VIEW POINT

# ELEMENTS TO CONSIDER IN A THIRD-PARTY CYBER SECURITY RISK MANAGEMENT PROGRAM


## Abstract

This paper focusses on the elements that must be considered in a Third-Party Cyber Risk Management program. It discusses some of the challenges that an organization faces while handling a large questionnaire driven cyber security assessment program for their suppliers. It aims towards bringing out solutions to those challenges by adoption of foundational principles, practical enablers and implementable best practices.


Infosys®
Navigate your next

Organizations have become more and more cost-conscious, focussing on their core competencies and strategic functions and outsourcing all non-core activities to third parties. As they grow, so does their reliance on third parties. What also grows is the perceived technology, infrastructure and data boundaries. With this increased reliance and cross sharing of critical data, a risk in the third parties' environment, becomes a risk for all.

Third Party IT Security Risk Management aims to address cybersecurity risks that exist in our third parties' landscape. It involves working with the third parties to increase their cyber security posture/maturity, thereby reducing the risk to us.

## Challenges

Conceptualizing, establishing and operating a Third-Party Cyber Security Risk Management program, has its own set of challenges that include

### Incomprehensive supplier coverage

Supplier coverage is about ensuring that none of the suppliers are getting missed out from the target scope. Quiet often, there is a disconnect in the process (and underlying tools) being used for third party lifecyle management and third party cyber security assessments. This disconnect results in one party (often the cyber security teams) being completely blind-sided to the very existence of a supplier and the other party (supplier relationship management/business) to the existence of supplier assessment process/ requirements. How can an organization protect itself from a threat within its supplier's environment, if it (as in the third party assessment process) is not even looking at that supplier?

### Outdated or irrelevant questionnaire

It's important to have a questionnaire, which is exhaustive but proportional to the risk that the supplier poses. This risk (sometimes called as inherent risk) exists due to the very nature of business that an organization does with a third party. Can an organization spend the same efforts for a supplier providing them a packaging material vs a supplier providing a critical component?

### Late visibility of risk

Supplier assessments often run into months. Many times a risk is recorded, but not reported as the assessment has not completed a particular milestone (For e.g.: All evidences have not been provided/reviewed, All questions have not be answered etc.). Alternatively, certain risks might become more severe or prone to materialization, due to the changes in global threat landscape. How should such risks be handled, reported or prioritized?

### Longer turnaround time from suppliers

Turnaround time to get responses from suppliers is very long. Whether it is responses to initial questionnaire, or to queries, or to RTP plan. Longer turnaround times, often results in poor visibility of assessment completion timelines and inadequate utilization of resources. What can we do to reduce this turnaround time?

### Management of such large programs

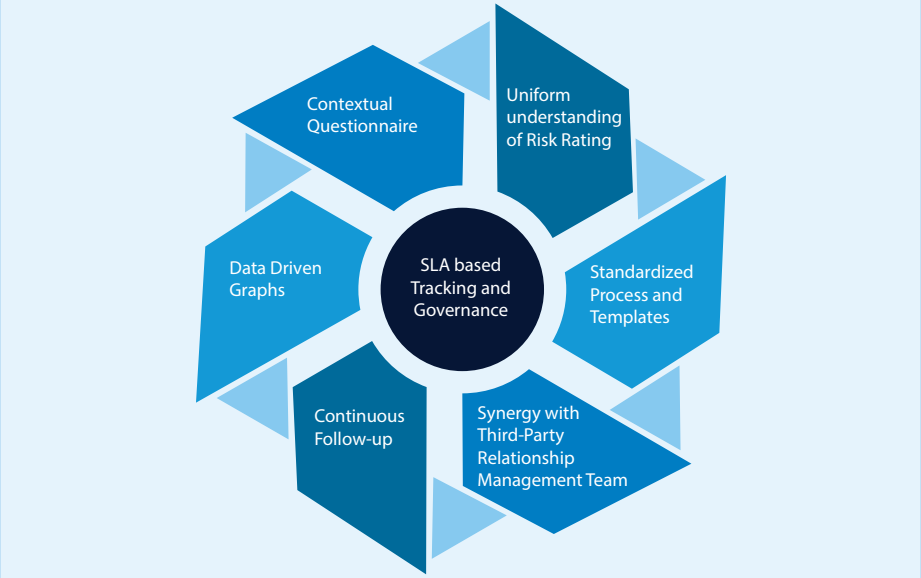
Assessment of suppliers has a lot of moving parts. Supplier keep getting onboarded, offboarded, put on hold or start providing additional services. With so many moving elements, such program has it's own set of inherent challenges. Can the program leadership be provided with answers to the following, on demand: In which state a supplier assessment is? Has a supplier been offloaded? Can we project how many assessment will we be able to complete by this quarter end? What escalations are still open and who are they pending with? Can we get a report of all suppliers and their current status for the consumption of a commodity leader/director? What will it take to trigger an adhoc assessment (For e.g.: Presence of Log4j Vulnerabilities in supplier environment)?

With limited resources, it becomes taxing on a leader to overcome the above challenges. There are principles that can solve these challenges specifically addressing the questionnaire driven remote assessments area.

## Solution and Architecture Principles

Third Party Cyber Security Risk Management program challenges can be overcome if we design right and then **operationalize with excellence.** Architecture principles and Enablers can help to design a powerful and practical Third Party IT Security Risk Management program. These principles can also help us in executing the **design with more certainty.**

The alongside figure, summarizes these principles:




**Contextual Questionnaire** ensures that the control areas being assessed are in line with the risk that the supplier poses. It also ensures that assessment efforts are better utilized

**Uniform understanding of Risk and Risk Ratings**, mandate that assessors asses the control failures coherently across multiple suppliers. It also ensures that two different assessors reviewing the same evidence of the same supplier, eventually conclude on the same observation

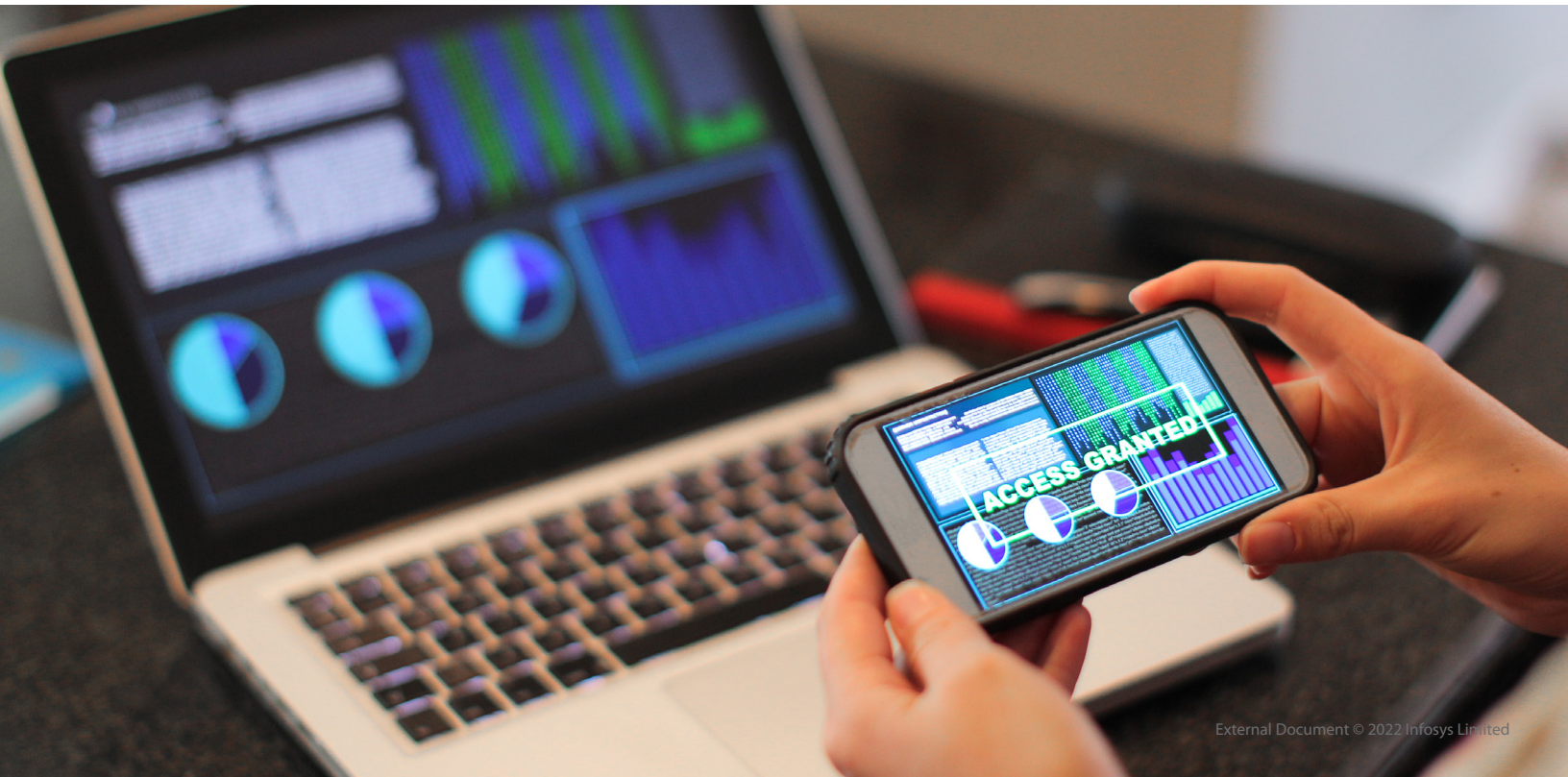
**Standardized Process and Templates** aims towards reducing ambiguity in communication with the supplier. It also improves productivity by reusage of artifacts

**Synergy with Third-Party Relationship Management Team** aims towards reducing the gaps in Third Party Lifecycle Management and Third Party Assessments processes/ tools. It also utilizes the influence that relationship managers have on their corresponding suppliers

**Continuous Follow-up** is a foundational principle for any third-party assessment. Without having adequate resources and documented processes for continuous follow-ups (process/people/technology), not much can be achieved

**Data-Driven Graphs, SLA Tracking and Governance** aim towards doing more with less. These principles help in providing meaningful information on-demand.

Let us look at the **Enablers and Best Practices** for implementing the above architecture principles



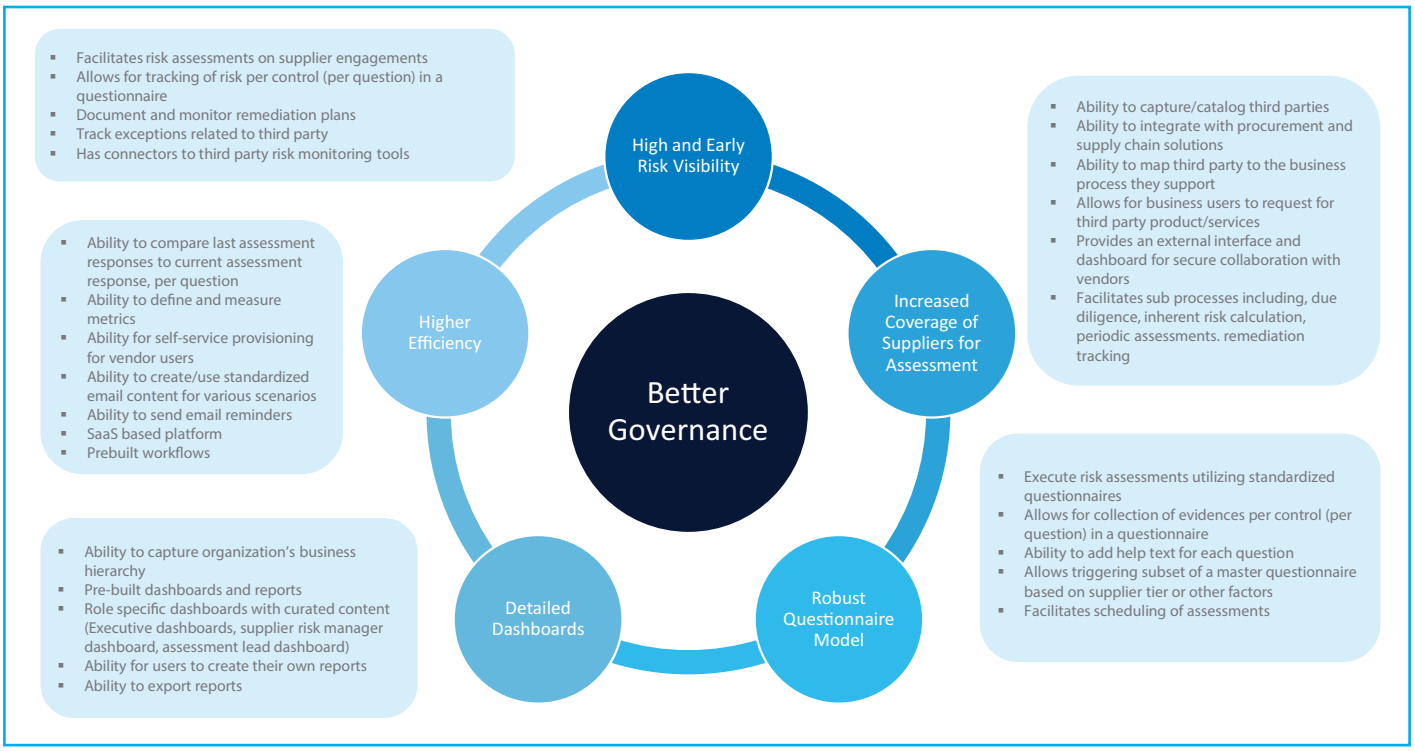
| | |
|---|---|
|  <br>**Contextual Questionnaire** | • Create or adopt a questionnaire for third parties that is aligned to the **organization's risk appetite**<br>• Have **qualifiers** that help in **reducing or expanding** the question sets based on the supplier's tier (or inherent risk's levels)<br>• Review **previous responses** from the supplier and accordingly simplify the questionnaire. For e.g.: Splitting this question<br>*"a) Do you allow remote access to systems and is it secured with MFA"* into two parts can reduce the need of additional clarifications: *"a) Do you allow remote access to systems*<br>*If Yes,*<br>*b) Is MFA enforced for remote access?"*<br>• Be explicit on the **type of evidence** that is required per question/control (For e.g.: DR Plan, MFA Configuration Screenshot, Redacted Vulnerability Scan report etc.)<br>• Ensure that the assessment questionnaire is aligned with Industry standard/regulations, so that you can readily consume the **attestation reports** or the **certifications** provided by the supplier |
|  <br>**Standardized Process and Templates** | • Design the detailed process beforehand with **clear entry and exit criteria** for conducting the assessments, getting the remediation plan and following up for remediation closure<br>• Anticipate challenges (For e.g.: Evidence in local language) and firm your views on how they will be handled<br>• **Create templates** for everything that you can think of, including emails (missing evidence, evidence clarification, reminder for responses, escalations, assessment triggered, RTP expected etc.), trackers (escalation trackers, risk tracker, remediation tracker etc.), definitions (control expectation, risk statements etc.) and reports (assessment summary, remediation plan report, remediation completed report etc.) |
|  <br>**SLA based Tracking and Governance** | • **Formulate the SLAs** (For e.g.: number of days for initial response from supplier, number of days for response review, number of days for providing RTP etc.) and create escalation mechanisms to handle violations<br>• Conduct periodic reviews, understand/address challenges (both from your team as well as from external stakeholders) |
|  <br>**Continuous Follow ups** | • Questionnaire drive remote assessment requires continuous follow ups (responding to a questionnaire is not the key business of a supplier), so be prepared and adequately staffed<br>• If possible, use system generated reminders |
|  <br>**Uniform Understanding of Risk Ratings** | • Train your team to have a **uniform understanding** of the controls, expected evidence and risk<br>• Use standardized templates to communicate the control expectations and risk statements to the supplier and internal stakeholders |

| | |
|---|---|
| **Data Driven Graphs/ Metrics/Insights** | • Envision or understand (from management) what **data points** will be required at the end of the Program cycle and start capturing it before hand<br>• **Predict (and represent)** the outcomes based on the data being captured (How many assessments will get completed by particular date etc.) using metrics. For e.g.:<br>  • % of suppliers that provide sizeable evidence as part of first response<br>  • % of suppliers that respond to the assessment survey<br>• Provide **actionable deep insights** to leadership. For e.g.: Create correlation of risk exposure of the suppliers with current top attack vectors. This data can be used in prioritizing the remediation timelines based on more prevalent threats |
| **Stakeholder Management** | • **Run campaigns** for the third-party relationship management team(s), communicating the need of the program and expectations<br>• Suppliers are very sensitive towards their rapport with third-party relationship managers. **Established synergy with the relationship managers** to utilize the influence that they have on respective suppliers (For e.g.: escalating in case of no response from Supplier etc.)<br>• Inform the suppliers about the program start, before hand |

## Expected features from a Third Party Risk Management Platform

Often Third Party Risk Management is also about covering a large pool of supplier base in a short time. One of the key elements of third party risk management is to have a single platform that can help in managing such a program so that it runs effectively and efficiently at a larger scale.

A Third Party Risk Management platform should support the below feature "out of the box" (aligned to challenges):




## Conclusion:

Risk arising due to third parties can paralyze an organization and has rightly earned it's place in board meeting agendas. Managing third party cyber security risk is no longer about a regulatory obligation that needs to be fulfilled, it is a good business practice. It is imperative for the organization to have a well planned and adequately resourced Third Party Cyber Risk Management Program.

The key takeaways for managing questionnaire drive supplier assessments from this paper are:

- Keep the questionnaire contextual to the risk posed by supplier
- Standardize and develop reusable templates
- Established synergy with the relationship managers
- Provide actionable deep insights to leadership
- Formulate and enforce SLAs
- Develop uniform understanding of the controls, expected evidence and risk

We hope the insights provided in this paper, makes your Third Party Risk Management program more rewarding and fruitful.

Third Party Cyber Security Risk Management can be taxing on your teams. Infosys can work with you at every stage of your Third Party Risk Cyber Security Management program journey.

For more information on Third Party Risk Management Services of Infosys, please write to: CyberSecurity@infosys.com

## About the Author

Gaurav Negi
Principal Consultant

Gaurav Negi has 19+ years of experience across industries in the areas of Information Security Implementation and Consulting, which includes Program Compliance Management, Information Risk Lifecycle Management and Implementation of e-GRC Framework/Tools. Gaurav has worked with clients on SOX Compliance, ISO 27001 Implementation, eGRC Tool Implementation and Third Party Risk Management. Gaurav possesses industry certifications like "SABSA Chartered Security Architect – Foundation Certificate (SCF)" and "Certified Information Systems Auditor (C.I.S.A)"

For more information, contact askus@infosys.com

Infosys®
Navigate your next