) incident analysis; and (4) incident response.

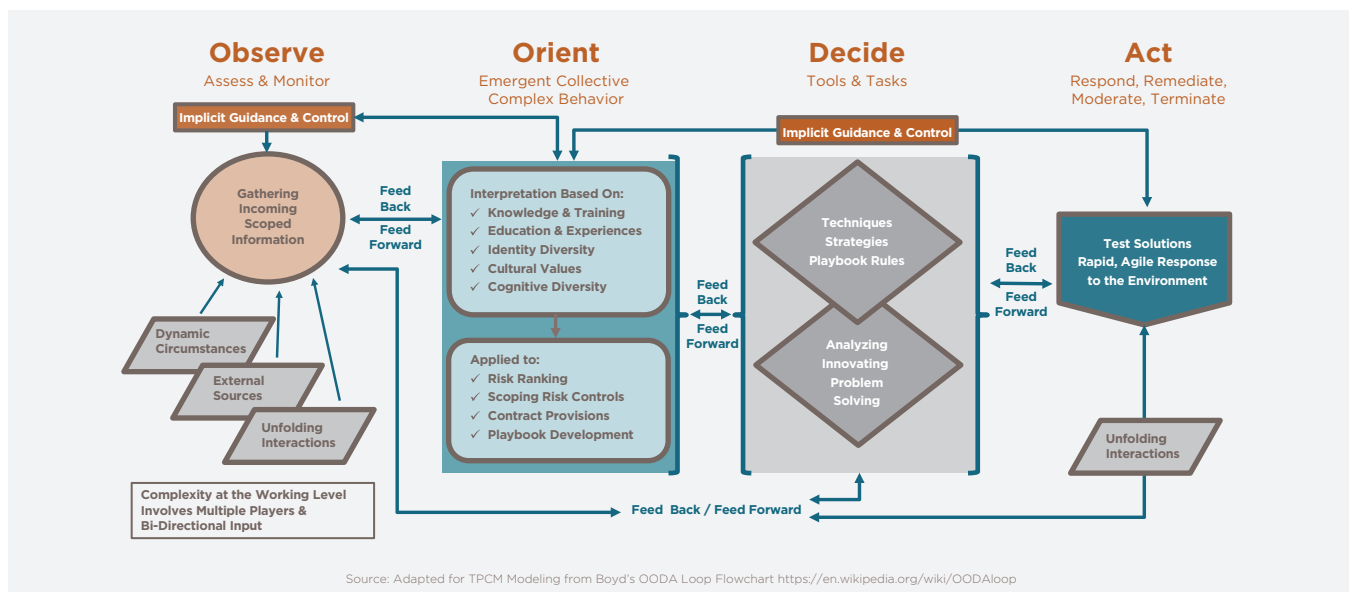


Figure 2: The Parts of the OODA Loop

The OODA Loop is the natural flow of human thinking and process; however, *it demands forethought, documentation and feedback, plus feed-forward processes to be effective and successful.* This means that decisions should be based on data that is pertinent, available, readily analyzed and actionable by third party risk professionals in ways that require the availability of implicit guidance – in other words pre-prepared guidance that has been practiced – that can be followed reliably at a moment's notice. The availability of implicit guidance eliminates the need to go back to a higher authority during a threat situation, making the response timelier and the risk professionals who need to make decisions more confident that their response is the right response. Implicit guidance, by its nature, requires training, so that the response is pre-planned and practiced and can be executed properly and in a more timely manner.

In the context of third party continuous monitoring, the use of implicit guidance is twofold:

1. The first use is for responsible parties within organizations to ensure that they have the availability of highly experienced analysts who have the ability to recognize a threat and act accordingly.
2. The second use is for leadership in an organization to ensure the availability of pre-defined actions that are linked to specific types of threats (also known as playbooks) that can guide less experienced analysts and also allow more experienced analysts to document their actions against policy and playbook processes.

## The OODA Loop, Program Governance and Continuous Monitoring

Continuous monitoring is most robust when the program employs strategies that are designed to work across the enterprise; a difficult task in any size organization. A strategy that calls for integrating the OODA Loop into continuous monitoring processes provides the type of collaboration throughout enterprise risk management to remedy the lack of coordination that typically functionally constrains the effectiveness and efficiency of TPRM programs. The need for this is demonstrated in the 7th Annual IT Audit Benchmarking Survey – Business and Digital Transformation’s Effects on IT Audit Groups report, which places “more partnering and collaboration are needed to counteract silo mindsets and behavior” as one of its key recommendations.<sup>17</sup>

Because of the level of information required to provide an agile response to near real-time events,

embedding the OODA Loop into TPRM programs can be expected to improve an organization’s risk posture by providing a more proactive approach to risk identification and management. A governance model that includes the OODA Loop empowers people. In the context of continuous monitoring, this type of governance leverages implicit guidance for the third party risk professionals who receive monitoring control data and reports, allowing them to go through a pre-determined loop without having to slow down or stop at key decision points. This approach lets them work through a problem avoiding bottlenecks that can have dire consequences for operations, reputation and organizational resiliency.

Table 1: Summary of OODA Loop Use to Guide Third Party Continuous Monitoring provides a cross reference by the four OODA Loop stages (observe-orient-decide-act). A more in depth, guideline version of this table is included in the appendices.

Table 1: Summary of OODA Loop Use to Guide Third Party Continuous Monitoring

OODA Loop Process	Strategic Considerations (Goals and Objectives)	Tactical Processes (Techniques and Tools)	Best Practice Considerations
<b>OBSERVE</b>	<ul style="list-style-type: none"> <li>Assess and monitor as appropriate to level of risk.</li> <li>Balance techniques versus technology.</li> </ul>	<ul style="list-style-type: none"> <li>Use a variety of information sources and types of assessments (both ongoing, point-in-time and continuous).</li> <li>Use a variety of types of assessments.</li> <li>Examples of methods: Automated controls testing; preventative and detective controls.</li> </ul>	<ul style="list-style-type: none"> <li>Establish documented criteria for transparent and uninterrupted monitoring.</li> <li>Develop common metrics to produce positive feeds that are important to the organization.</li> <li>Establish third party relationship management processes aligned with industry best practices, that include monitoring and effective use of information.</li> </ul>
<b>ORIENT</b>	<ul style="list-style-type: none"> <li>Tone at Top Strategic Guidance.</li> <li>Appropriate training in terminology, dashboards, escalation triggers, assessment and reporting use type.</li> </ul>	<ul style="list-style-type: none"> <li>Set Risk Appetite at business unit level.</li> <li>Include Continuous Monitoring in program design.</li> <li>Employ the OODA Loop throughout the process: 1) adjust filters as required; 2) determine if the risk appetite remains the same or shifts and act accordingly.</li> </ul>	<ul style="list-style-type: none"> <li>Establish defined and documented roles for all stages of governance and processes.</li> <li>Utilize the critical combination of feed back and feed forward.</li> <li>Determine how the data obtained during the observe stage is used.</li> </ul>
<b>DECIDE</b>	<ul style="list-style-type: none"> <li>Provide documented tools to guide analysis and other critical tasks.</li> </ul>	<ul style="list-style-type: none"> <li>Tools that are scoped to specified controls and provide for real-time autonomy in decision making.<sup>18</sup></li> <li>Tasks: <ul style="list-style-type: none"> <li>Use <a href="#">Vendor Risk Management Maturity Model (VRMMM)</a> Benchmarking.</li> <li>Static assessment processes.</li> <li>Continuous monitoring.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Communications has emerged as a key point, including dynamic playbooks; continuous feedback between units; when there are changes (circumstances, third parties, needs, etc.) share that information widely in the enterprise.</li> <li>Design playbooks to including incident management policies and exit strategies.</li> </ul>
<b>ACT</b>	<ul style="list-style-type: none"> <li>Combine feedback <b>and</b> feed-forward information to create greater value for TPRM program.</li> </ul>	<ul style="list-style-type: none"> <li>Respond, remediate, terminate.</li> <li>Start with highest areas of risk.</li> <li>Identify effectiveness gaps.</li> <li>Apply learnings for future decision making.</li> <li>Apply pre-determined remediation or exit strategy(ies).</li> </ul>	<ul style="list-style-type: none"> <li>Ensure relationship manager and others are automatically involved in incident escalation.</li> <li>Document continuous quality improvement (CQI).</li> </ul>

This proactive OODA Loop approach can be expected to improve the rewards of using continuous monitoring and the agility of decision making versus traditional (point in time) periodic assessment practices. The greater success of the monitoring process in the OODA Loop/Continuous Monitoring model is based on the

implicit guidance provided through the pre-determined risk appetite-based criteria and other documentation that supports the feedback and feed-forward processes. This is demonstrated in Table 2: OODA Loop Stages in Static Environments versus Continuous Monitoring Environments.

Table 2: OODA Loop Stages in Static Environments versus Continuous Monitoring Environments.

OODA Process	Non-ODA Loop TPRM Monitoring Environment	OODA Loop TPRM Monitoring Environment
<b>OBSERVE</b>	Static assessments show only point in time information.	Monitoring shows that a third party is experiencing difficulties that might lead to loss of service and potential increased risk.
<b>ORIENT</b>	Static change analyses will be delayed until a point in time report reveals a change.	This constitutes a status change that may or may not lead to an 'event'.
<b>DECIDE</b>	Changes can require high levels of resources to resolve when real or near real-time information is unavailable.	Decision may lead to third party risk professionals putting more 'eyes on the third party' or implementing additional controls, as well as exploring the possibility that a new provider might be required. <sup>19</sup>
<b>ACT</b>	Action is taking place based on old information, which may no longer be valid.	Actions taken by executing this process is outside most incident management; however, it fits into the OODA Loop approach to strategic governance.

Pre-established documentation describes specific expectations for each type of activity involved in establishing risk management policies and processes, implementing those processes, and the feedback that leads to program improvement over time. A playbook can be constructed that is appropriate for an organization's unique needs to provide a pre-determined set of rules defining roles, responsibilities, options, and guidance for responding to risk indicators, events or incidents. The playbook provides clear guidance and assigns responsibility for in-the-moment action setting the stage for ensuring that important decisions are made in a timely manner. Since time is the dominant factor in successfully executing a strategy in the TPRM space, where the threat environment is rapidly evolving, establishing playbook options helps to keep from getting hung up (delayed) at any point in the process.

To empower each team member, training should be conducted in which team members are able to demonstrate that they understand the goals, strategies,

rules of engagement (i.e., the playbook rules). Team members can then better advocate for individual commitment and enforcement by ensuring that those responsible for program management have the authority to execute changes that come to light over time through the feedback, feed-forward process. 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. Table 3: Applying the OODA Loop to Continuous Monitoring Solutions & Governance Strategies in the appendices provides a cross reference by the four OODA Loop stages (observe-orient-decide-act). Table 4: Tracking Continuous Monitoring Process Roles and Responsibilities across the TPRM Lifecycle can be tailored to the organization and used to record the roles and responsibilities for each task involved in the review of an organization's third party governance and monitoring solutions sets.

## Summary of the Benefits of Using the OODA Loop

Robust governance across the enterprise's TPRM program requires timely risk information, strong accountability, transparency and decisive approach to remediation. The key benefit of the application of the OODA loop to continuous monitoring and related governance is the ability for all third party risk teams to mature and employ monitoring without fear of not being able to act appropriately on monitoring alerts, not knowing what the alert means, or who to engage to escalate or resolve a problem when it arises.

Effective application of the OODA Loop in a continuous monitoring TPRM setting can:

- 1) *Improve situational awareness* through more effective training and planning enterprise-wide.
- 2) *Improve cost/reward (i.e. return on investment)* in terms of the improved insights (rewards) gained through continuous monitoring and agile decision making (costs) vs. traditional (point in time) periodic assessment practices.
- 3) *Potentially reduce legal and regulatory compliance costs* through demonstrated implementation of defensible risk management practices.

The OODA Loop can also be integrated into other monitoring processes within the third party lifecycle (e.g., program benchmarking, trust assessments, onsite/virtual assessments and other relevant monitoring sources).

## Conclusion

The integration of OODA Loop principles within continuous monitoring and related governance tactics provides more effective risk mitigation and decision making tools. The benefits of a consistently applied criteria and processes extend to both the outsourcer and the third party provider. Governance is naturally most effective when the outsourcer and third-party work as a team. Planning responses, rather than reactions, will allow the enterprise to take steps that achieve benefits, reduces threat impacts and associated risk management costs.

A robust TPRM would employ the OODA Loop throughout all phases of monitoring to help determine the value and limitations of continuous monitoring data, its implications and the capacity for providing feedback that dynamically improves the risk management program and overall TPRM governance and processes. When properly integrated into mature TPRM program and procedures, a well-designed, well-managed continuous monitoring program that embodies OODA Loop concepts, can effectively transform an otherwise static third party control assessment and risk determination process into a dynamic process that reduces risk and provides improved, timely control and corrective action status.



## Thank You To Our Contributors

This is one in a series of papers on best practices in third party risk management written and conducted by industry leaders who participate in Shared Assessments committees and working groups. We'd like to thank the Shared Assessments Continuous Monitoring Working Group volunteer subcommittee members who conducted this effort:

- **Eric Blatte**, President, RiskRecon
- **Hugues Bourassa**, Senior Assurance Advisor, Rio Tinto
- **John Bree**, SVP and Partner, NeoGroup
- **Jared Feinberg**, Senior Director, Threat Intelligence, Prevalent, Inc.
- **Martin Freeman**, Director, Cybersecurity and Compliance, Calastone
- **Bob Maley**, Former Global Head, Third Party Security and Inspections, PayPal, Inc.; Co-Chair, Continuous Monitoring Working Group
- **Caree Wagner**, Corporate Operational Risk Management – Third Party Operational Risk, BNY Mellon; Co-Chair, Continuous Monitoring Working Group

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

- **Mike Jordan**, Senior Director
- **Charlie Miller**, Senior Vice President
- **Gary Roboff**, Senior Advisor
- **Sylvie Obledo**, Project Manager
- **Marya Roddis**, Vice President of Communications, Editor

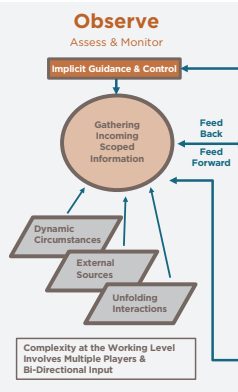
Join the dialog with peer companies and learn how you can optimize your compliance programs while building a better understanding of what it takes to create a more risk sensitive environment in your organization.

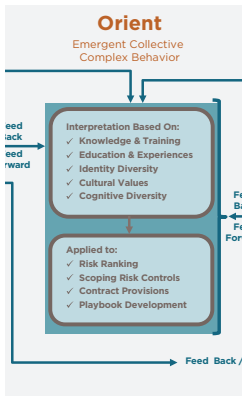
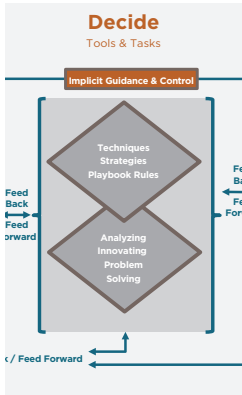
## About the Shared Assessments Program

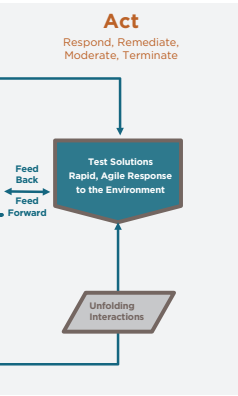
The Shared Assessments Program is the trusted leader in third party risk management, with resources to effectively manage the critical components of the third party risk management lifecycle. Program resources are: creating efficiencies and lowering costs for all assessment participants; kept current 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 customers. The Shared Assessments Program is managed by The Santa Fe Group ([www.santa-fe-group.com](http://www.santa-fe-group.com)), a strategic advisory company based in Santa Fe, New Mexico. Shared Assessments offers opportunities for members to address global risk management challenges through committees, awareness groups, interest groups and special projects. Our papers, articles and research studies are written and conducted by industry leaders – members of Shared Assessments Program Awareness Groups, The Santa Fe Group's partners, consultants and advisors – and cover the hottest, member-driven topics in risk management and business innovation. For more information on Shared Assessments, please visit: <http://www.sharedassessments.org>.

## Appendix 1: Third Party Continuous Risk Management Guideline Tool

Table 3: Applying the OODA Loop to Third Party Continuous Monitoring Solutions & Governance Strategies<sup>20</sup>

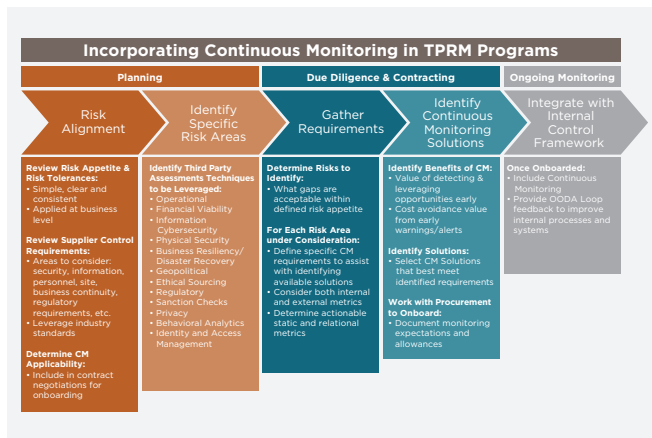
OODA Loop Reference Point	Strategic Approach	Tactical Processes	Best Practice Considerations
<b>OBSERVE</b>  	<ul style="list-style-type: none"> <li>Assess and monitor as appropriate to level of risk.</li> <li>Use a variety of information sources and types of assessments (both ongoing, point-in-time and continuous).</li> <li>Sufficiently support staff with appropriate resources at the operations, analysis and engineering levels</li> <li>Ensure that a robust corporate social responsibility policy trickles down into the procurement/sourcing through training and procedural mandates.</li> </ul>	<ul style="list-style-type: none"> <li>Balance techniques versus technology using appropriate advanced problem-solving tools, including use of algorithmic assessment and business analyst assessment to remove system noise.</li> <li>Examples of types of Information by risk domain: <ul style="list-style-type: none"> <li>Financial reports, including credit risk, labor costs and market fluctuations.</li> <li>Core security/IT risk management practice reviews, e.g., software hygiene, data protection, etc.</li> <li>Breach notifications.</li> <li>Geopolitical/Regional impacting events.</li> <li>Infrastructure risks, including physical security and production capacity.</li> <li>Service maturity, risks including services, technology or platform shifts, and patent filings.</li> </ul> </li> <li>Examples of assessments sources: Point-in-Time; Trust Assessments; Onsite Inspections; Audit reports (SSAE18, etc.); Third Party Audits, Assessments or Certifications (PCI-DSS ROC, etc.); Continuous Surface Risk Assessments; Automated publicly accessible data collection.</li> <li>Examples of methods: Automated controls testing; preventative and detective controls.</li> </ul>	<ul style="list-style-type: none"> <li><b>Establish documented criteria for transparent and uninterrupted monitoring.</b> Develop common metrics to produce positive feeds that are important to the organization.</li> <li><b>Establish third party relationship management processes aligned with industry best practices, that include:</b> <ul style="list-style-type: none"> <li><b>Monitoring of third party performance.</b></li> <li><b>Effective use of assessment results.</b></li> <li><b>Prompt response to and management of any third party performance issues.</b></li> </ul> </li> <li>Consideration of implementation and operational needs, including: <ul style="list-style-type: none"> <li>Data validation and volume.</li> <li>Data security environment.</li> <li>Integration of processes into existing solutions.</li> <li>Threat intelligence capabilities across all risk domains (dangerous conditions hunting, triage for vulnerability management).</li> <li>Governance and control points.</li> </ul> </li> </ul>

OODA Loop Reference Point	Strategic Approach	Tactical Processes	Best Practice Considerations
<p><b>ORIENT</b></p> 	<ul style="list-style-type: none"> <li>• Tone at Top Strategic Guidance with documented Implicit Guidance and Control Component.</li> <li>• Communicate across the enterprise: <ul style="list-style-type: none"> <li>○ Top to bottom/bottom to top.</li> <li>○ Clear communications.</li> <li>○ Appropriate training in terminology, dashboards, escalation triggers, assessment and reporting use type.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Risk Appetite Set by Group.</li> <li>• Include CM-by-design: <ul style="list-style-type: none"> <li>○ Preventative versus detective controls (e.g., Intrusion Detection System - IDS).</li> <li>○ Anti-Money Laundering (AML) analytics and reporting.</li> <li>○ Resolve known issues.</li> <li>○ Balance techniques versus technology.</li> <li>○ Support implementation operations.</li> </ul> </li> <li>• Employ the OODA Loop feedback loop throughout the process: 1) adjust filters as required; 2) determine if the risk appetite remains the same or shifts and act accordingly.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Establish defined and documented roles for all stages of governance and processes.</b></li> <li>• <b>Utilize the critical combination of feed back and feed forward.</b></li> <li>• Determine how the data obtained during the observe stage is used: <ul style="list-style-type: none"> <li>○ Detection and interdiction. Prevention of additional loss or damage.</li> <li>○ Predictive analytics. Develop historical data and predict patterns based on key indicators on both fraud and marketing.</li> <li>○ Ensure people with required training are in place; great data is only as good as the individuals who are analyzing that data.</li> <li>○ Keep training and scenario testing abreast with need as issues do not arise often and execution must be seamless.</li> <li>○ Where resources are not available internally, utilize appropriate external expertise.</li> </ul> </li> </ul>
<p><b>DECIDE</b></p> 	<ul style="list-style-type: none"> <li>• Provide documented guidance for analysis and other critical tasks.</li> </ul>	<ul style="list-style-type: none"> <li>• Tools: <ul style="list-style-type: none"> <li>○ Scoped to specified controls.</li> <li>○ Use Playbook for agile decision making.</li> <li>○ Tactical Playbook – If x, y, z, then a, b, c.</li> <li>○ Provide for real-time autonomy in continuous monitoring.</li> </ul> </li> <li>• Tasks: <ul style="list-style-type: none"> <li>○ Review incoming reports at pre-determined intervals that include trigger points.</li> <li>○ Annual SIG processes.</li> <li>○ TP analysis processes.</li> <li>○ Onsite/virtual control testing processes.</li> <li>○ Use VRMMM Benchmarking.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Communications has emerged as a key point, including dynamic playbooks; continuous feedback between units; when there are changes (circumstances, third parties, needs, etc.) share that information widely in the enterprise.</b></li> <li>• Playbook should include: <ul style="list-style-type: none"> <li>○ Incident management policies (from a BCP viewpoint).</li> <li>○ Exit strategies on third parties in extreme situations. Link up some real-time monitoring to playbook exit strategy(ies).</li> <li>○ Develop playbook options that are third party agnostic.</li> </ul> </li> </ul>

OODA Loop Reference Point	Strategic Approach	Tactical Processes	Best Practice Considerations
<b>ACT</b> 	<ul style="list-style-type: none"> <li>• Appropriate, Timely Action Through Clear Understanding of “Implicit Guidance &amp; Control”</li> <li>• Combined Feed Back – Feed Forward Creates Value.</li> </ul>	<ul style="list-style-type: none"> <li>• Respond, remediate, terminate.</li> <li>• Apply to risk assessment and audit lifecycles.</li> <li>• Start with highest areas of risk.</li> <li>• Identify effectiveness gaps.</li> <li>• Apply learnings to future OODA Loop cycles for future decision making.</li> <li>• Apply pre-determined remediation or exit strategy(ies).</li> </ul>	<ul style="list-style-type: none"> <li>• <b><i>Needs to be the cleanest part of the process from an intuitive viewpoint.</i></b></li> <li>• <b><i>Key that anything you are retrieving gets to the relationship manager and others involved in the escalation.</i></b></li> <li>• Document the type of continuous quality improvement (CQI) that is possible from this type of feedback in TPRM improves outcomes overall and allows the OODA Loop to work smoothly within the TPRM setting.</li> </ul>

## Appendix 2: Tracking Roles in Continuous Monitoring

Table 4: Tracking Continuous Monitoring Process Roles and Responsibilities across the TPRM Lifecycle



The chart below can be tailored to their own unique settings in order to assign and track roles and responsibilities for various aspects of continuous monitoring strategic planning, documenting requirements, solution selection, and integration within the organization's internal control framework. See Figure 1 for a full scale version of this overview graphic.

Risk Alignment	Assigned Process Owner	Identify Specific Risk Areas	Assigned Process Owner	Gather Requirements	Assigned Process Owner	Identify Continuous Monitoring Solutions	Assigned Process Owner	Integrate with Internal Control Framework	Assigned Process Owner
Review Risk Appetite & Risk Tolerances		Identify Appropriate Assessment Techniques		Determine Risks to Identify Gaps within Internal Guidelines		Document Benefits of CM		Perform Agreed Upon Continuous Monitoring	
Review Supplier Control Requirements				Define Specific Requirements for Each Risk		Identify CM Solutions		Provide Feedback into Internal Processes	
Determine Applicability of Continuous Monitoring				Define Actionable Metrics		Work with Procurement to Onboard			



## Appendix 3: Definition of Key Terms

**“Continuous Monitoring”** This is a subset of ongoing monitoring, and processes and provide for more effective decision-making regarding third party risk. Monitoring (both ongoing and continuous) is often viewed as being primarily concerned with data security controls. However, increasingly, third party risk professionals recognize that not only is there a need to respond to the shift in regulated moves the risk posture of systems to a level that allows tracking over time, often in real-time, to raise awareness of changing vulnerabilities industries that requires monitoring to extend beyond cyber security.<sup>21</sup> Continuous Monitoring of Third Party Vendors: Building Best Practices. The Santa Fe Group, Shared Assessments Program. Best Practices Awareness Group. 2017.

**“Continuous Third Party Risk Monitoring”** For the purposes of discussion, within this paper the definition distinguishes continuous third party risk monitoring as an uninterrupted, real-time (or near real-time) risk management approach designed to improve an outsourcer’s awareness related to their third party risks and potential control weaknesses as they emerge. This continuous monitoring approach is additive to more traditional assessment processes. It allows an organization to go beyond IT control monitoring to enhance their awareness of cybersecurity, privacy, technology, operational and strategic third party risk exposure.

**“Critical Activities”** apply to all industries and may be defined by either operational needs or by regulators. Critical activities are those that could cause significant risk if a third party fails to meet expectations; could have significant customer impacts; require significant investment in resources to implement the third-party relationship and manage the risk; or could have a major impact on an entity’s operations if the organization has to find an alternate third party or if the outsourced activity has to be brought in-house. A critical activity could enable specific oversight processes. For example, as defined by the Office of the Comptroller of the Currency (OCC), critical activities refers to significant bank functions, significant shared services or other activities that could cause a bank to face significant risk if the third party fails to meet expectations; could have significant customer impacts; require significant investment in resources to implement the third-party relationship and manage the risk; or could have a major impact on bank operations if the bank has to find an alternate third party or if the outsourced activity has to be brought in-house.<sup>22</sup>

**“Inherent Risk”** The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls). [Source: ISACA Glossary. ISACA. 2017.]

**“Operational Risk”** Third party operational risk (including IT and Infrastructure Risks, etc.) occurs when either a service provider or the outsourcer exposes an organization to direct or indirect losses due to inadequate or failed internal processes or systems.

**“Residual Risk”** A calculation of the risk that remains after mitigating controls have been applied.

**“Risk Appetite”** The level and type of risk an organization will take in order to pursue its strategic objectives.

**“Risk Appetite Statement”** A documented definition of the organization’s risk appetite.

## Appendix 4: References

For additional background on Continuous Monitoring, please see ***Continuous Monitoring of Third Party Vendors: Building Best Practices***, which provides an introduction to the underlying methodology, risk areas, tools and definitions. That paper includes a guideline table focused on existing techniques that readily lend themselves to continuous monitoring, which organizations can use throughout the relationship lifecycle to add dimension to their TPRM processes. ***Building Best Practices in Third Party Risk Management: Involving Procurement*** covers outsourcing due diligence considerations by the stage of the third party relationship lifecycle. Recommendations in the Involving Procurement paper include applying four guiding principles in the development of a holistic standards for vetting and onboarding third parties: consistency, objectivity, balance and management oversight.

Other Shared Assessments resources related to continuous monitoring include:

- ***Vendor Risk Management Benchmark Annual Survey***. Shared Assessments and Protiviti 2017 Research Study.
- ***Shared Assessments General Data Protection Regulation (GDPR): Data Processor Privacy Tool Kit***. 2018 Program Tool and Template Set.
- ***Risk Rating Third Parties: Optimizing Risk Management Outcomes***. 2017 White Paper.
- ***Evaluating Cloud Risk for the Enterprise: An Updated Shared Assessments Guide***. 2017 White Paper.
- ***Fourth Party Risk Management: Supply Chain Issues and Emerging Best Practices***. 2017 White Paper.
- ***Building Best Practices for Effective Monitoring of a Third Party's Incident Event Management Program***. 2015 White Paper.

Other, industry-specific guidelines for monitoring governance include:

- ***AT 9 Outsourcing***. August 15, 2013. Germany's Federal Financial Supervisory Authority (BaFin).
- ***Commission Delegated Regulation (EU) 2015/35***. October 10, 2014. Official Journal of the European Union. January 17, 2015.
- ***Cybersecurity Legal Task Force Vendor Contracting Project: Cybersecurity Checklist***. American Bar Association (ABA). November 2016.
- ***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. February 2015.
- ***New York State Department of Financial Services cybersecurity regulation 23 NY CRR500***. New York State Department of Financial Service. March 2017.
- ***Outsourcing Risk Management. Monetary Authority of Singapore*** (MAS), March, 2013.
- ***SYSC 8.1 General Outsourcing Requirements***. May 2016. United Kingdom's Financial Conduct Authority (FCA).
- ***Third-Party Relationship: Supplemental Examination Procedures Bulletin***. OCC 2017-7. January 2017.
- ***OCC Advisory Letter 2000-9***; February 2015.
- ***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.

Other OODA Loop and Strategic Planning references:

- Richards, Chet. *Certain to Win: The Strategy of John Boyd Applied to Business*. 2004. Xlibris, Corp. Xlibris.com.
- Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. 2002. Hachette Book Group. New York.
- Sun Tzu. *Ancient Art of War*.
- Musashi, Miyamoto. *The Book of Five Rings*. Translated by Thomas Cleary. Unabridged. 1994. Shambhala. Boston & London.
- The OODA Loop is being applied in real-world risk management settings through, for example, the Integrated Adaptive Cyber Defense (IACD) Framework for cybersecurity automation, orchestration and information sharing. This project is a collaboration between Johns Hopkins University Applied Physics Laboratory (APL) and the Financial Services Information Sharing and Analysis Center (FS-ISAC), under sponsorship of the Department of Homeland Security (DHS), in which information sharing around cyberattacks, helping to increase cyber investigation capacity and reduce investigation and response times.

## ENDNOTES

- 1 [Vendor Risk Management Benchmark Annual Survey](#). Shared Assessments and Protiviti 2018 Research Study.
- 2 Bertalanffy, Ludwig von. General Systems Theory. <https://www.panarchy.org/vonbertalanffy/systems.1968.html>
- 3 Richards, Chet. Certain to Win: The Strategy of John Boyd Applied to Business. 2004. Xlibris, Corp. Xlibris.com; Coram, Robert. Boyd: The Fighter Pilot Who Changed the Art of War. 2002. Hachette Book Group. New York.
- 4 Maley, R. Thinking Strategically: Third Party Continuous Monitoring. Shared Assessments Continuous Monitoring Group Presentation. December 2017.
- 5 [Continuous Monitoring of Third Party Vendors: Building Best Practices](#). The Santa Fe Group, Shared Assessments Program. Best Practices Awareness Group. 2017.
- 6 The feed-forward process is based on based on a mathematical model of the process and/or knowledge or measurements of changes on a system over time. Haugen, F. Basic Dynamics and Control. 2009. Tech Teach.
- 7 Lam, J. Implementing Enterprise Risk Management: From Methods to Applications. 2017. John Wiley & Sons, Inc. Hoboken, NJ.
- 8 For the purposes of discussion, within this paper the definition distinguishes continuous third party risk monitoring as an uninterrupted, real-time (or near real-time) risk management approach designed to improve an outsourcer's awareness related to their third party risks and potential control weaknesses as they emerge. This continuous monitoring approach is additive to more traditional assessment processes. It allows an organization to go beyond IT control monitoring to enhance their awareness of cybersecurity, privacy, technology, operational and strategic third party risk exposure. For additional discussion on this and related terms, see [Definition of Key Terms in the appendices](#).
- 9 Zients, J. D. ISACA. 2011. <https://www.csiac.org/journal-article/information-security-continuous-monitoring-iscm/>; Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, [Office of Management and Budget, 2012](#).
- 10 Risk Appetite: The level and type of risk an organization will take in order to pursue its strategic, measurable objectives. Risk Appetite Statement: A documented definition of the organization's risk appetite.
- 11 Zients, J. D. ISACA. 2011. <https://www.csiac.org/journal-article/information-security-continuous-monitoring-iscm/2012/>; Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, Office of Management and Budget, 2012. [www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf](http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf) 2015 reference: <https://www.isaca.org/Journal/archives/2015/Volume-1/Pages/Information-Security-Continuous-Monitoring.aspx>
- 12 For example, as of July 2018, 28 states had enacted cyber security laws and 14 more had introduced or adopted rules around cyber hygiene to improve security, address threats to critical infrastructure, and in some cases requiring agencies or organizations to implement specific types of security practices, including continuous monitoring. Further, some states, including rules that include insurance, malpractice, banking and other regulated institutions such as the New York State Department of Financial Services (NYS DFS) 500 and the California Cyber Security Law, recognize continuous monitoring as a best practice. Source: Cyber Security Legislation 2018. <http://www.ncsl.org>
- 13 Within the U.S. Office of the Controller of the Currency (OCC) "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." [Third-Party Relationship: Supplemental Examination Procedures Bulletin](#). OCC 2017-7. January 2017; [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.
- 14 Operational Risk (including IT and Infrastructure Risks, Third Party Risk Management, etc.) occurs when either a service provider or the outsourcer exposes an organization to direct or indirect losses due to inadequate or failed internal processes or systems. Adapted from: US Federal Reserve. <https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf>
- 15 Continuous monitoring is a subset of ongoing monitoring. Its application 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.
- 16 Feed-forward processes complement the feedback loop, which relies solely on cause and effect to improve system processes. The feed-forward process is based on based on a mathematical model of the process and/or knowledge or measurements of changes on a system over time. Combined, the two provide a stronger, more agile model of system improvement. Haugen, F. Basic Dynamics and Control. 2009. Tech Teach
- 17 [7th Annual IT Audit Benchmarking Survey – Business and Digital Transformation's Effects on IT Audit Groups](#). ISACA/Protiviti. 2018
- 18 A playbook can be constructed that is appropriate for an organization's unique needs to provide a pre-determined set of rules defining roles, responsibilities, options, and guidance for responding to risk management events or incidents. The playbook provides clear guidance and assigns responsibility for in-the-moment action sets the stage for ensuring that important decisions are made in a timely manner.
- 19 [Third-Party Security: Risk Management Playbook](#). RiskRecon Study. 2018.
- 20 This table is provided for informational purposes only. It 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. This table includes the strategic processes and tactical processes deemed the most generally applicable to and useful for the most parties, both outsourcers and third party providers. It 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.
- 21 [Continuous Monitoring of Third Party Vendors: Building Best Practices](#). The Santa Fe Group, Shared Assessments Program. Best Practices Awareness Group. 2017.
- 22 [Third-Party Relationships: Risk Management Guidance](#). Office of the Comptroller of the Currency (OCC). OCC Bulletin 2013-29. October 30, 2013.