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
- Roundtable – **Findings & Follow-Up**
  - Issue Validation
  - Escalation & Risk Acceptance
  - Reporting
  - Issue Tracking & Remediation
- Closing Remarks

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks

- Fall Virtual Conference – "Evolving Past Point-In-Time Assessments" will be held on Wednesday, August 11th from 9 AM to 5 PM Central. Registration is now open! Please visit our conference site under "Events" or go to https://www.tprassociation.org/2021-virtual-conference.
- 7/13 @ 10 AM CST - TPRA New Member Call
- 7/15 @ 10 AM CST - Healthcare/Health Insurance Special Interest Call
- 7/15 @ 1 PM CST - Finance & Insurance Special Interest Call - Guest Speaker - ISS Corporation on ESG Scoring
- 7/20 @ 10 AM CST - Manufacturing Special Interest Call
- 7/20 @ 1 PM CST - Technology Special Interest Call
- 7/22– TPRA Focus Group: Assist TPRA with building out our TPRM 101 Guidebook.

TPRA | THIRD PARTY RISK ASSOCIATION

Roundtable - Findings and Follow-Up: Issue Validation

- Assumption: You are working from set criteria used to evaluate governance, risk management, and controls. May come from a standard/framework you and/or third party uses, contract clauses, regulations, and/or communicated assessment criteria.
- Constructive/transparent communication is helpful to your assessments and can lead to improvements where needed. Communications must be accurate, objective, clear, concise, constructive, complete, and timely.
- Determine who will send out the communication to ensure a consistent message.
- Validation of issues with the third party is key to not only ensuring you have accurate information and tested the right controls, but also to establish a trusting relationship with your third party.
- Information sent to validate issues can include, but not be limited to, the scope of your assessment, scope limitations, evidence obtained and reviewed, results of your test, and the conclusion reached, as well as the risk rating.
- When releasing results to third parties, you may want to include limitations on distribution and use of the results. You may also want to consult with Legal and your impacted Business Unit before distribution to make them aware.

TPRA | THIRD PARTY RISK ASSOCIATION

Roundtable - Findings and Follow-Up: Escalation & Risk Acceptance

- If the finding is Critical and/or you are not making progress with your vendor on action plans, then you will want to follow an established escalation plan. This is to ensure the impact of the risk is communicated and a plan of action is established.
- Escalation Process
  - Be prescriptive about this process and ensure supported by leadership.
  - Make sure certain levels of leadership can accept certain levels of risk.
  - Establish a third party risk management committee. (Board and executives may need to be made aware.)
  - Track escalations and approvals in a central repository. Also note next steps to downgrade the escalation. (Types of actions you can take related to a risk.)
  - Work off cycle when escalation is required immediately.
- Risk Acceptance
  - May want to align risk approval to contract spend approval levels.
  - Quantify potential business impact value (risk appetite of organization)
  - Note the Issue, risk (level + likelihood + velocity), impact (value * probability), proposed remediation, approval levels

TPRA | THIRD PARTY RISK ASSOCIATION

Roundtable - Findings and Follow-Up: Reporting

- May want to issue a final report to the Business and/or Risk Committee.
- This report can include, but not be limited to, general information on the third party and the services they provide (as well as their inherent risk rating), assessments performed, when performed, and who performed them, validated issues and established corrective actions, as well as target dates and risk levels for each finding, an overall opinion of risk for the third party and potential impact should the third party fail (residual risk rating), and any other relevant information. Will also want to include acknowledgement of satisfactory performance.
- Overall residual risk rating is driven off assessment results, outstanding issues, and risk acceptances.
- An opinion should take into account the expectations of senior management, the board, and other stakeholders and should be supported by sufficient and relevant information.
- May have a GRC tool or a TPRM platform that performs reporting capabilities. Third party profiles, assessments, and results may be captured within this tool. Would then need to ensure reporting capabilities are set up on a frequent basis and provide to relevant audiences (Business Owners and Risk Committees, as well as Senior Management).

TPRA | THIRD PARTY RISK ASSOCIATION

Roundtable - Findings and Follow-Up: Issue Tracking & Remediation

- Issue Tracking
  - Central repository for findings, risk levels, and target dates. where the vendor can access their own issues, add remediation plans and updates, provide evidence of remediation, and submit for closure.
  - Establish a cadence for following up on the remediation of issues (may be based off risk (High = every week & Medium = 30 days before due date).
  - Ensure the follow up process is automated so that you are addressing risk in a timely manner.
  - Communicate the progress of remediation activities to key stakeholders and request assistance if needed.
- Validation of Remediation
  - Establish a validation process and ensure it includes re-testing where applicable. Ensure business also signs off on validation of remediation.
- Closing Issues
  - Establish a close-out procedure for issues. May want to determine cycle of next review based on risks and remediation of current issues.

THIRD PARTY RISK ASSOCIATION

Next Meeting: Thursday, August 12th from 10 to 11 AM Central

Have a great weekend