

# RISK MANAGEMENT PROCESS DOCUMENT

Document Number : CEO PRM 001

Controlled Document Copy No: Original

Created By : E/ IS III


Checked By : ISBQMF

Approved By : ISBQMF

Issue No : 001

Issue Date : 26.04.2018

Issued By : IS & QM Division

 Sri Lanka Telecom PLC	<b>RISK MANAGEMENT PROCESS DOCUMENT</b> Document Number : CEO PRM 001 Internal Use Only	Issue No. 001 Date of Issue : 26.04.2018 Revision No: 001 Date of Revision : 01.07.2021 Page <b>2 of 17</b>
--	---	---

## Document Control Sheet

### Contact for Inquiries & Proposed Changes


Name : Ms. R.A.S.D. Perera      Designation : Engineer/Information Security I  
Telephone : 0112432365      Extension : 1047  
Email : [shakila@slt.com.lk](mailto:shakila@slt.com.lk)      Fax : 0112434758

### Controlled Circulation List

Designation of the Officer	Division	Copy No.
GM/ IS & qm	Information Security	Original
SLT Common Document Portal		Soft Copy


### Enforcement / Revision Table

Issue No. & Date	Revision No. & Date	Page No.	Description of Changes	Prepared/ Updated By	Checked By	Approved By
001 26.04.2018	-	All	New risk management process document for ISBQ common management framework	E/ IS III	ISBQMF	Priyantha Fernandez (ACTO) Kiththi Perera (ACCO)
002 26.04.2018	001 01.07.2021	All	Contact details were updated. SLT logo change was updated. Introduction was updated.	E/ IS I	GM/ IS & QM	GM/ IS & QM

	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page <b>3 of 17</b></p>
---	---	--

## Table of contents

1.	INTRODUCTION.....	4
2.	ESTABLISHING THE CONTEXT .....	5
3.	RISK ASSESSMENT .....	6
4.	TREATMENT OF RISKS .....	12
5.	COMMUNICATION OF RISKS .....	13
6.	MONITORING OF RISKS.....	14
7.	ANNEXURE 1 : FORM FOR ACCEPTANCE OF HIGH RISKS .....	15

	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page <b>4 of 17</b></p>
---	---	--

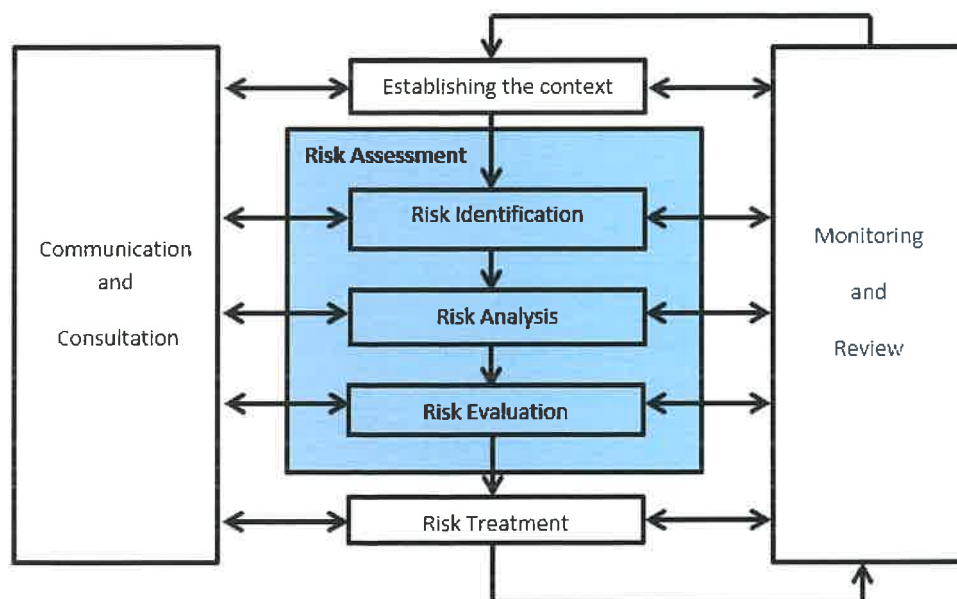
## 1. Introduction

Risk management is the process by which the organization manages risk to acceptable levels within acceptable tolerances, identifies potential risk and its associated impacts, and prioritizes their mitigation based on the organization's business objectives. Risk management develops and deploys internal controls to manage and mitigate risk throughout the organization.


The Risk Management process in SLT is carried out as per the following steps:

1. Establishing the context of the organization
2. Risk Assessment
  - Risk Identification
  - Risk Analysis
  - Risk Evaluation
3. Risk Treatment
4. Communication and Consultation
5. Monitoring and Review

Risk management process is elaborated in Figure 1.



**Figure 1: Risk Management Process**

	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page <b>5 of 17</b></p>
---	---	--

## 2. Establishing the Context


Context on the entity where the risk assessment is carried out is required to be established. Following are required to be considered when establishing the context.

### 2.1. Establishing the external context involves familiarization with the environment in which the organization and the system operates, including:

- Cultural, political, legal, regulatory, financial, economic and competitive environment factors, whether international, national, regional or local.
- key drivers and trends having impact on the objectives of the organization; and
- Perceptions and values of external stakeholders.

### 2.2. Establishing the internal context involves understanding

- capabilities of the organization in terms of resources and knowledge,
- information flows and decision-making processes,
- internal stakeholders,
- objectives and the strategies that are in place to achieve them,
- perceptions, values and culture,
- policies and processes,
- standards and reference models adopted by the organization, and
- Structures (e.g. governance, roles and accountabilities).

	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page <b>6 of 17</b></p>
---	---	--

### 3. Risk Assessment

#### 3.1. Identification of Risk

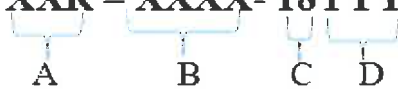
- Risk elements for ISMS should be identified based on the IS objectives
- Risk elements for QMS should be identified based on the quality objectives
- Risk elements for BCM should be identified based on the Business Continuity objectives

#### 3.2. Assignment of Risk ID

In order to maintain a track of all risks that were identified, following notation shall be adopted as the risk ID. This risk ID shall always be referred when communicating the identified risks across the organization.

Following format shall be adopted when assigning a risk ID.

**XXR – XXXX- 18YYY**



**A** – Unique identifier for Risks (shall not be changed)

- Information Security-**IS**
- Business Continuity –**BC**
- Quality Management - **QM**


**B** – Short code assigned to the section. Please refer the business standards issued by the quality assurance division.

**C** – Last two digits of the year the risk is identified.

**D** – 3 digit sequence number from 001 to 999.

#### 3.3. Assign Risk Elements

Risk element is a specific component or a domain that risks are considered. Risk elements support to identify the heat map of risks in each domain. Table 1 shows the risk elements for Information Security, Business Continuity and Quality Management.

 Sri Lanka Telecom PLC	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page 7 of 17</p>
--	---	---

**Table 1: Risk Elements**


Information Security	Business Continuity	Quality Management
Hacking	A/C plant failure in equipment rooms	Business Process
Malware	Single point of failures (eg. No redundancy)	Governance
Cyber Attacks	Prolonged power outages	Infrastructure
Power Failure	Internal IT network or system failure	Obsolete Technology
Insider Threats	Transmission media failure	Employee behavior
Social Engineering	Obsolete Infrastructure	
Legal & Regulatory Compliance	Cyber security	
Security Technologies	Employee unrest	
Governance	Natural disasters	
Competency	Fire	
Aged Systems	A/C plant failure in equipment rooms	
Resources		

### 3.4. Assessment of Risk

Risk analysis process involves

- Evaluating the probability and impact of each risk qualitatively and quantitatively.
- Ranking risks according to their importance

In order to quantify the level of impact and the likelihood of the risks following Scales shall be used;


	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page <b>8 of 17</b></p>
---	---	--

### 3.4.1. Impact

#### Operational

Level	Score	Explanation	
Very High –Significant Devastating	5	Not meeting Quality Specifications resulting suspension of business (with major financial losses), and major fines	Defective quality resulting in critical public or media outcry; International coverage; Boycotts
High-Major Critical	4	Not meeting Product Quality Specification resulting in an investigation (made public) by Government or regulatory body, and major fines	Defective quality resulting in serious public outcry or adverse media publicity
Medium –Moderate Controllable	3	Non meeting Product Quality Specification resulting in an investigation (not made public) by Government or regulatory body, and fines of moderate amount	Service quality resulting in public complaints that needs careful public relations
Low –Minor Irritating	2	Inferior Product Quality resulting in warnings from relevant Authorities, or fines or penalty of minor amounts	Service quality receiving negative public feedback involving authorities that can be resolved
Very Low Negligible	1	Product Quality not meeting desired Specification that can be corrected and resulting in minor consequences	Service quality receiving public complaints that can be corrected



 Sri Lanka Telecom PLC	<b>RISK MANAGEMENT PROCESS DOCUMENT</b> Document Number : CEO PRM 001 Internal Use Only	Issue No. 001 Date of Issue : 26.04.2018 Revision No: 001 Date of Revision : 01.07.2021 Page 9 of 17
--	---	--


## Financial

Level	Score	Explanation
Very High –Significant Devastating	5	Rs500 mil > 50% of the preceding year's NPAT
High-Major Critical	4	Rs100 mil to Rs500 mil > 20% < 50% of the preceding year's NPAT
Medium –Moderate Controllable	3	Rs10 mil to Rs100 mil > 5% < 20% of preceding year's NPAT
Low –Minor Irritating	2	Rs1 mil to Rs10 mil > 1% < 5% of preceding year's NPAT
Very Low Negligible	1	Less than Rs1mil <1% of the preceding year's NPAT

## Compliance

Level	Score	Explanation
Very High –Significant Devastating	5	Noncompliance resulting in public censure, suspension of business (with major financial losses), and major fines
High-Major Critical	4	Noncompliance resulting in an investigation (made public) by Government or regulatory body, and major fines
Medium –Moderate Controllable	3	Noncompliance resulting in an investigation (not made public) by Government or regulatory body, and fines of moderate amount
Low –Minor Irritating	2	Noncompliance resulting in fines or penalty of minor amounts
Very Low Negligible	1	Recommendations from relevant Authorities

Consider the maximum impact value which are measurable and affect ISMS, BCMS and QMS objectives operationally, financially and compliance.

	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page <b>10 of 17</b></p>
---	---	---

### Probability

Level	Score	Explanation
Almost Certain	5	Event will occur in most circumstances and is a persistent issue (>95%) (It will occur almost daily)
Probable	4	Event is likely to occur but is not a persistent issue (50%-95%) (2days to 1 month)
Possible	3	Event may occur occasionally (20%-49%) (1 month to 1 year)
Unlikely	2	Event could occur at some time, but the chance is very small (6%-19%) (1 year to 5 years)
Rare	1	Event may occur only in exceptional circumstances (<6%) (More than 5 years)

### 3.5. Risk Evaluation

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment.

A risk impact rating shall be calculated in order to prioritize the risks. Following formula shall be used to calculate the risk impact rating (RIR);

$$\text{Risk Impact Rating (RIR)} = \text{Risk Impact} * \text{Probability of Occurrence}$$


The highest Risk Impact Rating on this basis is therefore 25 (5\*5), with the lowest possible Risk Impact Rating being 1 (1\*1).

The Risk impact rating helps to prioritize the risk into three different levels:

**High**, where the RIR ranges from 12-25 (i.e.  $12 \leq \text{RIR} \leq 25$ )

**Medium**, where the RIR ranges 6 - 10 (i.e.  $6 \leq \text{RIR} \leq 10$ )

**Low**, where the RIR ranges from 1- 5 (i.e.  $1 \leq \text{RIR} \leq 5$ )

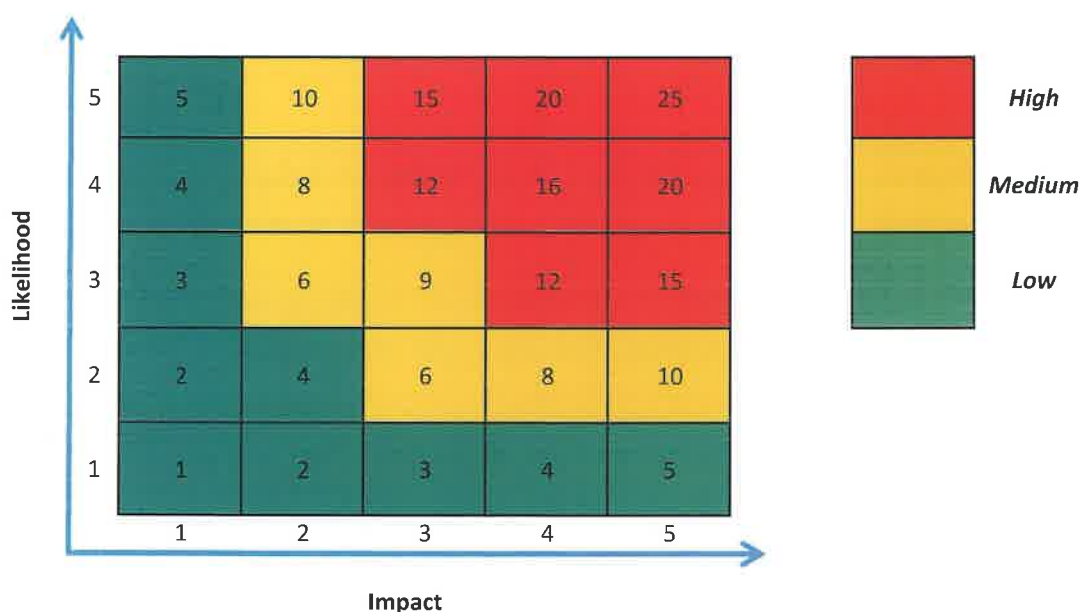
 Sri Lanka Telecom PLC	<b>RISK MANAGEMENT PROCESS DOCUMENT</b> Document Number : CEO PRM 001 Internal Use Only	Issue No. 001 Date of Issue : 26.04.2018 Revision No: 001 Date of Revision : 01.07.2021 Page 11 of 17
--	---	---

### Acceptable Level of Risk:

Any Risk Impact Rating **greater than or equal to 12** shall be considered for risk treatment.

Thus, a RIR value of **10** or below will be considered as acceptable risk and no additional controls will have to be applied.

### Prioritization of Risks




### 3.6. Accountability

A risk owner shall be assigned for each risk identified. . The Deputy General Manager of the section or a higher officer as applicable shall be assigned as the risk owner for all groups except CRO and CSO groups.

Risk owner for CRO Group-OPMC Manager, Network engineer, regional accountant

Risk owner for CSO Group – RTOM , DGM/Sales

It is required to ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls.

	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page <b>12 of 17</b></p>
---	---	---

### 3.7. Roles and responsibilities of Risk Owner

Risk Owner is the entity with the accountability to manage a risk.


Risk owner shall provide approval for risk treatment plan and the acceptance of residual risk, which is explained under section 5.

Risk owner is also responsible for monitoring risks assigned to him/her.

## 4. Treatment of Risks

All risk items above the acceptable level of risk are chosen for risk treatment. These items can either be,

- **Terminated** – In this case sources of risk are removed or replaced. Activities may need to be modified or processes reengineered that can serve to mitigate or manage risks to acceptable levels.
- **Treated** – Controls are implemented to reduce the level of risk
- **Transferred** – The liability is transferred to an external entity through an agreement. An insurance policy is one such example. While the possible financial impacts associated with the risk can be transferred, the legal responsibility for the consequences of compromise cannot be transferred.
- **Tolerated** – The management decides that it is ready to accept that risk, because of business limitations. They might address the issue when appropriate resources are available. This shall be performed as per the risk acceptance framework established under section 6.

	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page 13 of 17</p>
---	---	--

## 5. Communication of Risks

### a. Escalation of Risks

Sectional ISBQ Teams are responsible for ensuring that all applicable information security, business continuity and quality risks for their section are identified and appropriately assessed.

Residual risks that are identified as high during the risk assessments in the sections shall be escalated to the ISBQ management forum with the consent of respective ISBQ steering committee with identified mitigation strategies and predicted cost and resource requirements if applicable.


ISBQ management forum shall provide approval for the risk mitigation strategy proposed. ISBQ management forum shall escalate the risks to enterprise risk management process if required.

All risks above the acceptable level shall be communicated to General Manager/Information Security & Quality Management once in Three months by the respective ISBQ team.

It is essential that the communication of risks shall always refer the assigned risk ID.


### b. Notification of Risks

Risks that will impact quality, Information Security, Business continuity shall be assessed by the project manager before handing over to the operation. Any risks that may affect the operational activities during the implementation stages and after handing over the project to corresponding operational section shall be communicated to the relevant DGM of the section. It is the responsibility of the DGM to assess the risks within the IBQ team.

	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page <b>14 of 17</b></p>
---	---	---

## 6. Monitoring of Risks


- 6.1.** Risk assessments conducted shall be reviewed at least once a year or whenever following changes occur;
- A change in the operational process
  - A change in the technologies used
  - A change in internal/external context
  - Any other change that affects the operations
- 6.2.** Risk assessment sheets shall represent the up-to-date risk profile of the entity at the time of review. Hence all risks including terminated risks which were assessed during the present assessment cycle shall be indicated in the sheets. All risks which were terminated during the previous assessment cycle shall be removed from the sheets and a record shall be maintained on all such terminated risks and applied controls.
- 6.3.** Risk owner shall evaluate the effectiveness of actions taken for the risks those are not terminated at least once in 3 months.

 Sri Lanka Telecom PLC	<b>RISK MANAGEMENT PROCESS DOCUMENT</b> Document Number : CEO PRM 001 Internal Use Only	Issue No. 001 Date of Issue : 26.04.2018 Revision No: 001 Date of Revision : 01.07.2021 Page <b>15 of 17</b>
--	---	--

## ANNEXURE 1: Form for Acceptance of High Risks

Form for acceptance of high risks					
To be filled by the Risk Owner					
Section:					
Risk ID:					
Risk Description:					
Sources and causes of risks:					
Existing controls:					
Risk Impact:					
Likelihood:					
Risk Impact Rating:					
Risk Owner:					
Risk Element:					
Reason for accepting risks:					
Plan for the minimize the impact:					
Signature & Rubber stamp of risk owner:			Designation:		Date:



	<p align="center"><b>RISK MANAGEMENT PROCESS DOCUMENT</b></p> <p align="center">Document Number : CEO PRM 001</p> <p align="center">Internal Use Only</p>	<p>Issue No. 001</p> <p>Date of Issue : 26.04.2018</p> <p>Revision No: 001</p> <p>Date of Revision : 01.07.2021</p> <p>Page 16 of 17</p>
---	---	--

**To be filled by Chairman of respective ISBQ Steering Committee**

Note: If a group does not have a ISBQ Steering committee in group, this should be filled by respective Chief Officer of the relevant group

Recommended/not recommended due to following reasons:

**Chairman of  
ISBQ Steering  
Committee/Chief  
Officer:**

**Signature &  
Rubber  
stamp:**

**Date:**

**To be filled by Chairman of ISBQ Management Forum**

Approved/not approved due to following reasons:

**Chairman of  
ISBQ  
Management  
Forum:**

**Signature  
& Rubber  
stamp:**

**Date:**

**Next review  
date:**

Within a period of 06 months from the approval of risk