RISK MANAGEMENT (TIER 2)

1. Scope

This applies to the risk management framework in MBP Pvt Ltd and will be conducted in line with MSS DOC 4.1 and DOC 4.2.

2. Responsibilities

2.1 The Chief Information Security Officer is responsible for identifying management system risks, and for the development, testing and maintenance of plans to manage those risks.

2.2 The Chief Information Security Officer (CISO) is responsible for managing business continuity on a day-to-day basis, and is also responsible for carrying out the risk assessments relevant to business continuity.

2.3 The Chief Information Security Officer is responsible for ensuring that all information security issues have been included and appropriately treated under this risk management framework.

2.4 The Chief Information Security Officer is responsible for ensuring that all quality management issues have been included and appropriately treated under this risk management framework.

2.5 Manager/Executive responsible for (owners of) key processes are also responsible for implementing controls relating to those processes as determined in the risk assessment.

3. Risk management

3.1 Risk management is conducted within the internal and external context of MBP Pvt Ltd.

3.2 Risk management takes MBP Pvt Ltd's legal and regulatory requirements into account.

3.3 Chief Information Security Officer defines risk criteria accordingly:

3.3.1 Definition – most commonly, this is as a combination of likelihood and impact, but may take into account characteristics relevant to your business.
ISO 31000 suggests taking into account the following:
the nature and types of causes and consequences that can occur and how they will be measured;
how likelihood will be defined;
the timeframe(s) of the likelihood and/or consequence(s);
how the level of risk is to be determined;
the views of stakeholders;
the level at which risk becomes acceptable or tolerable; and
whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.]

3.3.2 Chief Information Security Officer determines risk acceptance criteria as appropriate to the management systems.

3.4 The risk assessor for the management system identifies risks to its management systems.

3.5 The risk assessor for the management system analyses the risks to determine their relation to the risk criteria, including their likelihood and impact.

3.6 The risk assessor for the management system evaluates the risks by comparing the level of risk identified in 3.5 above to the risk criteria established in 3.3.

3.7 The risk assessor for the management system determines risk treatments:

RISK MANAGEMENT (TIER 2)

3.7.1 Treatments are selected by agreement with the appropriate process, risk or asset owner.

3.7.2 Risk treatment options are as follows:

3.7.2.1 Eliminate the risk by removing the activity affected by the risk

3.7.2.2 Accepting the risk to pursue an opportunity

3.7.2.3 Removing the source of the risk

3.7.2.4 Changing the likelihood of the risk coming to pass

3.7.2.5 Changing the consequences of the risk coming to pass

3.7.2.6 Sharing the risk with another party or parties (such as via suppliers, insurance or other third parties)

3.7.2.7 Accepting the risk by informed decision

3.8 The risk assessor creates a risk treatment plan providing the following information:

3.8.1 The reasons for selected treatments, including expected benefits

3.8.2 Those responsible for approving the risk treatment plan

3.8.3 Those responsible for implementing the risk treatment plan

3.8.4 Proposed actions

3.8.5 Resource requirements and contingencies

3.8.6 Treatment performance measures and limitations

3.8.7 Requirements for reporting and monitoring

3.8.8 Timing and schedule for the risk treatment

3.9 The risk treatment plan is agreed with the appropriate stakeholders.

3.10 The risk treatment plan is implemented in accordance with MBP Pvt Ltd’s processes and the risk treatment plan itself.

Document Owner and Approval

The Chief Information Security Officer is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

The current version of this document is available to [all/specified] members of staff on the [corporate intranet] and is published [describe other/hardcopy availability].

This document is approved by the *Management System Owner (MSO)*.

Signature: Date:

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Zamir Shaikh	24th July 2024