Third Party Information Security and Data Privacy Assessment

Version 4.0

12/06/2021

Document Ownership – Cyber Security Assurance Team

NOTICE

The information contained in this document is not to be used for any purpose other than the purposes for which this document is furnished by Genpact, nor is this document (in whole or in part) to be reproduced or disclosed to other Genpact employees without a need to know, or to any third party or made public without the prior express written permission of Genpact.

Version Control

Version No.	Version Date	Type of Changes	Author	Approver	Date of next review
1.0	02/02/2018	First draft	Vinay Bangera	Vinay Bangera	
2.0	21/03/2019	Updated	Vinay Bangera	Ram Hegde	20/03/2020
3.0	19/02/2020	Updated sections to remove specific guidelines	Vinay Bangera	Sriram Lakshmanan	18/02/2021
3.1	09/06/2020	1. Updated sections on Data Privacy and Scope Change Reassessments 2. Aligned/formatted as per DMS	Vinay Bangera	Sriram Lakshmanan	08/06/2021
4.0	12/06/2021	• Updated step 4 of section 4 • Updated step 3 in section 6	Vinay Bangera	Sriram Lakshmanan	11/06/2022

Contents

1. Introduction

Third Party Risk Management is one of the vital areas to manage as far as information security is concerned. Enterprises with a better understanding of their third-party ecosystem have a better chance in managing third party risks effectively. With advancement in digital technologies, and spurt in cloud services, it is all the more important to have a good grasp of third parties.

2. Purpose

The Purpose of this document is to describe the Information security assessment process for Third Parties (Vendors / Contractors / Partners). The objective is to proactively identify and manage third party information security / data privacy risks so that Genpact can take proactive steps to avoid and/or mitigate risks. Information Security Assessment for all third parties are conducted as per the process and guidelines provided in this document.

3. Third Party / Vendor Governance

Genpact has established the Vendor Governance Office (VGO) which has the mandate to manage and govern all third parties. Information Security team provides Subject Matter Expertise to the Vendor Governance Office. Information Security Team works with the VGO to conduct information security assessment. Information Security Assessments are conducted during third party / vendor onboarding process and / or periodically as per the criteria set by the VGO.

4. Third Party / Vendor Onboarding

The successful onboarding of a third party requires co-ordination and communication between various stakeholders – Business, Sourcing, Vendor Governance Office (VGO), InfoSec team, Data Privacy team, Legal and other teams as required. Here are major steps in the onboarding process:

Step 1 – Review of Risk Assessment Questionnaire (RAQ)

RAQ which provides an overview of the services provided by the vendor, the type of data accessed by the vendor, and other high-level information about the third party, is submitted by the sourcing team to the VGO. Sourcing works with business to complete the RAQ. VGO circulates the RAQ with all concerned teams including Infosec. Infosec SME reviews the RAQ to determine the Infosec and Data Privacy Risk. Six key aspects are reviewed by the Infosec SME:

Genpact Data to be stored, processed or transmitted by the third party.

Highest data classification level of the data to be stored, processed or transmitted by the third party.

Personal Identifiable Information to be stored, processed or transmitted by the third party.

Volume of data stored, processed or transmitted by the third party

Access to Genpact's or Client's network.

Physical access to Genpact or Client premises.

Infosec SME also reviews various additional tabs of the RAQ to get more information about the engagement.

Step 2 – Request for Information Assurance Documents

Infosec SME gets a good high-level understanding of the third-party engagement. Depending on the engagement type, Infosec SME may request additional documentation to confirm understanding of the engagement or to get additional information. Typical documents that may be requested by the Infosec SME are as follows:

- Architecture Diagram / Document
- Data Flow Diagram
- SOC2 Type2 Report
- ISO 27001 Certification (with Statement of Applicability if required)
- Independent Penetration Test Report
- Self-Assessment Questionnaire
- PCI DSS Certificate
- Product Security Assurance
- Other documents as required

Once assurance documents are received, the InfoSec team reviews them for their validity, results and findings / observations. In case of any issues/findings, the team requests for a remediation response from the third party.

Risk Acceptance Process: If the Information Security SME / team determines that the vendor / third party does not have appropriate security controls or lacks key documents, the Infosec SME / team can refer the case to Risk Advisory Board / Risk Council. VGO coordinates the entire Risk Approval Process. Once the Risk is accepted by key stakeholders, as per the Risk Acceptance Process, the Infosec SME / team may provide conditional approval or final approval depending on the recommendation from CISO.

Step 3 – Information Security Clearance / Approval

The InfoSec team takes a final decision to approve the vendor / third from Information Security perspective. Clearance/approval is provided along with the InfoSec clauses/requirements that should be included in the vendor contract to cover Genpact from InfoSec risk associated with the engagement or the relationship with the third party. The Sourcing team works with legal in order to include these clauses in the vendor contract.
Please note that during any of the steps listed above, the InfoSec team may have calls/meetings with various stakeholders including vendor in order to obtain a better clarity or understanding. On-site visit can also be conducted. Infosec SME is authorized to provide clearance / approval.

Step 4 – Executive Summary

Infosec SME creates Executive Summary for high risk vendors who store / process or transmit significant volume of Genpact data. Please note Executive Summary is not created for all vendor engagements – consulting / time & material engagements are excluded.

See Appendix A for the Information Security Assessment Flow

5. Data Privacy Assessment

While privacy assessment / due diligence is conducted by the legal team for all engagements where Personally Identifiable Information is shared with third, enhanced Data Privacy Assessment will be conducted for high risk third parties. The criteria for high risk data privacy assessment will be set as agreed between Infosec and the Data Privacy Office.
Privacy Questionnaire will need to be completed by the third party. Industry recognized certificate will be accepted by the SME in lieu of the privacy questionnaire. Responses will be reviewed by Infosec SME and shared with the legal team and / or Data Privacy Office (DPO) as needed. Third parties who do not have adequate privacy controls will be referred to the DPO and the VGO for further action.

6. Periodic / Annual Assessment Process

Step 1 – Understand the Products / Services offered by the Third Party

Infosec SME interacts with Business SPOC for the third party, and relevant stakeholders to understand the product / services offered by the third party. Infosec SME may request details about the engagement such as “highest data classification” and volume of records of data, stored/processed or transmitted by the third party.

Depending on the engagement type, Infosec SME may ask additional questions to get a full and a broader understanding of the engagement. A formal notification or email will be sent to the third party either by the Infosec SME or Business SPOC or Sourcing Lead.

Step 2 – Review of contracts and historical documents

All relevant documents related to the engagement to confirm the understanding of the engagement type is reviewed in this step. This may include data flow diagrams, architectural diagrams, product whitepapers etc. Infosec SME will also request copy of the contract / agreement executed with the third party and / or other documents as required. Infosec terms / conditions related to the engagement will be reviewed for any major contractual deficiency or gaps.

Step 3 – Information Security Questionnaire / Review of Additional Documents

Depending on the engagement type, Infosec SME may request the third-party service provider to complete Genpact’s Infosec Assessment Questionnaire. Business SPOC / Sourcing may need to fill certain sections of the questionnaire as well.

Infosec SME will define the timeline / deadline to complete the questionnaire. Following domains are covered in the questionnaire:

- Risk Management
- Security Policies
- Asset Management
- Human Resource Security
- Physical Security
- Communication and Operations Management
- Access Control
- Information Systems Acquisition Development & Maintenance
- Incident Management

- Business Continuity and Disaster Recovery
- Network Security
- Third party Governance
- And Cloud Security

Infosec SME may also request additional documents such as:

- SOC2 Type2 Report
- ISO 27001 Certification (with Statement of Applicability if required)
- Independent Penetration Test Report
- Self-Assessment Questionnaire
- PCI DSS Certificate
- Product Security Assurance
- Other documents as required

Once all assurance documents are received, the InfoSec team reviews them for their validity, results, findings, etc. In case of any issues/findings, the team requests for a remediation response from the vendor.

Note: Infosec SME may setup interviews / calls to seek clarification or document any evidences which cannot be shared by the third party. Onsite audit may also be conducted and / or additional questionnaire may be sent to the third party if required.

Data Privacy Assessment will also be conducted by the Infosec SME during annual / periodic reassessment or any scope change assessment.

Risk Acceptance Process: If the Information Security SME / team determines that the vendor / third party does not have appropriate security controls or lacks key documents, the Infosec SME / team can refer the case to Vendor Governance Office. VGO coordinates the entire Risk Approval Process. Once the Risk is accepted by key stakeholders, as per the Risk Acceptance Process, the Infosec SME / team may provide conditional approval or final approval.

Note: Anytime during the assessment, if the Infosec SME experiences unreasonable delay from the third party or any other stakeholder, the SME may refer the case to the VGO and may recommend putting the third party in non-compliant list. The expectation is that VGO will highlight all such cases to the Vendor Governance Steering Committee for necessary action.

Step 4 – Closing Annual / Periodic Assessment

If all the documents / evidences are found to be satisfactory, the Infosec SME will prepare a summary report and work towards closing the periodic / annual assessment process. Recommendations, if any, will be sent to the third party. The recommendations typically includes mitigation steps to remediate any security gaps / deficiencies identified during the assessment. If there are any contractual gaps / deficiencies, the Infosec SME will notify the Business SPOC and VGO to consider amending the contract / agreement with the third party at the earliest possible date.

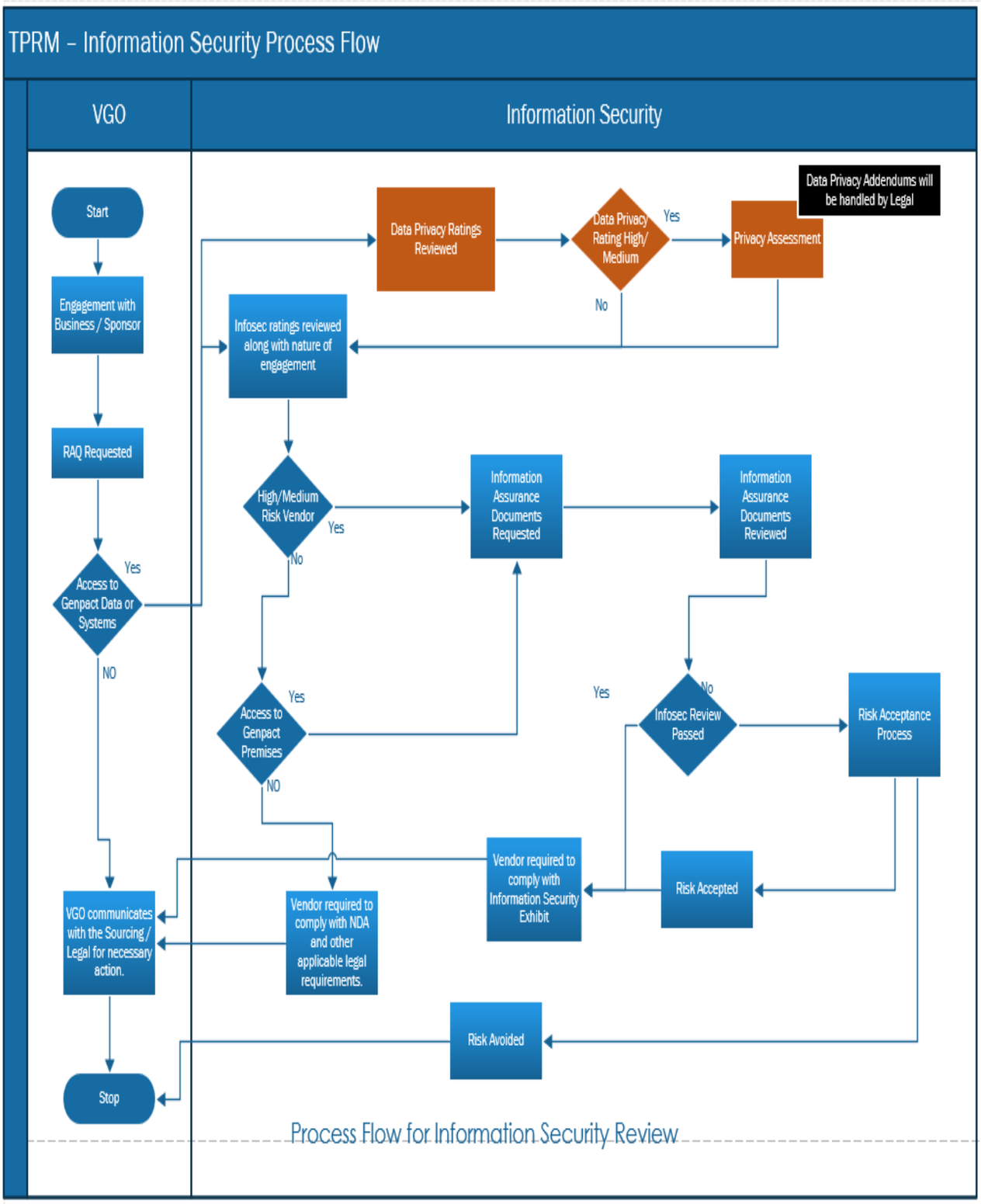
See Appendix B for the Periodic / Annual Security Assessment Flow

7. Scope Change / Reassessments

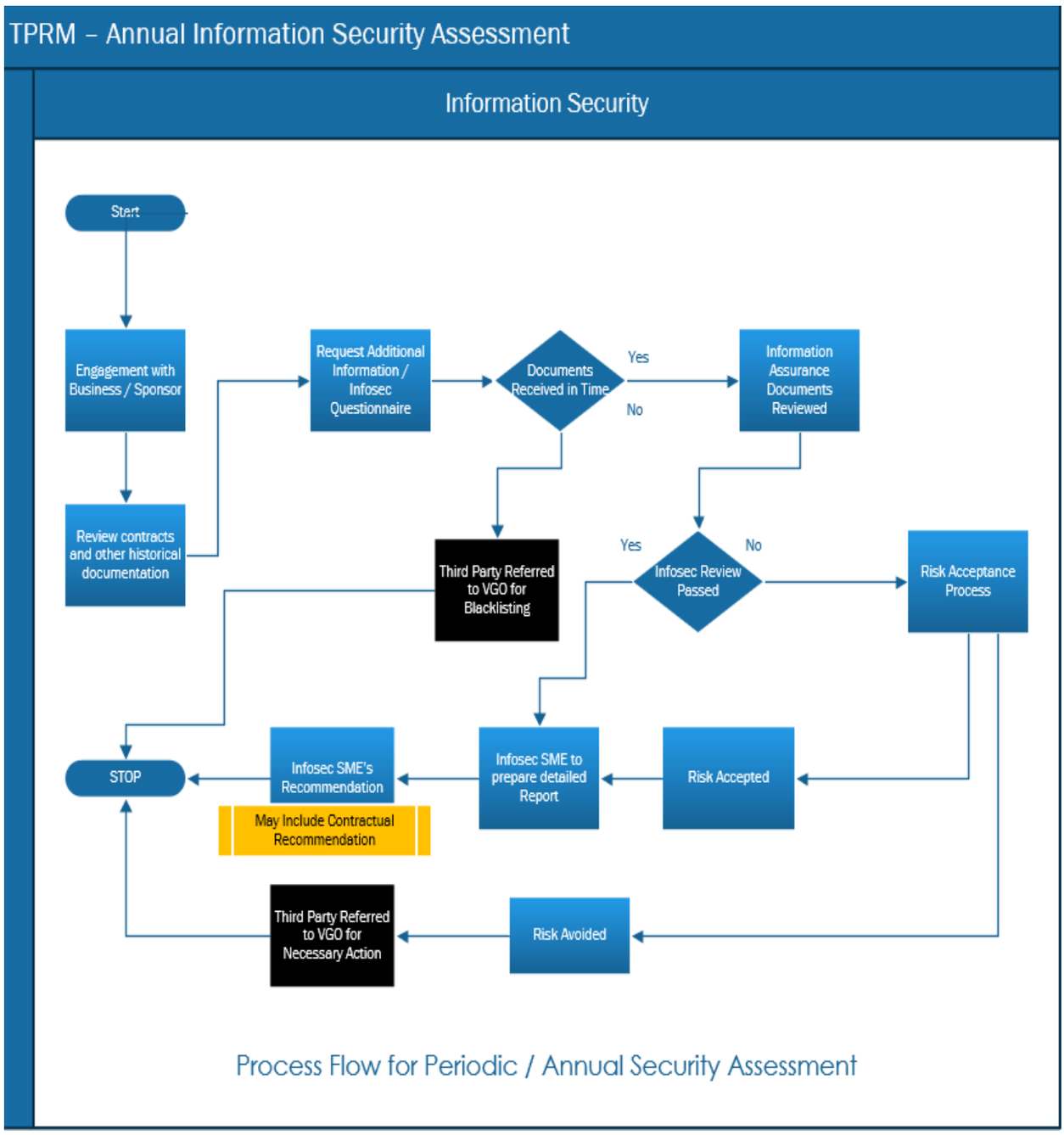
VGO will identify third parties who need to be reassessed due to change in the scope of the services. Infosec SME will consider the following aspects for any scope change or periodic reassessment engagements:

- Review of contracts / agreements.
- Change in the deployment model
- Change in the physical location of service facilities
- Change in the security architecture or controls
- Addition of new capabilities
- New Software
- New Process
- New development process
- New subcontractors

8. Appendix A – Information Security Process Flow



9. Appendix B – Periodic / Annual Information Security Assessment



10. Annexure

10.1 Document Reference List

Please refer to the ISMS Master List of Documents.

10.2 Abbreviations and Definitions

Please refer this Link.