TPRA

THIRD PARTY RISK ASSOCIATION

April’s Member Meeting

Julie Gaiaschi, CEO & Co-Founder

For your awareness, this call is being recorded

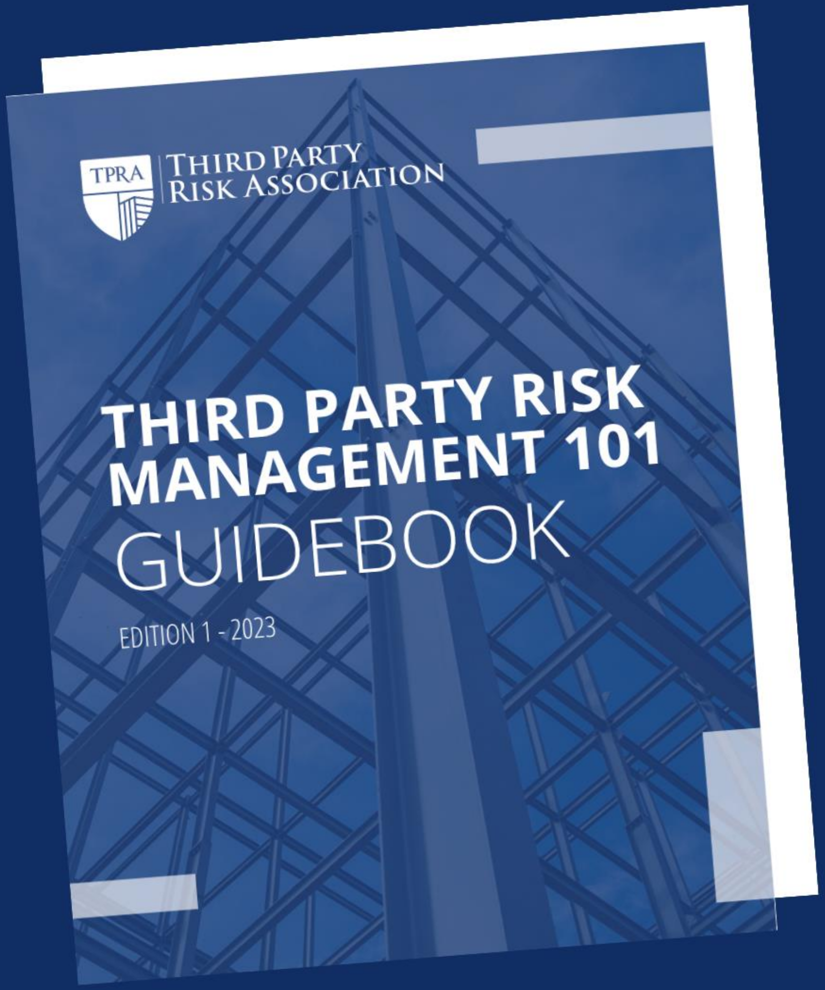
AGENDA

- Opening Remarks
- Roundtable: Executive & Business Owner Buy-In
  - Why is it important?
  - Setting Expectations
  - Roles & Responsibilities
  - Reporting & Metrics
  - TPRM Champions
  - Additional Items to Consider
- Closing Remarks
- TPRM “Tool Talk” Demo provided by Venminder

TPRA THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **4/9 - 4/12 Third Party Risk Madness In-Person Conference!**
- **4/16 New & Potential Member Meeting** @ 10 – 10:30 AM Central
- **4/16 Volunteer Interest Call** @ 10:30 – 11 AM Central
- **4/17 Retail/Manufacturing Special Interest Call** @ 1 – 2 PM Central
- **4/18 Focus Group Call** @ 10 – 11 AM Central
- **4/18 Retail/Manufacturing Special Interest Call** @ 1 – 2 PM Central
- **YouTube** Channel – Subscribe to Third Party Risk Association
- **Slack Space Forum** – Join under “Member Services” using the “Slack Forum” link.
- Join our **Meta, LinkedIn & Instagram pages** to view upcoming events and promotional opportunities.



TPRA THIRD PARTY RISK ASSOCIATION

THIRD PARTY RISK MANAGEMENT 101

GUIDEBOOK

EDITION 1 - 2023

TPRA THIRD PARTY RISK ASSOCIATION

THIRD PARTY RISK MANAGEMENT 101 GUIDEBOOK

Currently available for FREE to TPRA Members!

HTTPS://WWW.TPRASSOCIATION.ORG/GUIDEBOOK

THIRD PARTY RISK ASSOCIATION

Third Party Cyber Risk Assessor© (TPCRA©) Certification

The TPCRA Certification is a specialized designation to confirm your understanding and s in the assessment of third party cyber security controls and processes, as well as validate your competency in the creation, execution, and management of third party cyber risk assessments.

Examination: Scheduled at a **PearsonVue** location near you on the date and time you select.

Domains:

- Cybersecurity and TPRM Basics
- Pre-Contract Due Diligence
- Continuous Monitoring
- Physical Validation
- Disengagement
- Cloud Due Diligence
- Reporting and Analytics

2024 Training Dates:

- ~~Virtual: **February 26 - 29** @ 5 PM – 8 PM CT daily~~
- Virtual: **May 20 – 21** @ 8 AM – 3 PM CT daily
- Virtual: **August 26 – 29** @ 5 PM – 8 PM CT daily
- Virtual: **November 6 – 7** @ 8 AM – 3 PM CT daily
- **On-Demand Training** Launching in Q1 2024

Tomorrow is the LAST DAY to Register!!

[redacted]

TPRA ANNUAL IN-PERSON TPRM CONFERENCE

THIRD PARTY RISK MADNESS

APRIL 9 - 12, 2024 | SHERATON PHOENIX DOWNTOWN | PHOENIX, AZ

TPRA THIRD PARTY RISK ASSOCIATION

Day 1 - Tuesday, April 9th

Network Event @ 6 – 8 PM MST

Day 2 - Wednesday, April 10th

7:30 – 9 AM – Registration & Breakfast

9 – 10 AM – **Keynote:** Jeff Hornacek

10 – 10:50 AM – **Break Out** (4 Tracks)

11 – 11:50 AM – **Break Out** (4 Tracks)

11:50 AM – 1 PM - LUNCH

1 – 1:50 PM – **Roundtables** (4 Tracks)

2 – 2:50 PM – **Break Out** (4 Tracks)

3:10 – 4 PM – **Break Out** (4 Tracks)

4:10 – 5 PM – **Break Out** (4 Tracks)

5:30 – 7:30 PM – **Network Event**

Day 3 - Thursday, April 11th

7:30 – 9 AM – Registration & Breakfast

9 – 10 AM – **Keynote:** Edna Conway

10 – 10:50 AM – **Break Out** (4 Tracks)

11 – 11:50 AM – **Break Out** (4 Tracks)

11:50 AM – 1 PM – LUNCH & Raffles

1 – 1:50 PM – **Roundtables** (4 Tracks)

2 – 2:50 PM – **Break Out** (4 Tracks)

3:10 – 4 PM – **Break Out** (4 Tracks)

4:10 – 5 PM – **Break Out** (4 Tracks)

Day 4 - Friday, April 12th

7:30 – 9 AM – Registration & Breakfast

9 – 10 AM – **Keynote:** OCC, FDIC, FRB

10 – 10:50 AM – **Roundtables** (4 Tracks)

11 – 11:50 AM – **TPRA FUN! (Prizes)**

11:50 AM – 12 PM - Closing

TPRA THIRD PARTY RISK ASSOCIATION

Roundtable: Executive & Business Owner Buy-In

Why is Executive & Business Owner Buy-in Important?

- **Risk Awareness** at the Enterprise Level as leadership and the business often have a broader understanding of the organization's strategic goals.
- **Priority Setting** for TPRM to set a clear message throughout the org and align efforts across departments.
- **Resource Allocation** to implement and sustain TPRM.
- **Accountability** for implementing & maintaining the TPRM program.
- **Stakeholder Confidence** when leadership demonstrates their commitment to risk management.
- **Decision Making** to ensure risk considerations are integrated into the decisions made my leadership and to set risk tolerances.

Setting Expectations

- Communicate the importance of a TPRM program. (Can accomplish through a comprehensive Business Case.) Explain the risk third parties pose to the org.
- Outline the objectives of the program. Explain what the org will achieve (ROI) by implementing the program (reducing risk exposure, enhancing regulatory compliance, protecting sensitive data, and safeguarding reputation.
- Establish clear expectations for decision-making related to third party relationships. Outline the criteria for selecting, assessing, and approving third parties. Clarify how leadership will be involved and what authority they have.
- Note the risk of not having a TPRM program in place. Highlight the potential costs of inaction or inadequate investment in third-party risk management. Discuss the financial implications of third-party failures, such as financial losses, legal fees, regulatory fines, and remediation costs.
- Define the third parties that would be considered in vs. out of scope to set parameters around the size and scope of the program.
- Layout the maturity of the program within the first vs. fifth year.

Roles & Responsibilities

Clearly define the roles and responsibilities (R&R) of leadership in the third party risk management program. Explain what is expected of them in terms of support, oversight, decision-making, and resource allocation. Make it clear that leadership involvement is crucial for the success of the program.

Executive R&R

- Champions the program and acts as an advocate for program initiatives to ensure all lines of business are on board.
- Provides additional oversight through the risk escalation and acceptance process and/or by sitting on the risk committee.
- Provides governance for your overall TPRM program and ensures the program meets regulatory requirements and adequately manages risks at the highest level and in a manner consistent with the organization's strategic goals and risk appetite.
- Advises on and/or approves risk mitigation strategies, escalations, and risks requiring acceptance.

Roles & Responsibilities

Business Owner R&R

- Owns the third party relationship, as well as the risk related to said third party.
- Oversees the negotiation and management of contracts with the third party. This involves defining the scope of work, specifying service level agreements (SLAs), and ensuring compliance with contractual obligations.
- Reviews and acts on the results of third party reviews.
- Assists with escalations and approves risk acceptances (up to a certain level).
- Monitors the performance of the third party to ensure that they meet agreed-upon standards and deliverables. This involves tracking key performance indicators (KPIs) and addressing any performance issues.
- Works to resolve any issues or disputes that may arise during the course of the relationship. This may involve collaborating with the third party to find solutions, escalating issues as needed, and ensuring timely resolution.

Reporting & Metrics

- **Provide Regular Updates:** Commit to providing regular updates to leadership on the progress of the third-party risk management program. Keep them informed about key milestones, risk assessments, and any issues or challenges that arise. Make sure they are aware of the organization's overall risk posture and any emerging risks from third-party relationships.
- **Seek Input and Feedback:** Encourage leadership to provide input and feedback on the third-party risk management program. Solicit their ideas for improvement, address any concerns or objections they may have, and incorporate their feedback into the program's development. This helps foster a sense of ownership and engagement among leadership.
- **Demonstrate ROI:** Finally, demonstrate the return on investment (ROI) of the third-party risk management program to leadership. Show how the program contributes to the organization's strategic objectives, protects its assets, and mitigates potential losses. Use metrics and data to quantify the impact of the program wherever possible.

TPRM Champions – Why they are important.

- **Advocacy and Support:** Business champions advocate for the importance of third-party risk management within their respective departments or business units. They help garner support from key stakeholders and ensure that the program receives the attention and resources it needs to succeed.
- **Cross-functional Collaboration:** Third-party risk management programs require collaboration across various departments and functions within an organization. Business champions facilitate this collaboration by serving as liaisons between their department and the risk management team, helping to bridge communication gaps and align priorities.
- **Change Management:** Implementing a third-party risk management program often requires changes to existing processes, procedures, and systems within an organization. Business champions help facilitate change management efforts by promoting awareness, training employees, and addressing concerns or resistance to change.
- **Culture of Risk Awareness:** Business champions help foster a culture of risk awareness within their department or business unit.

TPRM Champions – How to find and engage them.

- **Identify Stakeholders:** The first step is to identify stakeholders who have a vested interest in third party relationships and risk management. This includes executives, business owners, department heads, compliance officers, procurement officers, legal counsel, and IT/security personnel. Make sure they are the decision makers that also have influence.
- **Educate and Raise Awareness:** Once stakeholders are identified, the next step is to educate them about the importance of third-party risk management and raise awareness about the potential risks associated with third-party relationships.
- **Demonstrate Value:** Show stakeholders the value that a robust third-party risk management program can bring to the organization. Highlight success stories, case studies, or examples from other organizations to illustrate the tangible benefits of effective risk management.
- **Align Objectives:** Align objectives between the TPRM program and their business objectives to encourage stakeholders to actively participate in and support the program.
- **Foster Collaboration:** Encourage collaboration and cross-functional teamwork among stakeholders involved. Facilitate regular communication and collaboration forums to foster a sense of community and shared ownership of the program.

Additional Items Executives & Business Owners Should Consider

- **Regulatory Compliance:** Discuss the importance of regulatory compliance in third-party risk management. Highlight relevant regulations and industry standards that govern third-party relationships, such as GDPR, HIPAA, SOX, or PCI DSS. Explain how compliance with these regulations is critical for protecting the organization from legal and financial consequences.
- **Reputation Management:** Explore the link between third party risk management and reputation management. Discuss how negative incidents involving third parties can damage the organization's reputation and erode stakeholder trust. Emphasize the role of executive buy-in in safeguarding the organization's reputation through effective risk management practices.
- **Emerging Risks:** Address the importance of anticipating and managing emerging risks in third party relationships. Discuss emerging trends and challenges in the landscape of third party risk, such as cybersecurity threats, supply chain disruptions, geopolitical risks, and environmental sustainability concerns. Explain how executive buy-in is essential for proactively addressing these risks.

Additional Items Executives & Business Owners Should Consider

- **Integration with Enterprise Risk Management (ERM):** Explain how third party risk management fits into the broader framework of enterprise risk management (ERM). Discuss the interdependencies between third-party risks and other types of risks faced by the organization, such as operational, financial, strategic, and compliance risks. Highlight the need for alignment and coordination between the TPRM program and ERM efforts.
- **Continuous Improvement:** Emphasize the importance of continuous improvement in the third party risk management program. Discuss strategies for ongoing evaluation, enhancement, and optimization of the program, such as conducting regular risk assessments, updating policies and procedures, and leveraging lessons learned from incidents or near misses. Stress the role of executive leadership in driving a culture of continuous improvement.

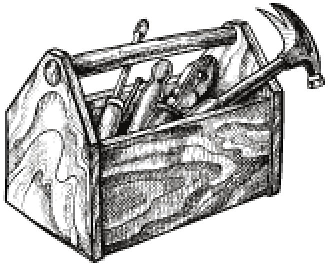
Questions?

THIRD PARTY RISK ASSOCIATION

Next Meeting: Thursday, May 9th @ 10 – 11 AM Central

Panel: **“Nth Party Reviews”** (Identification, Assessment Techniques, Contract Requirements, Findings, & Follow-up)

No TPRM “Tool Talk”



TOOL TALK

WITH

venminder