7. Risk management information system

An organization should document how it manages risk. Information about risks, and the output from all applications of the risk management process, should be recorded in a consistent and secure way, establishing the policies and procedures required to access, use and transfer information as a recorded part of an information management plan. Risk management information systems should be able to:

- Record details of risks, controls and priorities, and to show any changes in them;
- Record risk treatments and related resource requirements;
- Record details of incidents and loss events, and the lessons learned;
- Track accountability for risks, controls and treatments;
- Track progress and record the completion of risk treatment actions;
- Allow progress checks against the risk management plan;
- Trigger monitoring and assurance activity.

The organization should identify adequate resources in terms of information systems and document management systems, so that capability information is relevant, reliable, timely, secure and available. This requires the maintenance of proper records and processes which generate a flow of timely, relevant and reliable information. Therefore, each stage of the risk management process should be recorded properly. Record management is an important aspect of good corporate governance: it supports activities and decisions, as well as ensuring accountability to present and future stakeholders.

The quality of an information and document management system depends on the following principles:

- Information across the organization should be consistent, to allow for efficient and accurate flow;
- Standardizing the definitions of terms and taxonomies ensures that different parts of the organization do not have different understandings of information, or are not operating on conflicting sets of information;
- It is not necessary to have a single record management system across the organization, as long as management designs and operates multiple systems to allow an efficient consolidation, exchange and integration of information;
- At the operational level, the organization should first determine the definitions, classifications and procedures needed to identify and manage risk information, as a part of an information management plan. Subsequently, as core sub-practices, it should set up ‘risk management records’ through the following steps:

  1. Defining and maintaining a risk management classification scheme and methodology;
  2. Defining an ongoing process for risk management information inventory and classification, including characteristics such as: type, preservation requirement, retention requirement, disposal requirement, availability requirement, operational/strategic value, data owner, source of information (data base/application, email, spreadsheet, etc.), confidentiality requirement, and associated organizational processes and policies.

- The organization should periodically consider changes to the classification structure, and its underlying definitions and classifications, as necessary.

The whole risk management process should be documented through a web-based tool which allows risks and treatments to be delegated and escalated among the organizational levels, and also makes it possible to connect a risk to a specific goal or activity in the operational plan of the agency (or the departments’ own action plans). Consequently, the organization should identify resource requirements related to information systems and databases.

The main features of a risk management information system within each phase of the risk management process are: data exchange/interoperability, data integration, traceability, data security.

Risk identification, analysis and measurement should be carried out within a specific tool through four steps:
1. **Qualitative assessment** (risk identification and risk analysis). The risk management information tool should record the assessment of risk in a way that assists the monitoring and identification of risk priorities. Risk assessment should be documented in a way which records these processing phases. Documenting risk assessment reveals an organization’s risk profile which: facilitates identification of risk priorities (in particular to identify the most significant risk issues with which senior management should concern themselves); records the reasons for decisions made about what a tolerable exposure is and is not; facilitates recording of how it is decided to address risk; allows all those concerned with risk management to see the overall risk profile, and how their areas of particular responsibility fits into it; facilitates review and monitoring of risks.

2. **Prioritization**:

3. **Risk measurement**:

4. **Monitoring risk treatment actions**. Staff members/managers who are responsible for risk treatment actions have to periodically report (e.g., monthly, quarterly, yearly) on the implementation/execution of actions within the tool.

**QUESTION MARK BOX**

Q1. What are the most important lessons learned from implementing risk management in your organization that other organizations should take into account when developing their own risk management processes?

R1. “Efficient IT-tool is very important”

Source: Austria, *Survey on risk management practices*

Q2. In your organization, the amount of financial resources spent to run the risk management system is suitable.

R2. “Adequate resources in the information system supporting the risk management process have been invested”.

Source: Italy, *Survey on risk management practices*

Q3: In your organization, the risk management process is connected to:

R3. “Organization performance assessment: risk analysis is fully integrated in the planning and follow up process for operations and is reported by each department in a common web based tool”. As for standardized techniques for risk identification and assessment: “the important thing is that the result is documented correctly in the web based tool”.

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