THIRD PARTY
RISK ASSOCIATION

July's Member Meeting

Julie Gaiaschi, CEO & Co-Founder

For your awareness, this call is being recorded

THIRD PARTY RISK ASSOCIATION

AGENDA

- Opening Remarks
- Upcoming Events
- Presentation/Roundtable: Integrating your TPRM Program into the Procurement Process
  - Relationship Building w/ Your Procurement Department
  - Enhanced Vendor Due Diligence
  - Contract Review Process
  - Risk Recognition and Follow Up
- Closing Remarks

TPRA | THIRD PARTY RISK ASSOCIATION

OPENING REMARKS

- **Censinet** is helping healthcare organizations in dealing with fraud and scams in the supply chain for personal protective equipment (PPE). They are working to identify and avoid risks to help organizations evaluate supply chain risks for these non-data-related medical supplies by are offering free and open access to our platform to any HCOs and government buyers. https://www.censinet.com/open-access/
- **Risk Recon** has developed a playbook that provides a step-by-step methodology for assessing the security configurations of any AWS deployment to help practitioners understand the 33 essential AWS security assessment criteria with an assessment-ready questionnaire. https://www.riskrecon.com/aws-assessment-toolkit?hsCtaTracking=8e44b79f-1f6b-4199-b915-9338e06bce22%7C1e62e7b7-cbb1-4d16-8af3-21351e0361b2
- **Risk Recon** is offering healthcare organizations and US & Canadian small businesses with free cybersecurity rating assessments through 12/31/2020. https://blog.riskrecon.com/free-cybersecurity-assessments

THIRD PARTY RISK ASSOCIATION

Upcoming Events

- 7/16 – Q3 Healthcare/Health Insurance Special Interest Call – 10 AM to 11 AM Central
- 7/16 – Q3 Finance/Insurance Special Interest Call – 1 PM to 2 PM Central
- 7/23 - July Focus Group Call – "TPRM 101 Guidance" – 10 AM to 11 AM Central
- 8/5 - Fall Virtual Conference – "Tightening your Belt – Doing More With Less" – 9 AM to 4:30 PM Central. Hear directly from industry leaders on how to streamline current processes, increase risk awareness, break down silos and stop duplicating work. Registration is free for members and $25 for non-members. Use member code "**2020FallVirtual**".

To register for any of our upcoming events, please visit our Practitioner Member Events page at www.tprassociation.org/practitioner-member-events.

THIRD PARTY RISK ASSOCIATION

Presentation/Roundtable: Integrating your TPRM Program into the Procurement Process

THIRD PARTY RISK ASSOCIATION

Course Description:

Integrating Your TPRM Program Into The Procurement Process

It's critical vendor security controls are reviewed prior to a contract being signed to not only ensure the vendor has a sufficient security program in place, but also to ensure continuous monitoring requirements are incorporated into the contract. Once a contract is signed, an organization may lose the leverage required to effectively assess vendor security controls. A strong partnership with your organization's Procurement department can assist with your program objectives.

In this session, we will discuss:

1. Relationship building with your Procurement department;
2. Enhanced vendor due diligence;
3. Contract review process;
4. Risk recognition and accelerated follow-up.

TPRA | THIRD PARTY RISK ASSOCIATION

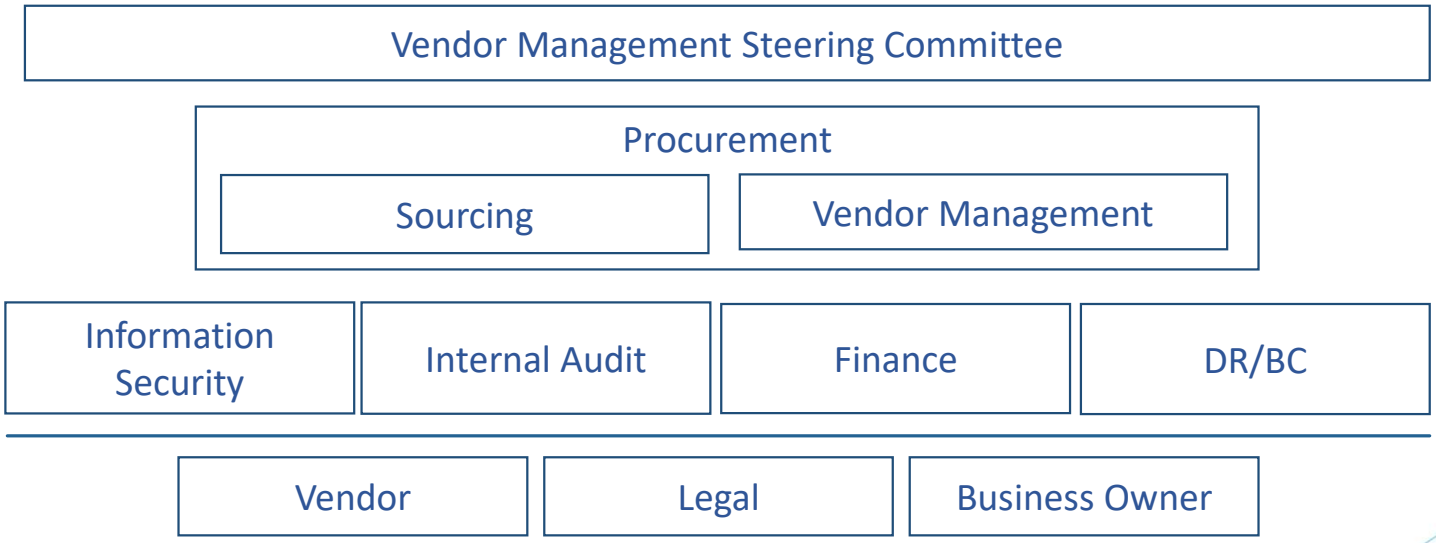
Relationship Building with your Procurement Department:

- Determine if the process will be centralized or de-centralized.
- Understand the processes that currently exists w/in Procurement. Identify review and approval touchpoints.
- Document and implement processes and workflows, checking in regularly to work through issues. Ensure your process includes alerts for triggered hand-offs.
- Request system access (if necessary).
- Ensure incorporated into the contract review process to review & approve language redlines.
- Establish a checklist for contract signature and moving to the implementation phase.
- Develop and execute an escalation process. Escalate when necessary and to the right stakeholders (Oversight Committee).
- Set expectations with stakeholders and vendors.

THIRD PARTY RISK ASSOCIATION

Ex. 1: Workflow for Vendor Due Diligence:

Governance Structure

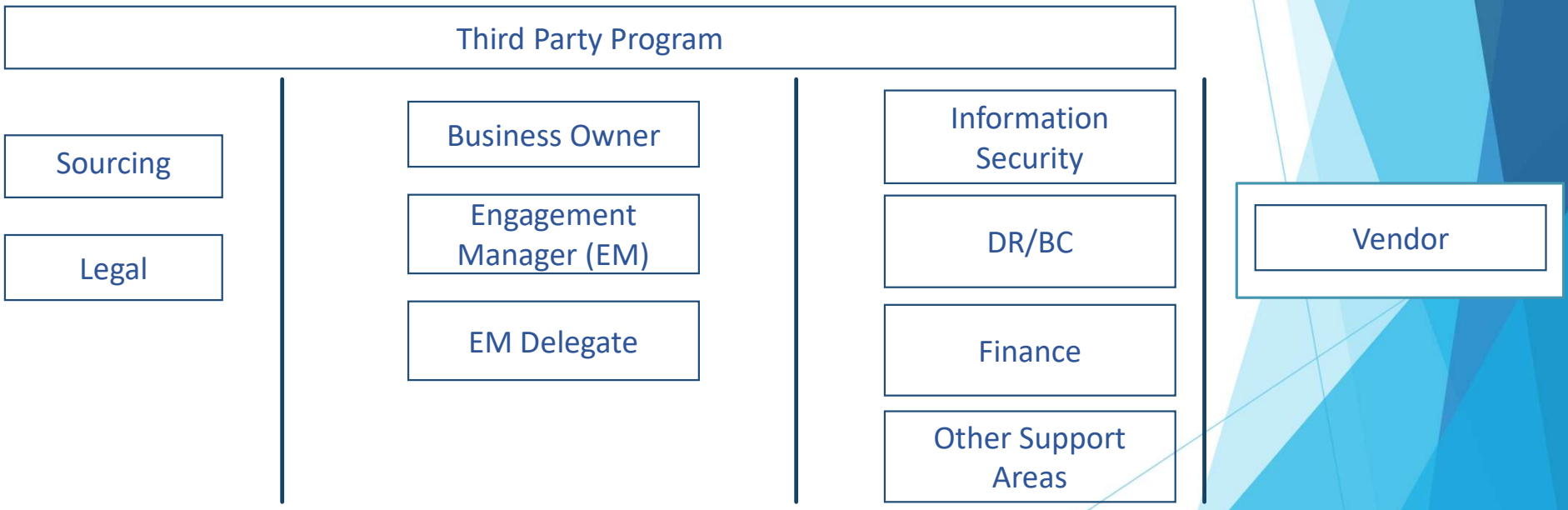


THIRD PARTY RISK ASSOCIATION

Ex. 2: Workflow for Vendor Due Diligence:

GRC Tool

Governance Structure



THIRD PARTY RISK ASSOCIATION

Enhanced Vendor Due Diligence:

- Inherent Risk Questionnaire – Weights based on organizational risk appetite
- Questionnaires
  - Information Security
  - Financial
  - Operational
  - Compliance
  - Continuity
- Assessments
  - Security – Patching & Penetration Testing
  - Country Assessment
  - Background Check
  - Viability Assessment
- Security Rating
- Onsite Visit

TPRA | THIRD PARTY RISK ASSOCIATION

Contract Review Process:

- Template Agreements (Master, Business Associate, SOW, NDA)
- Risk-Triggered Addendums (Minimum Information Security Addendum, Offshore Addendum)
- Implement a process for subject matter expert (SME) redlining and negotiating with the vendor
- Final version is routed through tool, which is approved by SME (if redlines were required).
- Contract signing should only occur after due diligence is completed.
- Regularly meet with Legal/Procurement to review frequent redline issues and ensure clauses are current and address risk.

Contract Clause Must Haves:

- Right to Audit or an Onsite Visit
- Respond to surveys/questionnaires and provide sufficient evidence
- Non-compliance Triggers & Breach Notification
- Insurance
- Critical Controls & Service Level Agreements (SLAs)
- Offshore Personnel and Sub-contractors
- Destruction of Data

TPRA | THIRD PARTY RISK ASSOCIATION

Risk Recognition & Accelerated Follow-up:

- Set expectations with business owners and vendors. Set up regular meetings where expectations, deliverables, and over-due items are discussed.
- Ensure vendors know the escalation process and the visibility it provides.
- Request an escalation process on the vendor's side (include legal, compliance, and CEO if necessary).
- Review risks discovered with the vendor to ensure information is accurately captured and agreement is reached.
- Provide high level expectations for risk remediation and request the vendor provide a more concrete plan with target dates.
- Set up a cadence for obtaining updates (make sure it's based on risk).
- Consider sharing the vendor's overall risk score with the vendor and discuss how the risk score can be reduced.
- Ensure risks are captured in a central repository with automated follow-up triggers. Capture all notes on progress within the central repository.

THIRD PARTY RISK ASSOCIATION

In Summary:

- Understand the processes that currently exist w/in Procurement and work to insert assessment steps where it already makes sense.
- Communicate, be transparent, and allow departments to review process documentation so as to reach agreement on process enhancements.
- Develop and execute an escalation process. Escalate when necessary and to the right stakeholders.
- For higher risk vendors, ensure your due diligence process is more than just checking a box.
- Ensure alerted for contracts that require SME redline reviews and approvals.
- Set expectations with your business and vendors regarding deliverables, review activities, and escalation processes.
- Set up regular meetings with vendors to ensure they provide you with necessary evidence for your reviews and agree to and address risks that are discovered.

Vendors are an extension of your own security programs. Thus, treat them as partners and not adversaries.

THIRD PARTY RISK ASSOCIATION

Next Meeting: Thursday, August 13th from 10 to 11 AM Central