THIRD PARTY
RISK ASSOCIATION

March's Member Meeting

Julie Gaiaschi, CEO & Co-Founder

For your awareness, this call is being recorded

TPRA | THIRD PARTY RISK ASSOCIATION

AGENDA

- Opening Remarks
- Presentation/Roundtable: “Assessing Inherent & Residual Risk”
  - Inherent Risk
  - Residual Risk
- No TPRM “Tool Talk” Today
- Closing Remarks

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **3/16 – Focus Group Call** @ 10 to 11 AM Central
- **3/21 - Quarterly Retail & Manufacturing Special Interest Call** @ 10 to 11 AM
- **3/21 – Women in TPRM Call** @ 1 to 2 PM Central
- **3/27 – 3/30 – TPCRA Virtual Training** @ 5 to 8 PM Central each night
- **YouTube** Channel – Subscribe to Third Party Risk Association
- **Slack Space Forum** – Join under "Member Services" using the "Slack Forum" link.
- Join our **LinkedIn Page** to view upcoming events and promotional opportunities.
- Follow our **Instagram Page** for Monday memes, behind the scene look at conference planning, and event updates.

THIRD PARTY RISK ROUNDUP

April 24 - 26, 2023

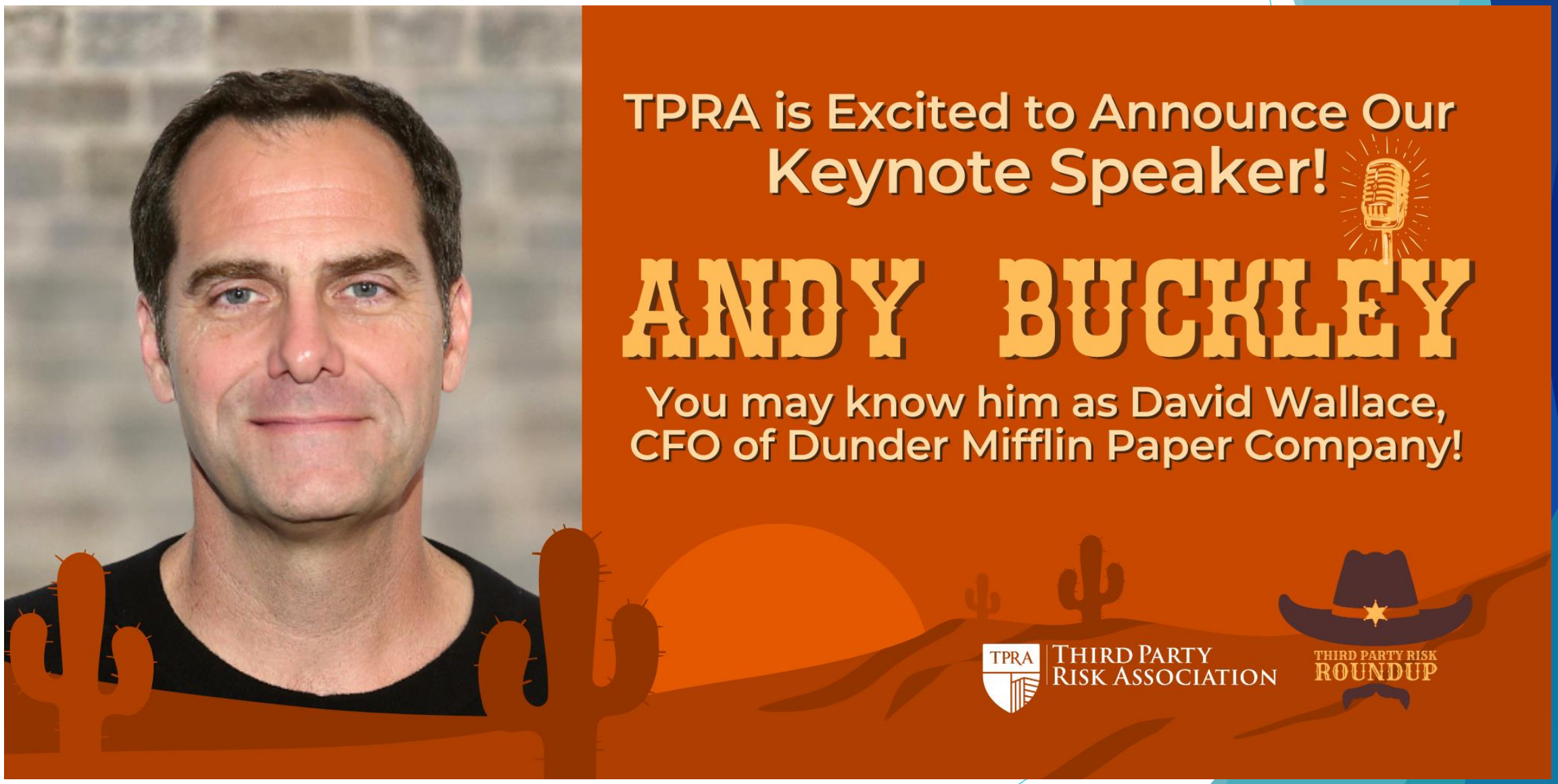
Nashville Marriott at Vanderbilt University

2555 West End Ave

Nashville, Tennessee

Friendly Reminders:
Early Bird Pricing ends March 24th.
Discount Hotel Room Rate ends March 24th.

TPRA | THIRD PARTY RISK ASSOCIATION



TPRA | THIRD PARTY RISK ASSOCIATION

TPRA is Excited to Announce Our Keynote Speaker!

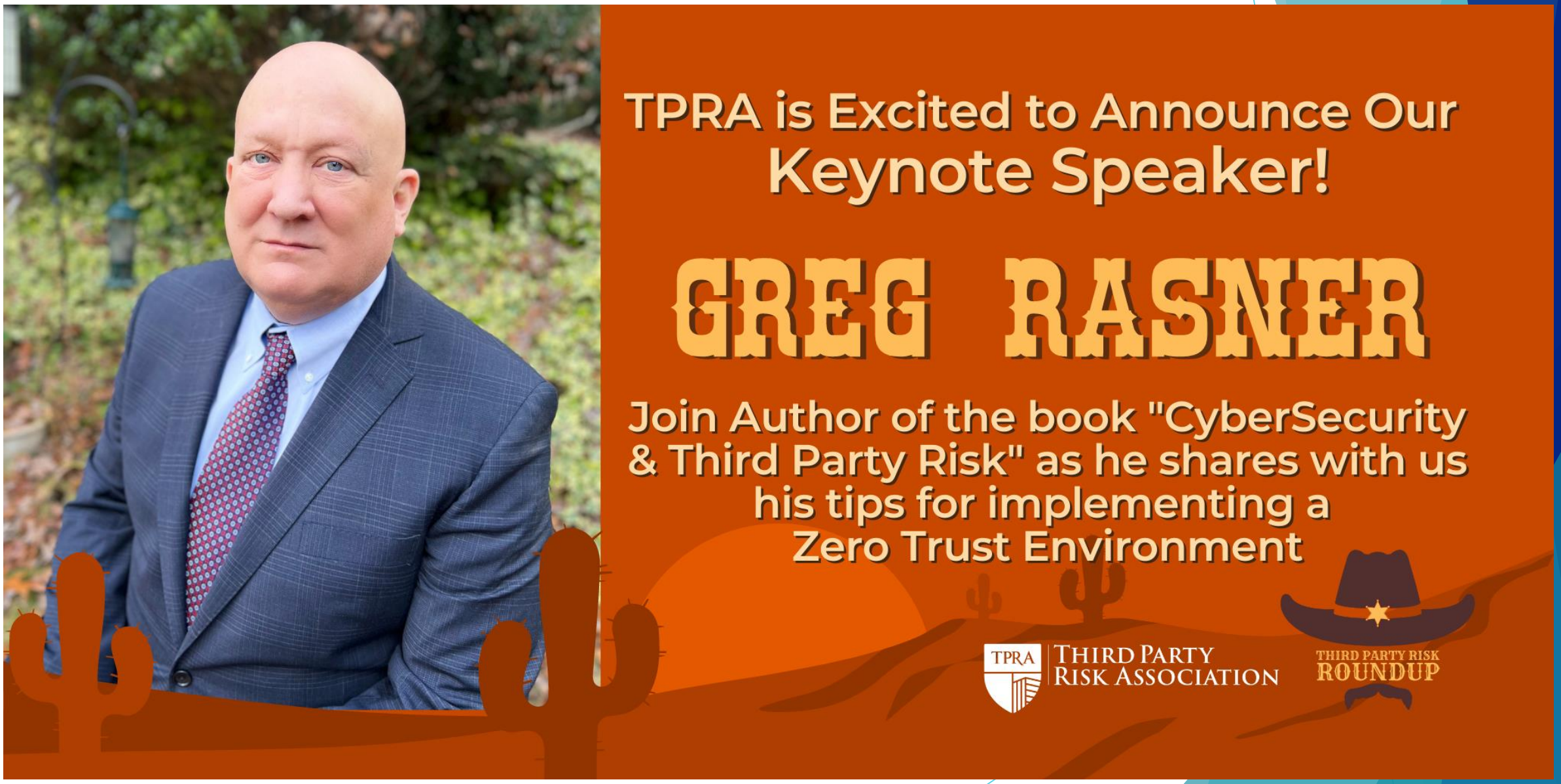
BIG 4 PANEL

Join Directors from each of the Big 4 organizations (EY, Deloitte, KPMG, PwC) as they discuss TPRM Better Practices

TPRA | THIRD PARTY RISK ASSOCIATION

THIRD PARTY RISK ROUNDUP

TPRA | THIRD PARTY RISK ASSOCIATION



TPRA | THIRD PARTY RISK ASSOCIATION

CERTIFICATION PROGRAM NOW OPEN

Submit your application today!

REGISTER

Check Our Website

WWW.TPRASSOCIATION.ORG/TPRA-CERTIFICATIONS

TPRA | THIRD PARTY RISK ASSOCIATION

Third Party Cyber Risk Assessor© (TPCRA©) Certification

The TPCRA Certification is a specialized qualification designation to confirm your understanding and skill 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. (Exam emails will begin to go out **March 20, 2023**.)

Domains:

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

Training Dates:

- Virtual: **March 6 - 7** @ 9 AM - 4 PM CT each day
- Virtual: **March 27 - 30** @ 5 - 8 PM CT each night
- In-Person @ Nashville, TN: **April 24** @ 3 - 6 PM CT, **April 25** @ 9 AM - 4 PM CT, and **April 26** @ 9 AM - 12 PM CT (at in-person conference)
- Virtual: **May 15 – 18** @ 8 AM - 11 AM CT each day
- Virtual: **June 12 – 15** @ 5 PM - 8 PM CT each night
- Virtual: **July 18 – 19** @ 8 AM - 3 PM CT each day

TPRA | THIRD PARTY RISK ASSOCIATION

Assessing Inherent & Residual Risk

TPRA | THIRD PARTY RISK ASSOCIATION

What Is Risk?

- **Risk** is the possibility of an adverse impact on an organization's data, financials, operations, reputation, or other business objectives, as a direct or indirect result of an organization's third party.

Risk = Potential Impact x Likelihood Will Occur

- Risk ratings should be calculated based on your organization's risk appetite (the risk your organization is or is not willing to accept). Does your organization already have an established risk rating methodology? Do you have an Enterprise Risk Management team and/or an Internal Audit team?
- Developing a risk matrix can be helpful in ensuring a consistent methodology is applied to the evaluation of risk, as well as ensuring risk ratings are in line with already established risk methodology. It also ensures each department within your organization is speaking the same language and what is provided to the Board is consistent.

THIRD PARTY RISK ASSOCIATION

What Does a Risk Matrix Look Like?

Qualitative scoring system		Chance				
		Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Impact	Very High (5)	5	10	15	20	25
	High (4)	4	8	12	16	20
	Medium (3)	3	6	9	12	15
	Low (2)	2	4	6	8	10
	Very Low (1)	1	2	3	4	5

		Consequences				
		Insignificant (1) No injuries / minimal financial loss	**Minor (2)** First aid treatment / medium financial loss	**Moderate (3)** Medical treatment / high financial loss	**Major (4)** Hospitable / large financial loss	**Catastrophic (5)** Death / massive financial loss
Likelihood	**Almost Certain (5)** Often occurs / once a week	Moderate (5)	High (10)	High (15)	Catastrophic (20)	Catastrophic (25)
	Likely (4) Could easily happen / once a month	Moderate (4)	Moderate (8)	High (12)	Catastrophic (16)	Catastrophic (20)
	Possible (3) Could happen or known it to happen / once a year	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
	Unlikely (2) Hasn't happened yet but could / once every 10 years	Low (2)	Moderate (4)	Moderate (6)	Moderate (8)	High (10)
	Rare (1) Conceivable but only on extreme circumstances / once in 100 years	Low (1)	Low (2)	Low (3)	Moderate (4)	Moderate (5)

TPRA | THIRD PARTY RISK ASSOCIATION

What are Inherent & Residual Risk?

- **Inherent Risk** – The level of risk after general information is provided but absent of evaluating any controls in place. Inherent risk takes into account the type of product/service provided, type of data that will be accessed or transferred, geographical location of the third party, and monies to be spent; but, does not take into account the controls the third party has in place.
- **Residual Risk** – The level of inherent risk remaining after implemented controls have been assessed and/or discovered risk has been treated. Residual risk provides a more accurate picture of the risk landscape of a third party as it evaluates the controls in place for sufficiency and effectiveness.

TPRA | THIRD PARTY RISK ASSOCIATION

Assessing Inherent Risk

TPRA | THIRD PARTY RISK ASSOCIATION

Why Assess Inherent Risk?

- Inherent risk is usually calculated before any assessments of the third party take place. It provides a worst-case scenario picture of the third party, should all controls fail.
- Inherent risk is used to categorize a third party, as well as determine what risk-based due diligence efforts should be performed.
- It also assists with determining continuous monitoring assessment cycle times.

TPRA | THIRD PARTY RISK ASSOCIATION

When Do You Assess Inherent Risk?

- Inherent risk is usually calculated during the request for proposal (RFP) process in order to determine what pre-contract due diligence activities are needed.
- If you are just creating your TPRM program, once you inventory your third parties, the next step is to run them through your inherent risk questionnaire to determine their potential impact to your organization (or criticality tier).
- You will also want to recertify your inherent risk questionnaire each time you assess your third party and on an ongoing basis to ensure it is kept up to date. Our relationships with third parties can change over time, as can how we leverage their products/services. Therefore, it is important to re-evaluate the inherent risk questionnaire.

TPRA | THIRD PARTY RISK ASSOCIATION

How Do You Assess Inherent Risk?

- Inherent risk is usually assessed via an Inherent Risk Questionnaire (IRQ). The questions within your IRQ are weighted based on your organization's risk appetite.

[Share a template IRQ]

TPRA | THIRD PARTY RISK ASSOCIATION

Assessing Residual Risk

TPRA | THIRD PARTY RISK ASSOCIATION

Why Assess Residual Risk?

- We assess residual risk to effectively identify, measure, monitor, and mitigate third party risk. It is why TPRM programs exist.
- It also ensures third parties are operating securely and effectively, as well as complying with regulatory requirements and other industry standards.
- Without measuring residual risk, a firm cannot consistently or meaningfully understand and mitigate risks related to third party access to your sensitive data, internal systems, and/or outsourced functions needed to support business operations.
- Failure to appropriately measure and manage this risk can cause organizations to face scrutiny from their regulators, subject them to fines and other legal repercussions, or cause major reputational or financial risk with their customers.

TPRA | THIRD PARTY RISK ASSOCIATION

When Do You Assess Residual Risk?

- Residual risk is measured during the pre-contract and post-contract (or continuous monitoring) phases.
- Once inherent risk is identified, it then drives the level of due diligence required. This due diligence is meant to assess the third party's residual risk.
- Residual risk should not be assessed once per year, but instead, assessed throughout the year using a variety of risk-based mechanisms.
- This ensures your organization maintains a comprehensive view of your third party risk landscape and can proactively mitigate risk that is identified.

TPRA | THIRD PARTY RISK ASSOCIATION

How Do You Assess Residual Risk?

- Residual risk is assessed using a variety of risk-based mechanisms. It all depends on what products/services the third party is providing, what you are providing to the third party, and how critical the third party is to you.
- Assessments of the third party can include, but not be limited to:
  - Information Security Questionnaire – To Include Cloud
  - Limited Information Security Questionnaire
  - Operational Resiliency Questionnaire
  - Financial Stability Questionnaire
  - Operational / Strategic Risk Questionnaire
  - Reputational Risk Questionnaire
  - Offshore Survey
  - Third Party Risk Management Program Questionnaire
  - Privacy Questionnaire
  - Nth Party Review
  - Environmental Social Governance (ESG) Questionnaire
  - Onsite Visits

TPRA | THIRD PARTY RISK ASSOCIATION

Evidence You Can Request/Review

- Penetration Test Results
- Independent Attestations – Including SOC 2, Type II
- Policies and Procedures
- Proof of Key Controls to Evidence Effectiveness (such as scans, logs, cloud security & compliance reports, etc.)
- Vulnerability Reports & Evidence of Patching
- Continuous Monitoring Reports from Risk Rating/Intelligence Organizations
- Financials
- DR/BC Plans & Evidence of Testing
- Incident Response Playbooks & Evidence of Testing
- Employee Counts and Titles (To Review Key Person Dependencies)
- Data Flow Diagrams and Network Architecture Diagrams
- Background Checks & Training Requirements
- Access Reviews
- Model Risk, to include Validation of Models
- Fraud Investigations
- Negative News

TPRA | THIRD PARTY RISK ASSOCIATION

Assessment Cycle Times

- The evaluation of residual risk should take into account your program's maturity, resources, organization's risk appetite, and the third party and/or engagement's current inherent & residual risk ratings. Cycle times may change as maturity increases.

			Residual Risk		
			High	Medium	Low
Information Security Questionnaire – To Include Cloud	Inherent Risk	Critical	Onsite	Every Year	Every 2 Years
		High	Onsite	Every Year	Every 2 Years
		Medium	Every Year	Every 2 Years	Every 3 Years
		Low	No Review	No Review	No Review

Perform Triggered Reviews

- Change in Location to Offshore
- Change in Risk Rating Score
- Change in Ownership
- Change in Product/Services
- Change in Data Sent/Stored
- Change in Contract
- Event or Incident

TPRA | THIRD PARTY RISK ASSOCIATION

Residual Risk Rating

- Based off due diligence assessments, risk rating reports, negative news, past assessments, etc.

	Score	Weight	Weighted Score		
Information Security Questionnaire – To Include Cloud	3	30%	0.9		
Limited Information Security Questionnaire	0	5%	0		
Operational Resiliency Questionnaire	3	20%	0.6		
Financial Stability Questionnaire	2	5%	0.1		
Operational / Strategic Risk Questionnaire	1	5%	0.05		
Reputational Risk Questionnaire	2	3%	0.06		
Offshore Survey	3	2%	0.06		
Third Party Risk Management Program Questionnaire	3	5%	0.15		
Privacy Questionnaire	3	10%	0.3		
Nth Party Review	3	5%	0.15		
Environmental Social Governance (ESG) Questionnaire	1	2%	0.02		
Passed Assessments	3	3%	0.09		
Negative News	1	5%	0.05		
		100%	2.53	High	Residual Risk
Key:					
3 = High					
2 = Medium					
1 = Low					

THIRD PARTY RISK ASSOCIATION

Questions?

Next Meeting: Thursday, April 13, 2023 @ 10 to 11 AM CST

Topic – Panel: “Emerging Risks (ESG, FinTech,Cryptocurrency, Open Banking, APIs)”