# Enterprise IT Risk Management Process

Version 1.4

Date – 02/04/2020

Document Ownership – Cyber Security Assurance Team

Transformation
Happens Here

# 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 | Oct 30, 2017 | First draft | Vinay Bangera | Vinay Bangera | Oct 30, 2017 |
| 1.1 | May 7th 2018 | Updated Risk Category Table – section 6.7 | Vinay Bangera | Vinay Bangera | May 7th 2019 |
| 1.2 | Feb 27th 2019 | Added Mission statement and updated to reflect govern current process | Vinay Bangera / Shailaja S | Ram Hegde | Feb 27th 2020 |
| 1.3 | Feb 18th 2020 | No Change | Vinay Bangera / Shailaja S | Sriram Lakshmanan | Feb 27th 2021 |
| 1.4 | 02/04/2020 | Format updated/aligned as per Document management procedure | Vinay Bangera / Shailaja S | Sriram Lakshmanan | 01/04/2021 |

## Contents

# 1 Introduction

With Information Technology becoming increasingly critical for Enterprises to meet their strategic business goals, it is imperative for Genpact to proactively manage potential risks associated with the use, ownership and adoption of Information Technology in Business Process'. This new reality has necessitated Genpact to establish a process that allows a comprehensive view of the key risks in the IT environment at Genpact.

# 2 Purpose

The Purpose of this document is to describe and govern the 'Enterprise IT Risk Management" (EITRM) program, set up to proactively identify and manage key IT risks, to optimize the impact of IT on Genpact's strategic objectives.

# 3 Mission

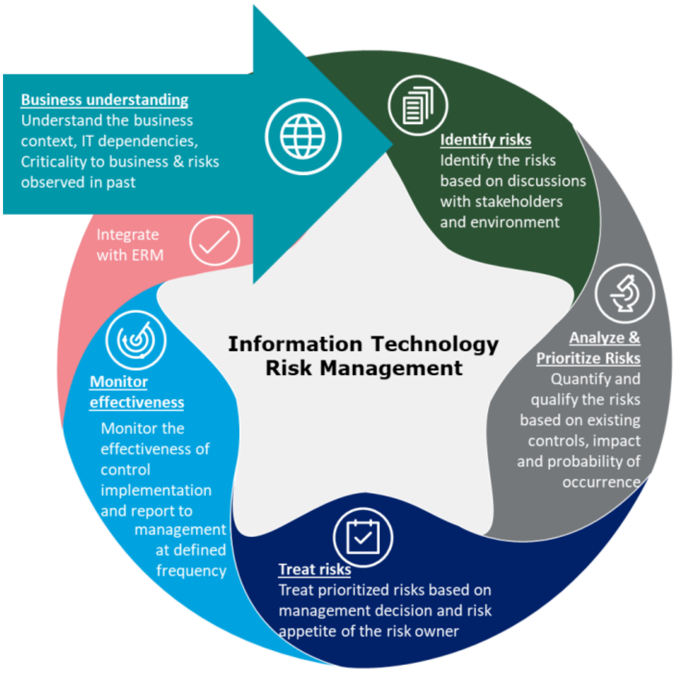
Mission of EITRM program is to "Optimize IT's contribution to Genpact's Business Objectives, by effectively managing key IT Risks"

# 4 Process

EITRM Process at Genpact consists of systematic steps of identifying, assessing, analysing and mitigating key IT risks. Based on RiskIT framework (COSO ERM framework adopted for IT), the Risk Management process is intended to improve management of IT risks, by -

- Defining methodology, practices and a common language and criteria for assessing key IT Risks
- Conducting Periodic Risk Assessment of key Technologies / IT Processes, in addition to need-based assessments (significant change in technology landscape or in major IT Process)
- Keeping an eye to identify key risk indicators from various sources viz major incidents, assessments, audit reports etc.,
- Driving prioritization through visibility of IT Risk Universe, to support Risk-Aware decision making.

# 5 EITRM- Process Framework



Information Technology Risk Management

**Business understanding**
Understand the business context, IT dependencies, Criticality to business & risks observed in past

**Identify risks**
Identify the risks based on discussions with stakeholders and environment

**Analyze & Prioritize Risks**
Quantify and qualify the risks based on existing controls, impact and probability of occurrence

**Treat risks**
Treat prioritized risks based on management decision and risk appetite of the risk owner

**Monitor effectiveness**
Monitor the effectiveness of control implementation and report to management at defined frequency

Integrate with ERM

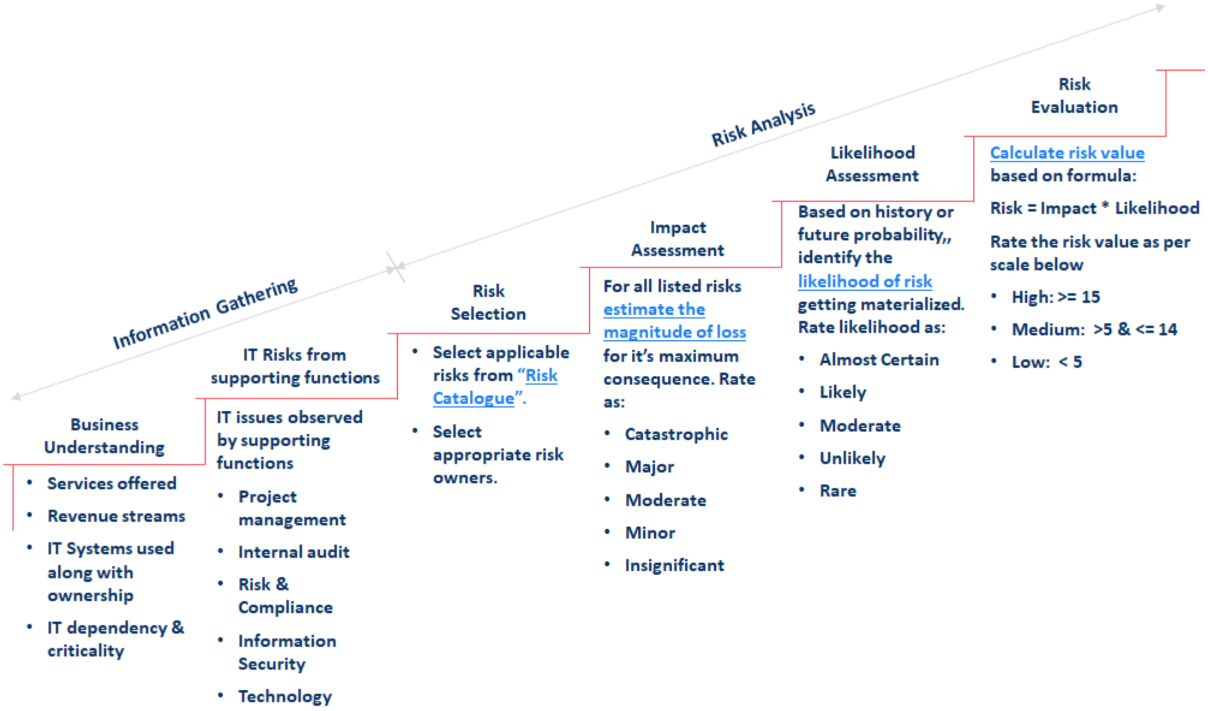
**Principles** of this framework:

- Connect to business objectives
- Align Enterprise IT Risk Management (EITRM) with Enterprise Risk Management (ERM)
- Balance cost / benefit of IT Risk
- Promote fair and open communication
- Establish tone at the top and accountability; and
- Function as part of daily activities

**Note:** While designing this framework, reference has been drawn from ISACA IT Risk Management framework

# 6 Risk Assessment Process

Based on the above EITRM framework, seven (7) step process is followed for identifying & assessing the risks



**Business Understanding**
- Services offered
- Revenue streams
- IT Systems used along with ownership
- IT dependency & criticality

**IT Risks from supporting functions**

**IT issues observed by supporting functions**
- Project management
- Internal audit
- Risk & Compliance
- Information Security
- Technology

**Risk Selection**
- Select applicable risks from "Risk Catalogue".
- Select appropriate risk owners.

**Impact Assessment**
For all listed risks estimate the magnitude of loss for it's maximum consequence. Rate as:
- Catastrophic
- Major
- Moderate
- Minor
- Insignificant

**Likelihood Assessment**
Based on history or future probability,, identify the likelihood of risk getting materialized. Rate likelihood as:
- Almost Certain
- Likely
- Moderate
- Unlikely
- Rare

**Risk Evaluation**
Calculate risk value based on formula:
Risk = Impact * Likelihood
Rate the risk value as per scale below
- High: >= 15
- Medium: >5 & <= 14
- Low: < 5

**Impact Assessment:** For all significant risks identified, loss magnitude is estimated, factoring in maximum business consequence, per the **Impact Guidelines** table below:

| Rating | Critical - 5 | Major - 4 | Moderate - 3 | Minor - 2 | Insignificant - 1 |
|---|---|---|---|---|---|
| Financial | > $5 million | $1 million - $5 million | $50K - $1 million | $10K - 50K | < $10K |
| Operations | Unable to conduct daily operations | Extremely limited daily operations functioning | Partial daily operations functioning | Majority of daily operations functioning | All but one or two daily operations functioning |
| Reputation | Continuous negative international media coverage; significant loss of market share | Continuous negative national media coverage; significant loss of market share | Temporary negative national media coverage | Local reputational damage | Local media attention quickly alleviated |
| Regulatory | Significant prosecution and penalties, litigation including class actions, incarceration of leadership | Report of breach to regulator requiring major corrective action | Report of breach to regulator with immediate correction to be implemented | Reportable incident to regulator, no follow up needed | Non-reportable to regulator |
| Security | No Security for employees, customers and third parties | Security threatened for employees, customers and third parties | Security deteriorating for employees, customers and third parties | Security slightly weakened for employees, customers and third parties | No Security breach for employees, customers and third parties |
| Health & Safety | Significant injuries, fatalities to employees and third parties | Hospital care required for employees and third parties | Out-patient medical treatment required for employees and third parties | Minor injuries to employees and third parties | No injuries to employees and third parties |
| Personnel | Senior leaders exit; mass staff problems; culture altered | Senior staff exit; high turnover; not perceived as employer of choice | Widespread staff morale problems; turnover experienced; shift in culture | General staff morale problems; culture questioned | Isolated staff dissatisfaction; culture remains intact |

**Likelihood assessment:** Based on known history or anticipated probability of risk materializing in future, likelihood of risk is calculated using the **Likelihood Guidelines** table below:

| **Rating** | **Almost Certain -5** | **Likely - 4** | **Moderate - 3** | **Unlikely - 2** | **Rare - 1** |
|---|---|---|---|---|---|
| Probability of Occurrence | The event is expected to occur in most circumstances (>90%). | The event will probably occur in most circumstances (60%-90%). | The event is likely to occur (30%-60%). | More likely not to occur under normal conditions (10%-30%). | The event may occur only in exceptional circumstances (<10%). |
| Historical Trend | Event has occurred in the last 6 months. | Event has occurred in the last 1 year. | Event has occurred in any one of the organizational units over the last 3 years. | Event has occurred in any one of the organizational units over the last 5 years. | Event has not occurred in the past. |
| Existing Controls | No controls in place. | Policies & Procedures in place, but lack of enforcement of controls. | Policies & Procedures in place, with minimal controls in place. | Policies & Procedures in place, controls are monitored & audited. | Very effective Policies & Procedures in place, controls are well monitored & audited. |

In addition, use of Velocity Guidelines is recommended for further prioritization, on need basis.

| **Velocity** | **Value** | **5** | **4** | **3** | **2** | **1** |
|---|---|---|---|---|---|---|
| | **Rating** | Very Rapid | Rapid | Moderate | Slow | Very Slow |
| | **Description** | Impact evident in a month or less | Impact evident in one quarter | Impact evident in 6 months | Impact not evident for more than 1 year | Impact not evident for more than 2 years |

## Risk evaluation

Once the Impact and Likelihood of the Risk is assessed, Risk Value is calculated using the formula:

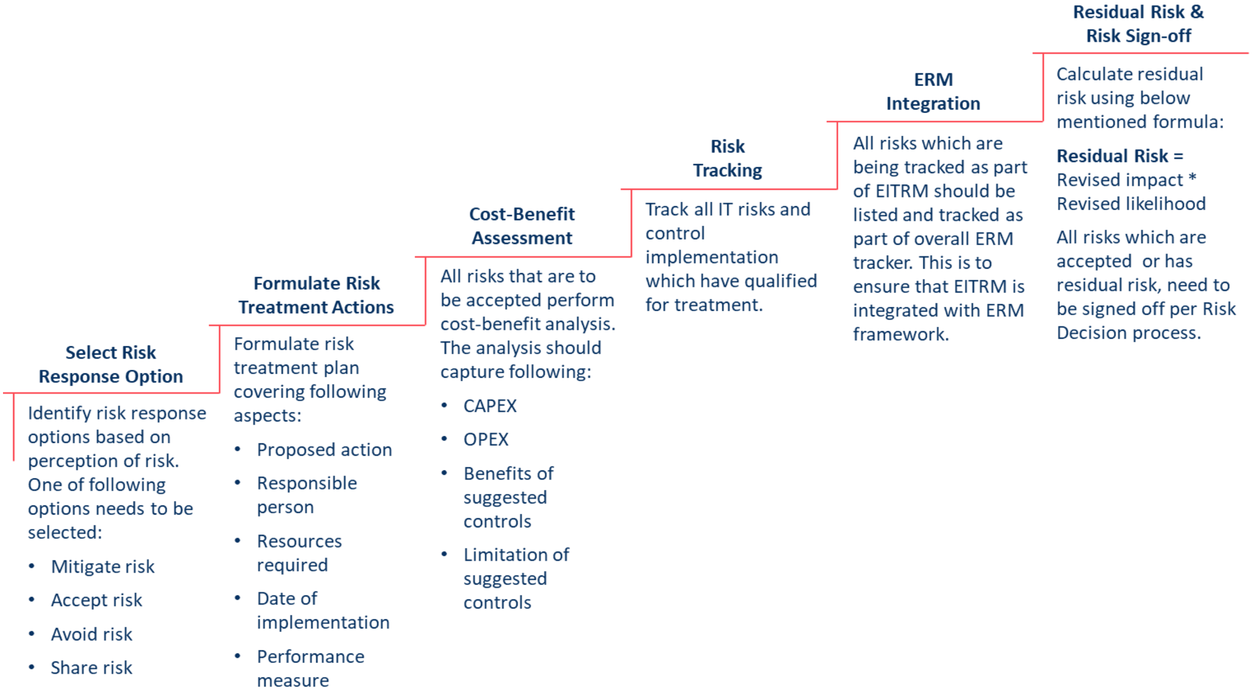
Risk= Impact * Likelihood

| Likelihood | | Insignificant | Minor | Moderate | Major | Catastrophic |
|---|---|---|---|---|---|---|
| 5 | Almost Certain | 5 | 10 | 15 | 20 | 25 |
| 4 | Likely | 4 | 8 | 12 | 16 | 20 |
| 3 | Moderate | 3 | 6 | 9 | 12 | 15 |
| 2 | Unlikely | 2 | 4 | 6 | 8 | 10 |
| 1 | Rare | 1 | 2 | 3 | 4 | 5 |
| | | 1 | 2 | 3 | 4 | 5 |
| | | Impact | | | | |

*more rigorous quantitative assessment of risks can be performed, on need basis, for better risk decisions.

# 7 Risk Response Process:

Steps mentioned below are taken to decide on Risk Mitigation Approach & actual mitigation of the Risk.



**Select Risk Response Option**

Identify risk response options based on perception of risk. One of following options needs to be selected:

- Mitigate risk
- Accept risk
- Avoid risk
- Share risk

**Formulate Risk Treatment Actions**

Formulate risk treatment plan covering following aspects:

- Proposed action
- Responsible person
- Resources required
- Date of implementation
- Performance measure

**Cost-Benefit Assessment**

All risks that are to be accepted perform cost-benefit analysis. The analysis should capture following:

- CAPEX
- OPEX
- Benefits of suggested controls
- Limitation of suggested controls

**Risk Tracking**

Track all IT risks and control implementation which have qualified for treatment.

**ERM Integration**

All risks which are being tracked as part of EITRM should be listed and tracked as part of overall ERM tracker. This is to ensure that EITRM is integrated with ERM framework.

**Residual Risk & Risk Sign-off**

Calculate residual risk using below mentioned formula:

**Residual Risk =** Revised impact * Revised likelihood

All risks which are accepted or has residual risk, need to be signed off per Risk Decision process.

Note: Cost-Benefit Assessment will be conducted upon request of if the risk assessment team deems it necessary

**Risk Response Option:** While IT Tower Leader identifies possible risk response options, Management need to consider cost-benefit analysis before deciding on the Risk Response Option, per below guideline.

| Category | Risk Response | Examples |
|---|---|---|
| Termination/ Avoid | Actions to exit the activity that causes the risk. *For example, risks classified with High Impact as well as High Likelihood could be handled in this manner.* | - Discontinuation of a services<br>- Pull out of market<br>- Redesign |
| Take/ Accept | Take no action to affect likelihood and impact; accept and live with the risk exposure. *For example, risks classified with Low Impact and Low Likelihood could be handled in this manner.* | - Intentionally pursue<br>- Set reward/loss targets and tolerance levels<br>- Establish & Monitor Key Indicators |
| Treat/ Reduce | Actions to reduce the risk exposure by reducing the likelihood, impact or both | - Proactive actions – reduce the likelihood of an adverse outcome<br>- Centralization of activities; Automation of controls |
| Transfer/ Share | Actions to reduce the likelihood or impact by transfer the full or portion of the risk | - Outsourcing<br>- Taking Insurance |

Each risk will have a clearly identified risk owner(s) and will own the responsibility of proposing risk mitigations strategies. These mitigation strategies are reviewed by the IT Leadership on quarterly basis, to ensure timely implementation of the mitigation strategies. Post mitigation, residual risk for significant risks in monitored for a defined period, to ensure the mitigation controls are sustainable.

# 8 Integration with ERM

EITRM's Risk Assessment & Risk Response processes are fully aligned with Genpact's Enterprise Risk Management program, and most significant of IT Risks are made available for ERM to decide on reporting further to Genpact's Risk Council, which reviews Organization's risk profile periodically.

# 9 Annexure

## 9.1 Document Reference List

Please refer to the ISMS Master List of Documents.

## 9.2 Abbreviations

Please refer this Link.