Enterprise Risk Management Framework

20th ACG Cross Border Training Program
Shanghai - China

Wamiq Ahmed
Central Depository Company of Pakistan Limited
Risk & Recovery Management Task Force – ACG 20 – May 10-11, 2018

CENTRAL DEPOSITORY COMPANY

Contents

Definition & Requirement

"Risk Management is the culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects."

"10(2)The board of directors is responsible for the governance of risk and for determining the company's level of risk tolerance by establishing risk management policies. The board shall undertake at least annually, an overall review of business risks to ensure that the management maintains a sound system of risk identification, risk management and related systemic and internal controls to safeguard assets, resources, reputation and interest of the Company and shareholders"

Listed Companies Code of Corporate Governance Regulations 2017

ERM Framework of CSD – Current Status

- Currently, risks are managed in silos within Central Depository Company of Pakistan Limited(CDCPL). We have developed risk registers for all services and departments, wherein we have identified and assessed risks along with mitigation controls. Risk registers are maintained by respective Head of Department as a risk owner.

- In order to streamline risk management in CDC, we are in the process of implementing Enterprise Risk Management (ERM) framework.

- Risk Management Committee (RMC) at management level has been formed to ensure that the Company has clear, comprehensive and well documented Enterprise Wide Risk Management Framework for the management of all major risks faced by the Company and risk management framework is adequate to support overall Company's objective.

- Risk & Regulatory Affairs Committee (RRAC) at Board level has also been formed to oversee the Company’s risk management function including strategy formulation, risk governance and performance reviews.

- Risk Management team has been hired and trained. The Enterprise Risk Management (ERM) framework has been designed and is in implementation phase.

ERM Broad Governance Framework

Boards (Oversight through RRAC)	1st line of defense: Business Units (Originate and manage risk)	2nd line of defense: Risk Management Lead by Chief Compliance & Risk Officer (CCRO) (To Design, interpret, monitor & report)	3rd line of defense: Internal Audit (Test & verify)
"Tone set from the top" • Approve ERM framework • Review Risk Reports and provide guidance on critical issues in the reports.	"Primary Risk Owner" • Identify, Assess, report and recommend mitigations on risks in their units.	• Interprets regulations/ leading policies • Develop & Implement the ERM Framework • Monitors risk appetite & tolerance limits & reports critical risks to the RRAC.	• Provide assurance that ERM framework is appropriate and functioning.

Risk Appetite Statement

- **Level 1 Risks**

Risks which are unacceptable under any circumstances and the Overall Threat Likelihood of risk is not "Unlikely or below". For example

1. Intentionally breaching of one or more laws or regulations;
2. Intentionally providing incorrect information to regulators or law enforcement agencies etc.

- **Level 2 Risks**

Risks which are avoidable under all circumstances and the Overall Threat Likelihood of risk is not "Likely or above" and the company has resources to mitigate the risks and controls are justified based on costs and benefits. For example

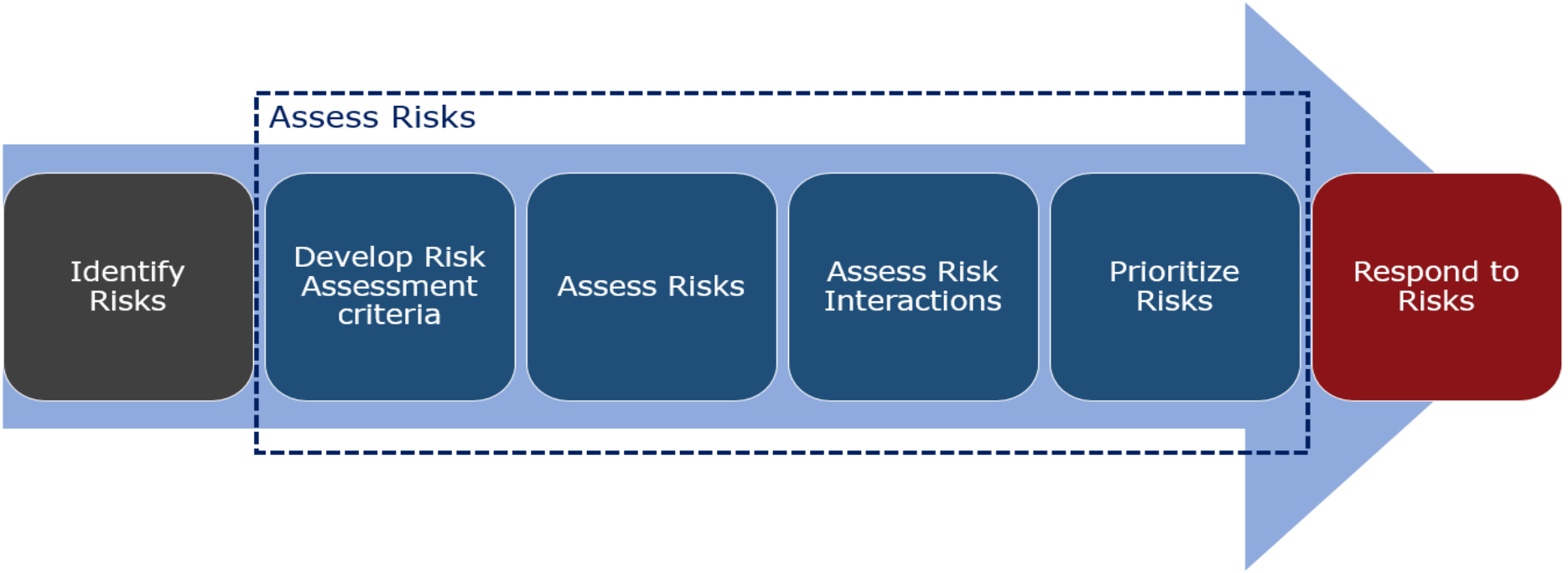
1. The risk may result in the Company unintentionally sharing information (e.g. about customers, employees, suppliers) with inappropriate individuals or external organizations;
2. The risk may result in the Company unintentionally breaching its contractual obligations to third parties etc.

- **Level 3 Risks**

Risks which are avoidable under all circumstances and the Overall Threat Likelihood of risk is "below Likely" and the company has resources to mitigate the risks and controls are justified based on costs and benefits. In this level, the company will define risk tolerance level against each identified risk and the same shall be monitored for breaches and overall changes in threat likelihood level to likely or above.

Risk Management Methodology

- **Risk Management Process**



Risk Management Methodology - Identification

In CDCPL, the following risk (or event) identification tools shall be used to identify risks to the objectives and targets:

- Risk Maturity Assessment Review;
- Risk Review Workshops with Business Units;
- Risk & Control Self-Assessment (RCSA);
- Review of Processes & Systems including sanctioning process;
- Risk Events Database Review;
- Security Incident Reports;
- Enterprise Annual Risk Review;
- Internal & External Audit Reports;
- Internal & External Regulatory Compliance Audit Reports;
- Review of External Business Environment including industry analysis.

As a result, a comprehensive list of risks will be developed and documented in respective business unit/department risk registers for assessment, risk treatment and reporting.

Risk Management Methodology – Assessment Criteria

- **Likelihood**

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may occur within the construct of the associated threat environment, the following governing factors must be considered:

  - Threat-source motivation and capability
  - Nature of the vulnerability

The likelihood that a potential vulnerability could occur due to a given threat-source can be described as Almost certain, Likely, Possible, Unlikely or Rare. The Table below describes these five likelihood levels.

Table 1 - Qualitative Measure of Consequences of Likelihood

Level	Descriptor	Description	Frequency
A	Almost certain	Is expected to occur in most circumstances.	More than once per year
B	Likely	Will probably occur in most circumstances.	1 in 1 - 3 years
C	Possible	Might occur at some time.	1 in 3 - 5 years
D	Unlikely	Could occur at some time.	1 in 5 - 10 years
E	Rare	May occur in exceptional circumstances.	1 in 10 years

Risk Management Methodology – Assessment Criteria

- **Impact**

An event can lead to range of impacts which may be certain or uncertain. It is important to recognize that there may be a number of direct and indirect impacts arising from any risk event. The level of loss associated with each risk event must then be determined within all relevant contexts, as follows:

Table 2 - Qualitative Measure as Consequences or Impact

Level	Description	Examples of description
1	Insignificant	No injuries, low financial loss, no risk to reputation, no legal obligations.
2	Minor	Minor First aid treatment, on-site release immediately contained, medium financial loss, some customer dissatisfaction and may lead to legal obligations
3	Moderate	Medical treatment required, on-site release contained with outside assistance, high financial loss/obligations, public visibility and threat to reputations.
4	Major	Major Extensive injuries, loss of operating capability, invocation of disaster recovery with no detrimental effects, major financial loss/obligations, leads to regulatory penalty.
5	Catastrophic	Death, off-site with detrimental effect, huge financial loss/obligations, huge financial penalty may imposed.

Risk Management Methodology – Assessment Criteria

- **Impact**

Table 3 - Quantitative Measure as Consequences or Impact		
Level	**Description**	**Example of description**
1	Insignificant	Nil – Negligible
2	Minor	Under 500K
3	Moderate	Between 500K - 5m
4	Major	Between 5m - 20m
5	Catastrophic	Above 20m

Risk Management Methodology – Prioritize Risk

- Once the risks have been assessed and their interactions documented, it's time to view the risks as a comprehensive portfolio to move on to the next step – prioritizing for risk response and reporting to different stakeholders.
- In CDCPL, all identified risks are prioritized and treated as per the following management responses:

(Risk Rating Matrix)

Table 4 - Overall Risk Rating Matrix

	Consequences				
	Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood:	**1**	**2**	**3**	**4**	**5**
A (almost certain)	**H**	**H**	**E**	**E**	**E**
B (likely)	**M**	**H**	**H**	**E**	**E**
C (possible)	**L**	**M**	**H**	**E**	**E**
D (unlikely)	**L**	**L**	**M**	**H**	**E**
E (rare)	**L**	**L**	**M**	**H**	**H**

Risk Management Methodology – Management Response

- **Management Response to the Assessed Risks**

Key	Description
E	Extreme Risk: Immediate action required to mitigate the risk.
H	High Risk: Action should be taken to compensate for the risk.
M	Moderate Risk: Action should be taken to monitor the risk.
L	Low Risk: Routine acceptance of the risk.

Risk Monitoring and Reporting

- Management uses relevant information from both internal and external sources to support enterprise risk management. The following reports shall be prepared and shared with the Management and Board's Risk & Regulatory Affairs Committee (RRAC) to ensure that ERM framework is functioning effectively and make informed decisions where necessary.

Report name	Report frequency	Prepared by	Reviewed & Agreed by	Reported to	Reported to RRAC
Portfolio view of risks (Dashboard) at Entity Level	Annually	Risk Management Team	Chief Compliance & Risk Officer	RMC	Annual
Portfolio view of risks (Dashboard) at Business Unit & Department Level	Quarterly of the selected department	Risk Management Team	Chief Compliance & Risk Officer	RMC	Quarterly
Incident/Risk events report	As & when required	Risk Owner Department	Risk Management Team	Chief Compliance & Risk Officer	Quarterly
Breaches of Risk appetite & tolerance limit	Annually	Risk Management & Risk Owners	Risk Owner and Chief Compliance & Risk Officer	RMC	Annually

Risk Monitoring and Reporting

Report name	Report frequency	Prepared by	Reviewed & Agreed by	Reported to	Reported to RRAC
Risk identification & Assessment	At the start of the risk management program. Then quarterly for selected departments	Risk Management Team	Risk Owner and Chief Compliance & Risk Officer	RMC	Quarterly – New emerging risks and modifications/ changes in identified Risks profile only of the selected departments.
Trends in Key Risk Indicators	Annually	Risk Owners	Chief Compliance & Risk Officer	RMC	Annually
Operational Risk Score card	Annual	Risk Management	Chief Compliance & Risk Officer	RMC	-
Operational Loss data	Annual	Risk Management	Chief Compliance & Risk Officer	RMC	-

Thank You!