

## **ENTERPRISE-WIDE RISK MANAGEMENT**

Cardno adopts an enterprise-wide risk management approach to the management of risk and as part of that approach has identified its most significant risks.

The Operational Risk Management Committee (ORMC) has the responsibility for the oversight of the maintenance of the company's operational risk management plan. This provides the framework for monitoring risk management activities. The plan follows AS/NZS4360:2004 and includes the following elements:

- Identification of possible risks;
- Measurement of risk by analysis in terms of probability and impact in the context of current controls and strategies;
- Evaluation and prioritisation of risks;
- Development and implementation of risk control strategies; and
- Monitoring and reviewing the effectiveness of the risk management system.

## **MEMBERSHIP**

The ORMC consists of the Managing Director (Chair), the CFO, General Manager (GM) Operations, Regional General Managers, Division Manager (DM), DM International, DM Cardno Bowler and the Risk Administrator.

The ORMC reports to the Managing Director and to the Cardno Board's Audit, Risk & Compliance Committee (ARCC).

## **OPERATIONAL RISK MANAGEMENT COMMITTEE RESPONSIBILITIES**

The ORMC has been established to oversee and ensure the efficient and effective management of Cardno's significant operational risks.

The ORMC is charged with the responsibility of establishing, maintaining and reviewing procedures at management and operational level to identify, monitor and mitigate operational risk in accordance with the company's risk oversight and management policies. It is responsible for checking that those procedures are designed to maintain the company's operational viability and to safeguard its assets and interests.

The ORMC's core responsibilities are to:

- Advocate, implement, maintain and review Cardno's enterprise-wide risk management framework, as advocated by the Audit, Risk & Compliance Committee (ARCC) within which Cardno's teams assume operational responsibility for managing operational risk in the performance of their respective functions;
- Regularly monitor and assess Cardno's organisation-wide risk profile and exposure to significant risks;
- Provide an oversight role:
  - For the maintenance of the Risk Registers for the organisation;
  - To ensure that employees undergo appropriate risk management training and maintain these skills;
  - For the management of operational risks directly under the ORMCs control; and
  - To ensure risk management is included within the planning process for all activities including projects by linkage with objectives to develop controls and strategies.

- Consider incident reporting as it pertains to operational issues directly under their responsibility.
- Review and input into risk identification activities.
- Receive and review regular reports against the severe and major risks in each division from the various Regional Risk Committees.
- Report to the ARCC on a quarterly basis a summarised account of Cardno's risk management activities including:
  - Commentary on significant residual risks (for ARCC consideration);
  - Update on consolidated issues register, including number of new issues, closed issues, and general implementation status of key actions
  - Significant control exposures / incidents / compliance breaches / potential fraud or malpractice; and
  - Progress against control implementation plans and any re-estimate of implementation timelines.
- Monitor and assess the adequacy of risk management policies and procedures through the review of the reports about the significant risks;
- Recommend to the ARCC policies for the management of significant risks affecting Cardno;
- Recommend to the Managing Director for approval, procedure for the management of the significant risks affecting Cardno;
- Review and improve internal processes for determining, monitoring and assessing significant operational risk areas; and
- Act as a forum for the discussion of significant operational risk issues. This process forms part of the governance process that ensures that Cardno's risk management function operates effectively, efficiently and economically.

In the discharge of the above mentioned responsibilities, the ORMC will report promptly to the ARCC where issues are identified that could present a material risk or threat to Cardno.

## **RISK MANAGEMENT SYSTEM**

Within each area of operational risk, the ORMC has the responsibility for determining the severity of the operational risks identified and evaluating each risk in terms of:

- the probability of its occurring; and
- the impact of the risk occurring.

From this evaluation, the ORMC rates the severity of each risk ranging from "severe" to "negligible" and reviews whether appropriate risk management policies, procedures and mitigation controls are in place which is commensurate with the assessed severity. The ORMC also reviews the effectiveness of those policies, procedures and mitigation controls and, where necessary, develops and implements new policies, procedures and mitigation controls.

## **REGIONAL RISK COMMITTEES**

Each region will form their own risk committee and report to the ORMC on a quarterly basis on their significant risks and annually on the full risk matrix. It is expected that each region will incorporate divisional risk committees to ensure the risk process is developed throughout the organisation.

The structure of the ORMC and the regional risk committees is attached.

## ORMC MEETINGS

### *Frequency*

The various risk committees will meet quarterly ensuring the meetings coincide with a two week period prior to the quarterly ARCC meetings. In addition, the Committee chairperson may call such additional meeting as may be necessary to address any matters referred to the ORMC or in respect of matters that the team wishes to pursue.

### *Minutes*

Minutes of meetings must be prepared and distributed to ORMC members as soon as possible after the conclusion of the meeting and, subject to any agreed amendments, shall be confirmed as an accurate record of the meeting at the next subsequent meeting of the ORMC.

### *Other attendees*

The ORMC chairperson may request a Cardno officer, internal auditors or other external parties to attend a meeting of the ORMC. Further the chairperson may invite a representative of external audit to attend any meeting of the ORMC and to present and comment on appropriate agenda items.

### *Agenda*

A common meeting agenda will be used by the ORMC and the regional risk committees. The common agenda will be structured around the key risk categories and the significant risks for each region will be reported on quarterly. In the setting of an agenda there will be an emphasis on the most significant risks and threats to Cardno and the ongoing evaluation of what is being done to mitigate such risks.

## RISK CATEGORIES AND AREAS

The Committee has identified nine key areas which are used to guide discussion and focus on risk identification as follows:

- Financial Risk
- Commercial Risk
- Business Process Risk
- Human Resources Risk
- Information Risk
- Property Risk
- Environmental Risk
- Health and Safety Risk
- Insurable Risk
- Other

These key areas form the basis of the organisations consequence table as included in Attachment 1. In conjunction with these areas of risk focus, the organisation has established the likelihood parameters also included in Attachment 1.

## BOARD RESPONSIBILITY

The Committee notes that the Cardno Board and specifically the Board's Audit, Risk and Compliance Committee, in consultation with executive management, is also responsible for identifying relevant risks and notifying the ORMC. The ORMC shall then consider the appropriate control procedures needed to adequately manage the risks and report to the ARCC as to what those procedures will be.