Third Party Risk Management Tools & Techniques

Secure Iowa Conference

October 6, 2021

Presenter: Julie Gaiaschi, CISA, CISM
Title: CEO & Co-Founder of TPRA

TPRA | THIRD PARTY RISK ASSOCIATION

Biography:

Julie Gaiaschi, CISA, CISM, is the CEO & Co-Founder of the Third Party Risk Association (TPRA). She has over 14 years of technology and information security risk experience, with the last 10 years specializing in third party risk. In her role as CEO, she provides strategic direction for the non-profit, whose mission it is to further the third party risk profession through knowledge sharing and networking. She also has a passion for helping others enhance their own third party risk management programs.

Prior to co-founding the TPRA, Julie consulted on third party risk for a large bank. She also developed and led a large health payer organization's Third Party Security program. There, she established and executed the third party risk assessment process, which included integration into the Procurement process. Prior to her role as the leader over Third Party Security, Julie was a Senior IT Auditor.

Julie resides in Iowa with her husband and two girls. She enjoys traveling and cooking.

Third Party Risk Association (TPRA)

We are a not-for-profit association created out of a necessity to build a community of like-minded third party risk professionals to allow for the sharing of best practices, exchanging of ideas, and influencing of an industry.

Mission: Further the profession of third party risk through knowledge sharing and networking.

Vision: To be the global voice and standard for the third party risk profession: Advocating its value, Promoting best practices, and Providing exceptional service to its members.

Membership-Based Organization

- Practitioner Plan - Individual
- Student Plan - Individual
- TPRM Service Provider (Vendor) Plan - Organization

Benefits

- Monthly Practitioner Calls
- Quarterly Special Interest Calls – By Industry
- In-Person & Virtual Conferences
- Quarterly Vendor Member Calls
- Members Only Forum, Newsletter, Templates

For more information, please visit www.tprassociation.org.

TPRA | THIRD PARTY RISK ASSOCIATION

Session Description:

THIRD PARTY RISK MANAGEMENT TOOLS & TECHNIQUES

Third Party Risk Management (TPRM), while not a new concept, is continuing to increase in importance. This is mainly due to the threat landscape growing in complexity, organizations having a greater reliance on third parties to support critical services, digital transformation projects growing in momentum, an increase in regulations, and environmental impacts (such as the effects of a pandemic on supply chains). In addition, there has been an increase in regulatory scrutiny on organizations, to ensure they are aware of the risks and impacts their third parties have to their organization.

In this session, we will explore the:

- Importance of TPRM and the role it plays within organizations
- Key components of a TPRM program
- Trending TPRM techniques and tools to address emerging risks

TPRA | THIRD PARTY RISK ASSOCIATION

Importance of TPRM and the role it plays within organizations

What has happened in the last year?

- Threat landscape growing in complexity
  - SolarWinds
  - Kaseya Ransomware Attacks
  - Increase in data breaches
- Organizations having a greater reliance on third parties to support critical services
  - Security – Increased risk for tools to support working from home.
  - Infrastructure – Cloud vendors
  - eCommerce Solutions – Payment Processing and Shopping Cart websites
- Digital transformation projects growing in momentum
  - Business Process Reengineering
  - Proactive Customer Engagement
  - Advances in AI & Machine Learning
  - Smarter Predictive Analytics
- Environmental threats
  - Pandemic
  - Political Threats
- Increased regulatory scrutiny on organizations

TPRA | THIRD PARTY RISK ASSOCIATION

Importance of TPRM and the role it plays within organizations

- To ensure third parties are operating securely and effectively, by adequately monitoring and mitigating risks related to the data and/or process that has been outsourced, an organization must have in place an effective TPRM program.
- Often times, third parties are accessing, transferring, manipulating, and storing organizational data. With this comes increased risk to the organization who has ownership of the data. Although third parties have some responsibility in safeguarding the organizational data, it's the responsibility of the owning organization to ensure that the third party is safeguarding said data appropriately. An organization is only as strong as their weakest link, which may be their third party.
- While there is no way to eliminate the risk of a data breach or verified incident, there are security measures that can be taken by the organization to ensure they understand the risk of working with the third party and take appropriate steps to mitigate the risk.
- Failure to appropriately measure and manage the risks that come along with an organization's relationship with its third party 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

Key components of a TPRM program

Third Party Risk Management Program Lifecycle:

TPRA | THIRD PARTY RISK ASSOCIATION

Planning & Oversight

Key components of a TPRM program

Planning & Oversight, provides an organization with the foundation to build upon and properly support their overall program. This phase ensures the program can address third party risk at the highest level, while also ensuring governance structures are in place to run the program effectively. This phase also ensures key stakeholders are aware of and assist with the implementation of program requirements.

- Policies and Procedures
- Inventory of Third Parties
- Organizational Risk Appetite
- Program Oversight and Governance
- Metrics and Reporting
- Education and Training
- Regulatory Compliance
- Budgeting

TPRA | THIRD PARTY RISK ASSOCIATION

Pre-Contract Due Diligence

Key components of a TPRM program

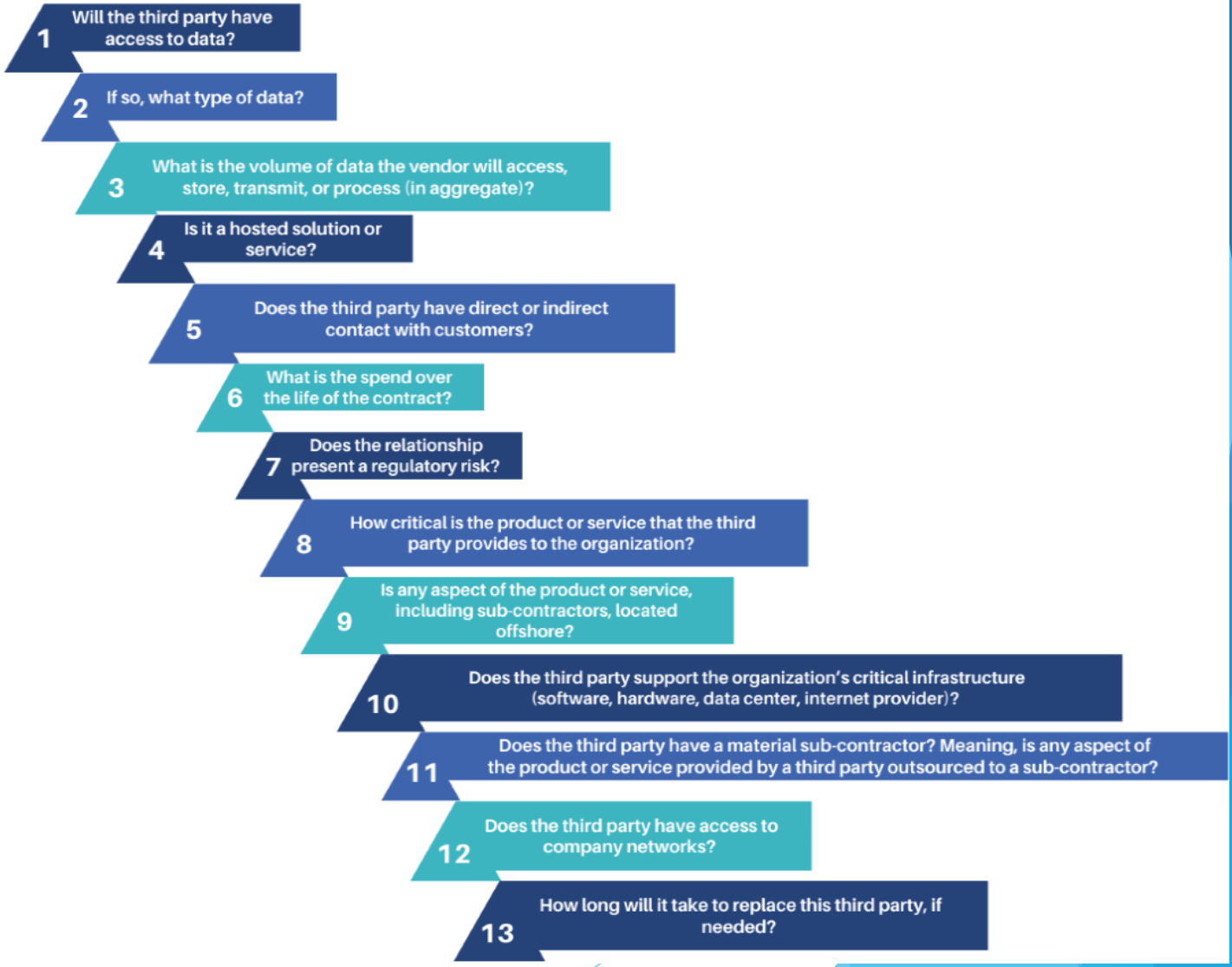
Pre-Contract Due Diligence, ensures that an organization evaluates and identifies potential risks in a third party relationship, prior to signing a legally binding contract. This phase describes how an organization performs risk-based assessments to identify the potential impacts a third party can have to their organization.

- Inherent Risk Questionnaire
- Risk-based Assessments
- Onsite Visits
- Risk Identification & Remediation
- Risk Escalation and/or Acceptance
- Reporting on Residual Risk

THIRD PARTY RISK ASSOCIATION

Pre-Contract Due Diligence

Inherent Risk Questionnaire (IRQ)



TPRA | THIRD PARTY RISK ASSOCIATION

Pre-Contract Due Diligence

Key components of a TPRM program

Types of Assessments:

- Information Security Risk Assessment – May include application, data, and network security, Software Development Lifecycle (LDLC), and Service Organization Controls (SOC) 2 reports.
- Privacy Impact Assessment – Includes data management and regulations.
- Financial Assessment – Involves the viability of an organization.
- Disaster Recovery and Business Continuity (DR/BC) – Covers techniques and processes for continuing business performance following a disaster.
- Physical Security Review – Looks at the badge process, cameras, guards, etc.
- Regulatory Assessment – Examples include Payment Card Industry (PCI), HIPAA, and Gaming.
- Negative News Monitoring – Includes review of negative news alerts (e.g., Google)
- Passive Monitoring – Examples include RiskRecon, BitSight, and Security Scorecard reports.

TPRA | THIRD PARTY RISK ASSOCIATION

Contract Review

Key components of a TPRM program

Contract Review, ensures an organization recognizes the importance of documenting relationship expectations in an agreement that can be upheld in a court of law. This phase discusses the key steps an organization should follow during their contract review process, as well as how to ensure the risk noted within the due diligence phase is properly addressed within contractual language.

- Ensure TPRM program has a seat at the table during negotiations.
- Template Agreements – Work through an Information Security Safeguards addendum, Offshore Addendum, or other addendum depending on the risk impact a third party adds to your organization.
- Ensure a process is in place to sign a contract only after due diligence has been completed.
- Depending on the level or risk, may want to note a transition plan and/or exit strategy within the contract.
- Ensure compliance triggers are in place for non-compliance.

TPRA | THIRD PARTY RISK ASSOCIATION

Continuous Monitoring

Key components of a TPRM program

Continuous Monitoring, requires the organization to assess third party risk on a continual basis to ensure contract terms, business obligations, legal and regulatory requirements, and performance expectations are met.

- Cyclical Assessments Based on Risk
- Onsite Visits
- Continuous Monitoring Tools
- Triggered (Ad Hoc) Reviews
- Risk Identification & Remediation
- Risk Escalation and/or Acceptance
- Reporting on Residual Risk

THIRD PARTY RISK ASSOCIATION

Continuous Monitoring

Key components of a TPRM program

Onsite Visits, important to conduct from a relationship management and assessment evidence/testing perspective.

- Pre-Planning:
  - Review the contract.
  - Review past assessments and current findings.
  - Meet with the business owner & vendor to scope review.
  - Draft agenda and send out for review. Set up travel. Schedule walk through.
  - Create workpapers, assessments, and tests to complete during the visit.
- During Visit:
  - Hold introduction meeting.
  - Perform testing and walkthroughs. Obtain evidence during the visit.
  - Ask follow up questions and note draft findings for validation. Perform testing for key controls and ask to see documentation to evidence testing.
- Post-Visit:
  - Complete workpapers, testing, and validation of evidence.
  - Draft findings for business and vendor review, validation, and response.
  - Close out reporting and note residual risk of vendor.

TPRA | THIRD PARTY RISK ASSOCIATION

Continuous Monitoring

Key components of a TPRM program

Example Evidence to Collect:

- Penetration Test Results (Can accept screen share)
- Independent attestation, including SOC 2, Type II Report
- Policies & Procedures
- Screenshots of key controls to evidence effectiveness (Configuration Settings)
- Vulnerability report & evidence of patching
- Continuous Monitoring report
- Financials
- DR/BC plans and testing
- Employee counts (key person dependency) & significant changes that have occurred
- Network diagram (including cloud architecture) & data flow diagram
- Background check policies and sample of actual background checks
- Employee & Subcontractor access review
- Training – Broadscale (ex. phishing) and specific/targeted training (ex. Developers)
- Model Risk – Ask for validation of models
- Regulatory Disclosures
- Negative News

TPRA | THIRD PARTY RISK ASSOCIATION

Continuous Monitoring

Key components of a TPRM program

Examples of Triggered (Ad Hoc) Reviews:

- Offshore Location(s) Added
- Material Fourth Party Added
- Regulatory Disclosure
- Event or Incident
- Intelligence/Risk Rating Score Drop
- Change in Ownership
- Change in current Product/Services
- Change in Data Sent/Stored
- Change in Contract

THIRD PARTY RISK ASSOCIATION

Disengagement

Key components of a TPRM program

Disengagement, ensures the organization is able to transition away from a third party with minimal impact should the relationship end due to contract expiration or adverse/unplanned conditions are met.

- Contract Review – Termination clause
- Termination Checklist
- Return of Data & Validation
- Destruction of Data & Certification
- Record Retention & Ongoing Review

TPRA | THIRD PARTY RISK ASSOCIATION

Continuous Improvement

Key components of a TPRM program

Continuous Improvement, is an ongoing activity which seeks to enhance the organization's TPRM program as third party risk management guidance, trends/techniques, and emerging risks are realized.

- Frameworks and Industry Best Practices
- Benchmarking & Collaboration Groups
- Maturity Model
- Tools & Techniques
- Regulations & Emerging Risks
- Communication & Education

Trending TPRM techniques and tools to address emerging risks

Revisit what has happened in the last year:

- Threat landscape growing in complexity
  - SolarWinds
  - Kaseya Ransomware Attacks
  - Increase in data breaches
- Organizations having a greater reliance on third parties to support critical services
  - Security – Increased risk for tools to support working from home.
  - Infrastructure – Cloud vendors
  - eCommerce Solutions – Payment Processing and Shopping Cart websites
- Digital transformation projects growing in momentum
  - Business Process Reengineering
  - Proactive Customer Engagement
  - Advances in AI & Machine Learning
  - Smarter Predictive Analytics
- Environmental threats
  - Pandemic
  - Political Threats
- Increased regulatory scrutiny on organizations

TPRA | THIRD PARTY RISK ASSOCIATION

Trending TPRM techniques and tools to address emerging risks

How has the last year changed Third Party Programs?

- Third Party Risk Programs are increasing their focus; no longer just on cyber. Now need to review an organization's financials, operations, compliance programs, and even environmental/social/governance (ESG) impacts.
- Third Party Risk Management departments are asked to do more with less.
- Working with additional subject matter experts (SMEs) to cover additional risks.
- Working with Legal and Procurement to enhance contract clauses.
- Being incorporated into the Incident Response and BC/DR plans.
- Increasing budget to purchase additional tools for due diligence and continuous monitoring processes.
- Automating more processes.
- Working with Compliance to ensure meeting regulatory requirements.
- Thinking more proactively instead of reactively.
- Enhanced Board and Executive level support.

TPRA | THIRD PARTY RISK ASSOCIATION

Trending TPRM techniques and tools to address emerging risks

- SME Assistance: Engage other teams to participate in the assessment process.
- Incorporating Regulatory Compliance Reviews Into TPRM Programs
  - **The Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC)[**Docket ID OCC-2021-0011] - Proposed Interagency Guidance on Third-Party Relationships: Risk Management – Goes through the Third Party Risk Management Lifecycle to be followed by Financial Institutions.
- Environmental Social Governance (ESG) – Incorporating components of ESG into your third party risk reviews. ESG refers to environmental, social governance impacts of an organization based on the decisions they make and activities they participate in.
- Incident Response Playbook – Third Party Risk Managers should be a part of the incident response playbooks. Often times, Security leads the incident response practices.
- Enhance contract clauses to ensure including security controls, compliance triggers, and update “force majeure” clauses to be more specific.
- Artificial Intelligence – Used to proactively monitor third party risk.

TPRA | THIRD PARTY RISK ASSOCIATION

Conclusion

- Importance of TPRM - To ensure third parties are operating securely and effectively, by adequately monitoring and mitigating risks related to the data and/or process that has been outsourced, an organization must have in place an effective TPRM program.
- Key components of a TPRM program
  - Planning & Oversight
  - Pre-Contract Due Diligence
  - Contracting
  - Continuous Monitoring
  - Disengagement
  - Continuous Improvement
- Trending TPRM techniques and tools to address emerging risks
  - Engage SMEs within your organization
  - Leverage smarter, more proactive tools
  - Incorporate more risk factors/views into your assessments
  - Enhance contract language
  - Review and enhance operational resiliency efforts

Questions? Thank you.

Third Party Risk Association (TPRA)

Website: www.tprassociation.org

2022 Spring Conference: www.artofthirdpartyrisk.org

LinkedIn: https://www.linkedin.com/company/TPRA

YouTube Channel: Third Party Risk Association

Email: Julie@tprassociation.org