



Enterprise IT Risk Management Process

Version 2.0

Date – 16/04/2021

Document Ownership – Cyber Security Assurance Team



genpact

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 7 th 2018	Updated Risk Category Table – section 6.7	Vinay Bangera	Vinay Bangera	May 7 th 2019
1.2	Feb 27 th 2019	Added Mission statement and updated to reflect govern current process	Vinay Bangera / Shailaja S	Ram Hegde	Feb 27 th 2020
1.3	Feb 18 th 2020	No Change	Vinay Bangera / Shailaja S	Sriram Lakshmanan	Feb 27 th 2021
1.4	02/04/2020	Format updated/aligned as per Document management procedure	Vinay Bangera / Shailaja S	Sriram Lakshmanan	01/04/2021
2.0	16/04/2021	Updated Section 4 as per CRA methodology	Shailaja	Sriram Lakshmanan	15/04/2022



Contents

1	Introduction	4
2	Purpose	4
3	Mission	4
4	Process	4
5	EITRM- Process Framework	5
6	Risk Assessment Process.....	5
7	Risk Response Process:	8
8	Integration with ERM	9
9	Annexure.....	9
9.1	Document Reference List.....	9
9.2	Abbreviations.....	9

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

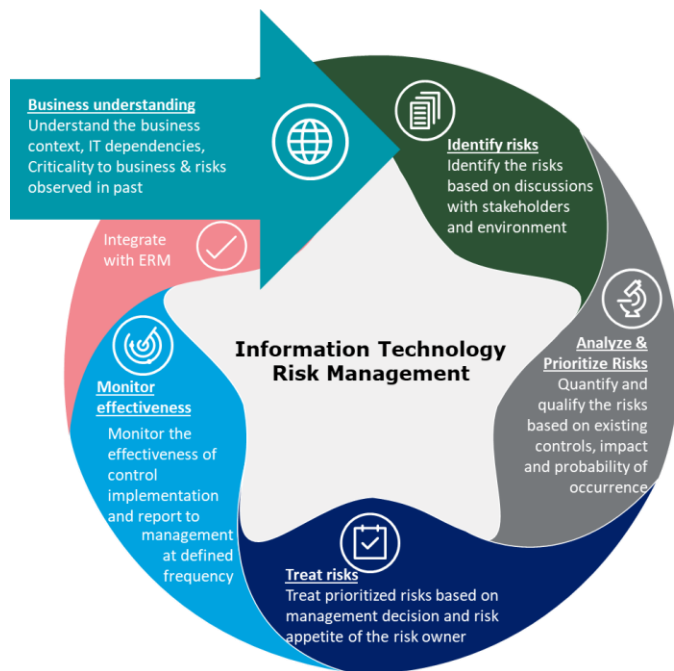
Mission of EITRM program is to "Optimize IT's contribution to Genpact's Business Objectives, by effectively managing key IT Risks"

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 and need-based Risk Assessments to identify, assess and manage key technology and cyber risks faced by organization.
- Identify & analyse key risk indicators from various sources viz major incidents, metrics, internal and external assessments, audit reports, industry research reports, advisories etc., to identify emerging risks.
- Driving prioritization through visibility of IT Risk Universe, to support Risk-Aware decision making.

5 EITRM- Process Framework



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



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:

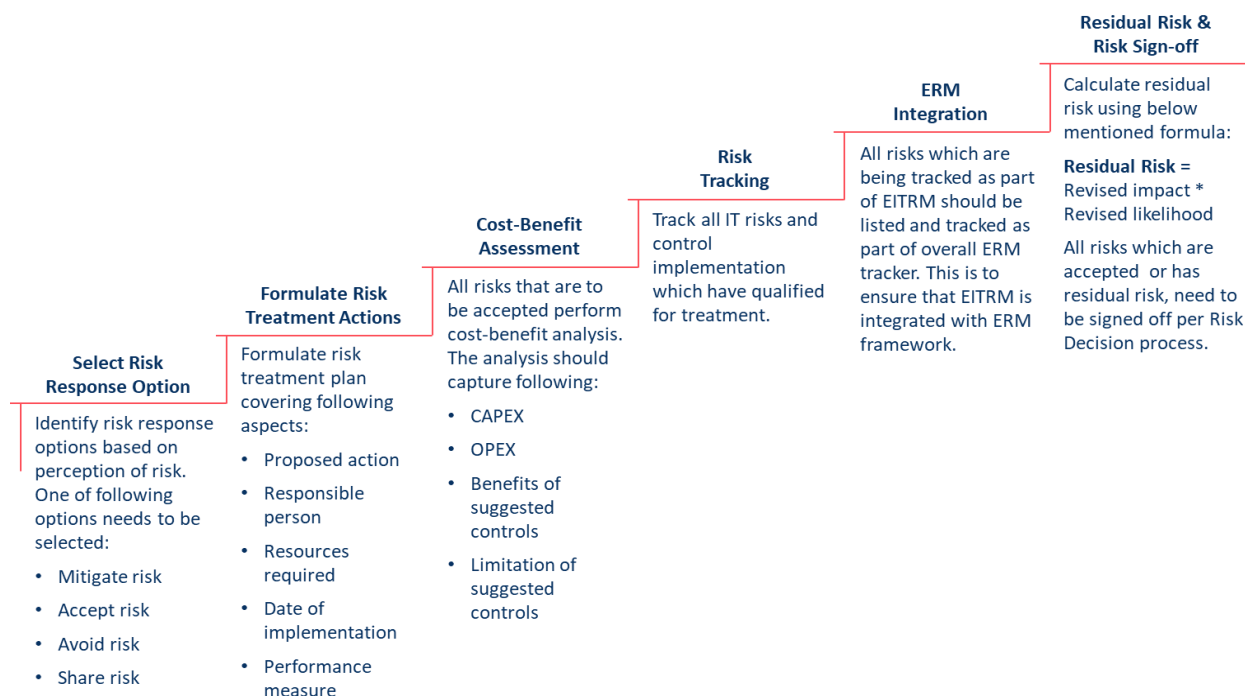
Risk= Impact * Likelihood

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 is 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.



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

Risk Response Option: While respective Tower Leaders decide on appropriate risk response option, 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. <i>For example, risks classified with High Impact as well as High Likelihood could be handled in this manner.</i>	<ul style="list-style-type: none"> ✓ Discontinuation of a services ✓ Pull out of market ✓ Redesign
Take/ Accept	Take no action to affect likelihood and impact; accept and live with the risk exposure. <i>For example, risks classified with Low Impact and Low Likelihood could be handled in this manner.</i>	<ul style="list-style-type: none"> ✓ Intentionally pursue ✓ Set reward/loss targets and tolerance levels ✓ Establish & Monitor Key Indicators
Treat/ Reduce	Actions to reduce the risk exposure by reducing the likelihood, impact or both	<ul style="list-style-type: none"> ✓ Proactive actions – reduce the likelihood of an adverse outcome ✓ Centralization of activities; Automation of controls
Transfer/ Share	Actions to reduce the likelihood or impact by transfer the full or portion of the risk	<ul style="list-style-type: none"> ✓ Outsourcing ✓ Taking Insurance

Each risk will have a clearly identified risk owner(s) who owns the responsibility of proposing risk mitigations strategies. These mitigation strategies are reviewed by the respective tower leaders 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](#).