THIRD PARTY
RISK ASSOCIATION

November's Member Meeting

Julie Gaiaschi, CEO & Co-Founder

For your awareness, this call is being recorded

TPRA | THIRD PARTY RISK ASSOCIATION

AGENDA

- Opening Remarks
- Elected Board of Directors
- Roundtable: “Contract Risk & Insurance Requirements”
  - Why are Contracts Important?
  - Contract Risk
  - Addressing Contract Risk
  - What is Insurance?
  - Evaluation of Insurance Coverage
  - Insurance Types & Limits
- Closing Remarks
- TPRM “Tool Talk” Demo w/ Breach Siren – Presented by Jay Bobo, Founder of Breach Siren

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **11/9 November Practitioner Call @** 10 – 11:30 AM Central – Contract Risk & Insurance Requirements + Breach Siren demo.
- **11/14 Retail/Manufacturing Special Interest Call** @ 10 AM
- **11/14 Technology Special Interest Call** @ 1 PM
- **11/16 Focus Group** @ 10 AM Central – Financial Assessment Questionnaire
- **11/16 Finance & Insurance Special Interest Call** @ 1 PM
- **11/21 Healthcare/Health Insurance Special Interest Call** @ 10 AM
- **11/21 Women in TPRM Call** @ 1 – 2 PM Central
- **12/1 Quarterly Virtual Network Event** @ 1 PM

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **YouTube** Channel – Subscribe to Third Party Risk Association
- **Slack Space Forum** – Join under "Member Services" using the "Slack Forum" link.
- Join our **Facebook, LinkedIn & Instagram pages** to view upcoming events and promotional opportunities.
- **Thank you** to those of you that took our **Practitioner Year-End Survey**! Your responses are assisting with our 2024 plans. For completing the survey and entering your email, you were entered into a raffle for a **$100 Amazon gift card**. **And the winner is… Michelle A.**

TPRA | 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.

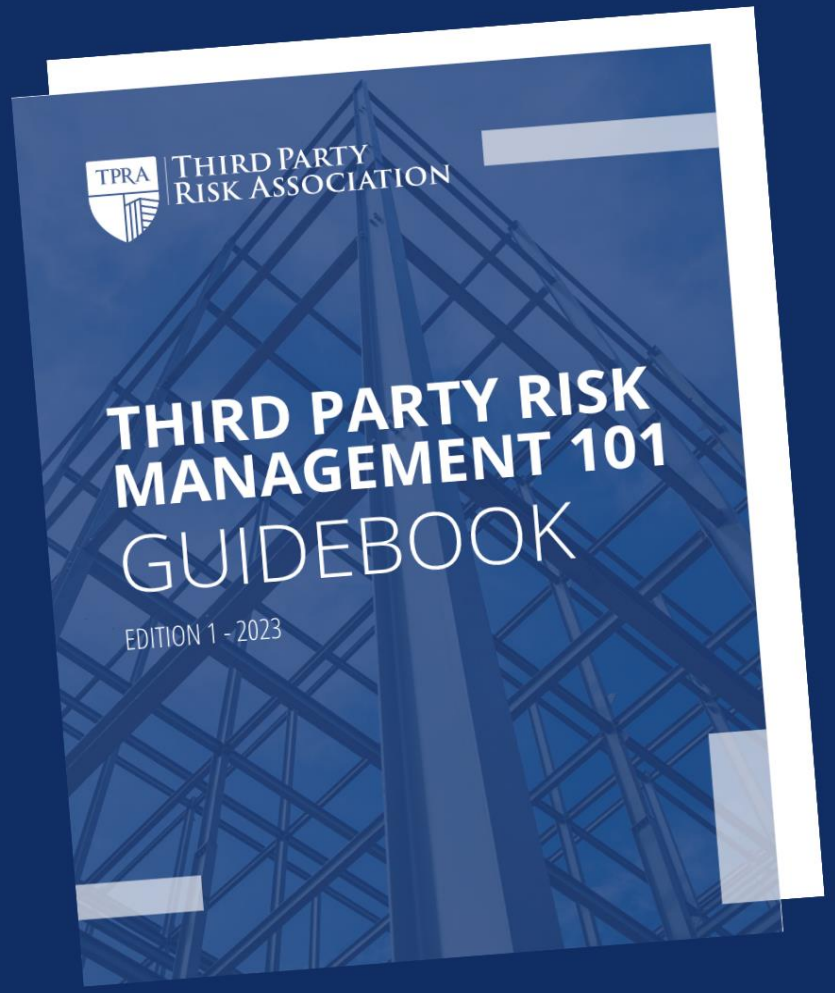
Examination: Scheduled at a **PearsonVue** location near you on the date and time you select.

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



TPRA | THIRD PARTY RISK ASSOCIATION

THIRD PARTY RISK MANAGEMENT 101 GUIDEBOOK

Currently available for FREE to TPRA Members!

HTTPS://WWW.TPRASSOCIATION.ORG/GUIDEBOOK


Early-Bird Registration, Call for Speakers, and Call for Sponsors now OPEN!
TPRA ANNUAL IN-PERSON TPRM CONFERENCE
THIRD PARTY RISK MADNESS
APRIL 9 - 12, 2024 | SHERATON PHOENIX DOWNTOWN | PHOENIX, AZ

Congratulations!

And your new 2024-2026 Board of Directors are…

- **Dustin Sachs –** Senior Manager for World Kinect Corporation
- **Morgan Binder -** Third Party Risk for Stripe
- **Paul Kurtz -** Director, Third-Party Risk Management for Merchante

They will join current Board members Vincent Scales (Chairman) and Kim LaBarbiera on 1/1/24.

TPRA | THIRD PARTY RISK ASSOCIATION

Roundtable: Contract Risk & Insurance Requirements

TPRA | THIRD PARTY RISK ASSOCIATION

Why Are Contracts Important?

- Documents relationship expectations that can be held up in a court of law.
- Allows TPRM practitioners to complete their assessments sufficiently.
- Ensures due diligence findings can be addressed within contractual clauses.
- Includes remedies in the event a third party fails to meet its obligations under the agreement.
- Reflective of your organization's risk tolerance.
- Allows for a smooth transition away from a third party.

TPRA | THIRD PARTY RISK ASSOCIATION

What Is Contract Risk?

- The risk of not including sufficient clauses within your agreement that can lead to gaps in your review process, as well as put the organization at risk should a potential impact be realized.
- The risk of not including control expectations within the agreement or a separate addendum that will ensure your data is appropriately safeguarded and your organization's strategic objectives are not impacted.
- The risk of not sufficiently reviewing contract terms and comparing them to a third party's control environment to ensure they are doing what they said they would do.
- The risk of not including safeguards within the contract should a third party risk be realized (such as incident response, breach notification, or non-compliance triggers).

TPRA | THIRD PARTY RISK ASSOCIATION

How Can We Address Contract Risk?

- By working closely with Legal and Procurement teams to ensure contracts align closely with your organization's risk management strategy.
- Templates for cybersecurity requirements should be drafted to ensure they provide sufficient coverage of key controls, define expectations for participating in compliance monitoring activities (i.e., due diligence assessments), as well as providing evidence items upon request.
- Templates should also detail appropriate remedies (non-compliance triggers) if/when the third party fails to meet its obligations under the agreement.
- Practitioners should also have a seat at the table when reviewing redlines within specific clauses that relate to cybersecurity terms, as well as terms that would allow a practitioner to perform his/her duties (such as a "Right to Audit or Review" and/or "Termination" clause).
- Practitioners can also ensure any high-risk findings noted during the due diligence process are noted within contractual terms. TPRM practitioners should work closely with legal counsel to ensure that the contractual language is clear, specific, and enforceable.

TPRA | THIRD PARTY RISK ASSOCIATION

How Can We Address Contract Risk?

- It is important to perform due diligence activities before a contract is signed.
- Contracts should be reviewed on a regular cadence to confirm they remain in line with your organization's risk appetite, as well as reflect any emerging risks that have been identified.
- If changes need to be made to bring contracts in line with current standards, then an amendment should be considered.
- It's important to review agreements carefully and identify which parts may be NEGOTIABLE and which parts are NON-NEGOTIABLE. This can help to streamline the negotiation process and avoid unnecessary delays or disputes.
- Contract negotiation techniques depend on the risks the third party presents to your organization, as well as the products/services they provide.

TPRA | THIRD PARTY RISK ASSOCIATION

Insurance - The primary purpose of insurance is to mitigate the financial impact of unforeseen events or risks, providing individuals and businesses with a sense of security and stability. It is a transfer of risk for when the likelihood of a risk occurring is low, but the impact is high. Ensure that your organization's insurance requirements are specified in the contract.

Evaluate the insurance coverage and policies held by third parties to ensure they have adequate coverage to mitigate potential risks and liabilities. The assessment aims to verify that the third party's insurance aligns with your organization's requirements and adequately protects both parties in case of unforeseen events.

TPRA | THIRD PARTY RISK ASSOCIATION

What To Evaluate

- **Coverage Types** - Evaluate the types of insurance coverage the third party holds, such as general liability insurance, professional liability insurance, cyber liability insurance, product liability insurance, workers' compensation insurance, and more.
- **Certificate of Insurance (COI)** - Obtain and review the third party's Certificate of Insurance to verify the details of their coverage, including policy numbers, effective dates, coverage types, and limits.
- **Coverage Limits** - Assess the coverage limits of the insurance policies to ensure they are sufficient to cover potential losses or liabilities that could arise from the third party's actions.
- **Scope of Coverage** - Review the policy language to understand the scope of coverage, exclusions, and limitations of the insurance policies.
- **Effective Dates** - Determine the renewal and cancellation terms of the third party's insurance policies to ensure continuous coverage during the contract period.

TPRA | THIRD PARTY RISK ASSOCIATION

What To Evaluate - Continued -

- **Additional Insured** - Determine if your organization is named as an additional insured on the third party's insurance policies. This provides your organization with coverage under their policies for specified liabilities.
- **Subcontractor Coverage** - Assess whether the third party's insurance extends to cover subcontractors or vendors that they may engage for services related to your business relationship.
- **Coverage Gaps** - Identify any gaps in coverage that could leave either party exposed to risks that are not adequately addressed by the third party's insurance.
- **Deductibles and Self-Insured Retentions** - Review the deductibles or self-insured retentions associated with the insurance policies and assess whether they are reasonable.
- **Claims History** - Inquire about the third party's claims history and any significant claims or incidents that may have occurred in the past.
- **Notification & Reporting** - Understand the third party's procedures for notifying the insurance carrier and relevant parties in the event of a claim.

TPRA | THIRD PARTY RISK ASSOCIATION

Insurance Types & Limits

Disclaimer: The appropriate coverage limits for different types of insurance policies can vary widely depending on factors such as the nature of the business, industry, size of the organization, risk exposure, contractual requirements, and local regulations. It's important to work with your insurance professionals and risk management experts to determine the optimal coverage limits for your specific situation. The below does not represent insurance advice.

That being said, here are some general guidelines for common types of insurance policies…

- **General Liability Insurance:**
  - Coverage Purpose: Protects against claims of bodily injury, property damage, and personal injury due to your business operations.
  - Recommended Coverage Limit: $1 million to $2 million per occurrence, with an aggregate limit (total limit for the policy period) of $2 million to $4 million.
- **Professional Liability (Errors & Omissions):**
  - Coverage Purpose: Protects against claims of bodily injury, property damage, and personal injury due to your business operations.
  - Recommended Coverage Limit: $1 million to $2 million per occurrence, with an aggregate limit (total limit for the policy period) of $2 million to $4 million.
- **Cyber Liability:**
  - Coverage Purpose: Protects against data breaches, cyberattacks, and related liabilities.
  - Recommended Coverage Limit: Varies depending on the size and nature of the organization, but coverage limits of $1 million to $10 million or more may be appropriate.

- **Umbrella or Excess Liability Insurance:**
  - Coverage Purpose: Provides additional coverage beyond the limits of your primary liability policies.
  - Recommended Coverage Limit: Should provide enough additional coverage to handle catastrophic events. It's often recommended to have a limit that matches your total assets or potential liabilities.
- **Workers Compensation:**
  - Coverage Purpose: Provides medical and wage replacement benefits to employees injured on the job.
  - Coverage Limit: Determined by legal requirements in your jurisdiction. It typically provides benefits according to state laws.
- **Business Interruption:**
  - Coverage Purpose: Provides coverage for lost income and operating expenses if your business is unable to operate due to a covered event.
  - Recommended Coverage Limit: Should cover your anticipated revenue and necessary ongoing expenses during the interruption period.

- **Product Liability Insurance:**
  - Coverage Purpose: Protects against claims arising from defective products causing bodily injury or property damage.
  - Recommended Coverage Limit: Depends on the type of products, industry, and size of the organization. Limits could range from $1 million to several million dollars.
- **Commercial Property Insurance:**
  - Coverage Purpose: Protects against damage or loss of physical assets, such as buildings, equipment, inventory, and furnishings.
  - Recommended Coverage Limit: The limit should be sufficient to cover the replacement or repair costs of your assets. Consider the value of your property and potential rebuilding costs.
- **Employment Practices Liability Insurance (EPLI):**
  - Coverage Purpose: Protects against claims related to employment-related practices, such as discrimination, harassment, wrongful termination, etc.
  - Recommended Coverage Limit: Varies based on the size of the organization and potential risks, but coverage limits of $1 million to $5 million are common.

- **Directors and Officers (D&O) Insurance:**
  - Coverage Purpose: Protects the personal assets of directors and officers from claims related to their management decisions.
  - Recommended Coverage Limit: Varies based on the size of the organization, industry, and exposure, but limits of $1 million to $5 million are typical.

These are general recommendations, and specific coverage limits should be determined after a thorough assessment of your organization's risk exposure and financial situation. Consulting with insurance professionals, brokers, and risk management experts can help you determine the most appropriate coverage limits for your business needs.

THIRD PARTY RISK ASSOCIATION

Questions?

Next Meeting: Thursday, December 14th @ 10 to 11:00 AM CST

Topic – TPRA Year-in-Review & Look Ahead + FUN!

TPRA | THIRD PARTY RISK ASSOCIATION

TOOL TALK

WITH

breachsiren