4.2 Establishing reporting mechanisms

An organization should ensure that information about risks derived from the risk management process is adequately reported, and used as a basis for decision making at all relevant levels. For this, clear reporting line mechanisms and strong inter-department knowledge sharing should be established in order to encourage accountability of risk, and to ensure reports are delivered in an accurate, consistent and timely manner. Moreover, the risk management policy (see Ch. 1) should clearly state the way risk management performance will be reported.

Inadequate risk reporting can lead to a failure to fully integrate identified risks into strategic and operational decisions. The organization should report on progress against the risk management plan by proving how well the risk management policy is being followed, to ensure that risk management is effective and continues to support organizational performance. More specifically:

1. The results from risk monitoring and review should be recorded and reported internally and externally, if appropriate;
2. Development in implementation of risk treatment plans should be incorporated into the organization’s overall performance management, measurement and internal and external reporting activities, as a performance measure;
3. Enhanced risk management includes continual communications with external and internal stakeholders (see Section 2, Ch. 1), including comprehensive and frequent reporting of risk management performance, as a part of good governance.

The quality and success of risk reporting depends on the following factors:

- Target audience;
- Input and processes;
- Frequency;
- Content;
- Format;
- Dissemination channels.

Determining the target audience is important because it affects other risk reporting decisions. Whenever a disclosure is demanded by a regulatory requirement, the organization must comply and provide appropriate disclosure. On the other hand, voluntary disclosures should be subject to cost-benefit analysis of audiences’ needs and the kind of disclosure (type and detail of risk). Reporting organizational risks should operate on multiple levels to address the needs of diverse audiences, each with their own specific needs, requirements, expectations, agendas and levels of expertise. In this regard, there are two areas of risk reporting:

a) Reporting to internal audiences.

b) Reporting to external audiences.

The reporting of risks is essential for internal decision makers to integrate risk evaluation into their operational and investment strategy, to review performance, and to review compensation/reward decisions. External risk reporting has rapidly developed in recent years: corporate governance reports also focus attention on internal control, and a review of risks is generally included in the annual reports. Both internal and external audiences can be further divided into two subgroups: on the one hand, some audiences (i.e., boards of directors and regulators, among external audiences) must be informed about the organizational risks and risk management processes because of regulation or recommendations. Voluntary disclosure to other internal audiences (i.e., employees) and external stakeholders (i.e., media, citizens’ associations) is recommended because of anticipated benefits to an improved decision-making.

‘Inputs’ and ‘processes’ are also critical. The most important inputs are represented by:

I. The various risks an organization is facing;
II. The stakeholder risk reporting requirements and expectations;
III. The organization’s existing risk management governance, that provides the context for establishing risk reporting processes;
IV. The organizational resources (such as individuals with the necessary skills and experience, financial resources, and access to required information).

Decision must be taken on which risks to report, in what detail, and with what reporting frequency.

a) Internal reporting
The organization should establish internal reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that: key components of the risk management framework; its effectiveness and the outcomes and any subsequent modifications, are properly disseminated; relevant information derived from the application of risk management is available at appropriate levels and times; there are processes for consultation with internal stakeholders (see Section 2, Ch. 1). These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information. Internal risk reports can either be real-time or periodic.

The main purpose of periodic internal risk reports is to provide aggregate information about various relevant organizational risks, with trend indicators and periodic comparisons highlighting changes in risks. Periodic internal risk reporting contributes to strategic oversight and decision-making, as well as improved operational business decisions. Risk information may be organized around specific key risk categories rather than around phases of the risk management process. Residual risk reporting involves comparing gross risk (the assessment of risk before controls or risk responses are applied) and net risk (the assessment of risk, taking into account any controls or risk responses applied) to enable a review of risk response effectiveness and alternative management options. Risk reporting to the board and committees should be made at least quarterly.

Internal audiences will not only be interested in disclosure of specific risks, but also in the risk management process. A well established and properly managed process will assure internal audiences about the reliability of risk reports: organizations must therefore include information on the quality of their risk management process, particularly in their periodic risk reports.

Comprehensive and frequent internal reporting on significant risks and risk management performance and process substantially contributes to effective governance. In this respect, different levels within an organization who need different information from the risk management process require different report types:

- **Executive reporting.** The board of directors has the highest oversight responsibility for developing and implementing the organization’s mission, values, and strategy, and must carefully review corporate processes of risk identification, monitoring, and management. The board also sets risk philosophy, risk appetite, and risk tolerances. Specific reviews of financial objectives, plans and other significant material transactions also typically fall within a board’s responsibility. These responsibilities require broad and transparent reporting on the various organizational risks (strategic, operational, reporting and compliance risks). Appropriate communication to the board includes reporting on:
  - Progress against organizational objectives and related risks;
  - Effectiveness of the ongoing monitoring processes on risk and control matters, including reporting any significant failings or weaknesses.

Risks can crystallize quickly, and the board should ensure that there are clear processes for bringing significant issues to its attention more rapidly when required, and agree the triggers for achieving this. The board should also specify the nature, source, format and frequency of the information it requires, and monitor the information it receives, ensuring that information quality is sufficient to allow effective decision-making.

- **Operational reporting.** The risk management system should include procedures for immediately reporting to appropriate levels of management any significant control failings or weaknesses that are identified, together with details of corrective actions being undertaken. In dividends should systematically and promptly report to low and middle level management any perceived new risks or failures of existing control measures. **Middle level management** should systematically and promptly report to senior management any perceived new risks or failures of existing control measures. Without proper internal reporting on organizational risks, managers cannot make optimal tactical decisions. **Senior management** needs relevant and reliable risk reports on a real-time and periodic basis for effective control: an example is represented by the risk matrix, a table in which rows show the risks and columns show their likelihood of occurrence and their impact.

- **Review/audit report.** Not every risk has an internal control, but every internal control should address a risk. Internal audit reports are a key source of information on the organization’s performance and control environment, to align internal controls to risks. The output of a review or audit will be a report summarizing its findings, and providing conclusions of the assessment against pre-determined criteria. This report may provide recommendations for system improvements, based on what the reviewers have observed. An annual report on the overall state of the organization’s internal controls should be also provided (see Section 2, Ch. 5).

#### QUESTION MARK BOX

Q. In your Organization, risk management reporting is about:

R. “Management goals, results of risk workshops, identification and measurement high priority risks, monitoring of risk treatment actions. Monitoring of the implementation of strategic goals is also part of the risk management reporting. The risk management reports are provided to the management, risk owners, staff involved and to the Economic Council”.

Source: Austria, *In-depth survey on risk management practices*

**b) External reporting**

Organizations are under increasing pressure for greater transparency, mandated or voluntary, and a **better alignment of externally reported information with that which is reported internally**. Stakeholders expect intensified corporate dissemination regarding risk, and awareness of the critical role of proper risk management. In view of this, an organization should provide accurate, timely and high quality reports to meet the external stakeholders’ needs. Specifically, it should periodically conduct a review of the effectiveness of the risk management system and report to stakeholders on that, and a robust assessment of the principal risks, describing them and explaining how they are being managed or mitigated.

Organizations may consider preparing different, customized risk reports for different external stakeholders. Whilst internal risk reports aim exclusively at internal audiences, external risk reporting, including corporate annual reports, may more broadly include both external users and interested internal groups.
ISO Guide 73:2009 defines risk reporting as a form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management.

Q. In your Organization, risk management reporting is about:

R. “Management goals, results of risk workshops, identification and measurement high priority risks, monitoring of risk treatment actions. Monitoring of the implementation of strategic goals is also part of the risk management reporting. The risk management reports are provided to the management, risk owners, staff involved and to the Economic Council”.

Source: Austria, In-depth survey on risk management practices

b) **External reporting**

Organizations are under increasing pressure for greater transparency, mandated or voluntary, and a better alignment of externally reported information with that which is reported internally. Stakeholders expect intensified corporate dissemination regarding risk, and awareness of the critical role of proper risk management. In view of this, an organization should provide accurate, timely and high quality reports to meet the external stakeholders’ needs. Specifically, it should periodically conduct a review of the effectiveness of the risk management system and report to stakeholders on that, and a robust assessment of the principal risks, describing them and explaining how they are being managed or mitigated.

Organizations may consider preparing different, customized risk reports for different external stakeholders. Whilst internal risk reports aim exclusively at internal audiences, external risk reporting, including corporate annual reports, may more broadly include both external users and interested internal groups.

[1] ISO Guide 73:2009 defines risk reporting as a form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management.