Don’t Recreate the TPRM Wheel: Foster Standardization of Operations to Combat Outsourcer Assessment Fatigue (OAF)

Agenda

- What is OAF?
- What are the root causes of OAF?
- Tools & Techniques
- Vendor Trust Package
- Wrap Up

What is OAF?

What is OAF?

- *Outsourcer Assessment Fatigue (OAF) is a sense of fear, disdain, anger, and frustration imparted onto a service provider, by an existing or prospective client organization, desiring to better understand their overall risk posture for the handling of their data.*

What is OAF?

- OAF tends to be *attributed* to *third party/vendors* as they are not being prepared or willing to undergo a third party risk assessment, ***however…***
- *Outsourcers* typically employ a "one size fits all" assessment strategy that is often overkill for most vendors
- As outsourcers are challenged with monitoring and managing the risk of third-parties and downstream vendors, they are trying to *ensure they've gone deep enough* into the assessment to cover notable topics (cyber, ESG, geolocation, N'th parties, etc.) using up a third party's valuable resources
- Third parties feel they don't need to go through an outsourcer's risk assessment because they *already obtained a third party attestation* (e.g. SOC2 Type2, ISO27,000, CMM, etc.) and aggressively argue against further due diligence

What are the root causes of OAF?

Root Causes of OAF

Fatigue brought on by outsourcers to third parties due to:

- Overbearing questionnaires
- Assessors going out of scope
- Can’t agree to the standards of the due diligence (e.g., NIST, ISO. HITRUST, etc.)
- Unreasonable assessment timeframes
- Outsourcer ad hoc processes
- Constant challenges to their Vendor Trust Package (VTP)
- Demanding an onsite assessment whether it is warranted or not

Tools & Techniques

Tools & Techniques

<u>Technology/Automation</u>: *One key solution to reducing fatigue lies in automation.*

- Leveraging *existing enterprise technology* (e.g., continuous monitoring, contract management systems) to get a handle on risk (i.e., repository), trends (i.e., BU, S&P, Privacy, etc.), and existing or proposed standards and regulations (Audit, Compliance, Legal, Finance, etc.)
- Implement and *properly utilize* automation technologies to alleviate both the technical and administrative burden of conducting third-party risk
- Utilize *existing department office tools* (e.g., email mailboxes, links, etc.) assessments

Tools & Techniques

<u>Techniques</u>: *"Be fluid, because flexible is too rigid" – Common Military Axiom*

- Automate *processes* where applicable
- Establish, develop *techniques* or *contribute* to the logging of vendor profiles, contacts, and risk scores, and utilize these to enhance operational efficiency.
- Perform "*load leveling*" to gauge your staffing, budgeting, and vendor needs for the remainder of the year
- Annually assess your *procedures, practices*, and *overall program*
- Update your *policy* accordingly

Building Your “Vendor Trust Package” (VTP)

Building Your "Vendor Trust Package" (VTP)

- Sell your message to all stakeholders on the benefits of "*Perform once; share with many*" that it will dramatically cut down on their staff's time on having to constantly complete or participate in inbound assessments
- Share with them expected "*exception organizations*" and when they're expected to come assess your organization
- Establish a period to allow onsite inspection and discussion
- Remind the stakeholders this exercise stems of audit/regulation/safety and soundness and that their participation is valued and appreciated
- Be proactive! Manage the project by gathering and preparing all relevant documentation covering critical domains in your environment
- Transparency is currency; be honest and transparent with all stakeholders & partners

Building Your “Vendor Trust Package” (VTP)

Consider the following areas when establishing your organization’s VTP. Decide if the VTP should encompasses the enterprise level or a specific business offering.

- Enterprise Risk Management
- Security Policy
- Organizational Security
- Asset and Info Management
- Human Resources Security
- Physical and Environmental
- IT Operations Management
- Access Control
- Application Security
- Cybersecurity Incident Mgmt
- Operational Resilience
- Compliance and Ops Risk
- Endpoint Device Security
- Network Security
- Privacy
- Threat Management
- Server Security
- Cloud Hosting Services

Wrap Up & Q/A

- Outsourcer Assessment Fatigue (OAF) is real and is the *primary cause* as to why people hate going through third party risk assessments
- OAF is caused by both the outsourcer and the third party so it's incumbent upon both organizations to end it
- Utilize technology (automation) and establish or revise techniques to put both organizations in a "win/win/win" – BU, vendor, and your TPR program
- Establishing a vendor trust package (VTP) is also a triple "win" because it allows the second line teams to operate with minimal disruption

Cheers!

Tom Garrubba

412-720-4248

tomgarrubba@gmail.com