4.2 Risk treatment process

Risk treatment involves a cyclical process of:

a) **Risk treatment assessment**: an organization should select the best option at its disposal. That involves balancing the costs of implementing each option against the benefits derived from it, with regard to legal, regulatory, and other requirements such as social responsibility. In general, the cost of managing risks needs to be balanced with the benefits obtained. When making such cost versus benefit judgments, the context should be taken into account. It is important to consider all direct and indirect costs and benefits, whether tangible or intangible, and measure them in financial or other terms.

b) **Risk Treatment Plan**: Treatment should involve, at the operational level, preparing and implementing a related plan. It shows how the treatment options selected will be implemented and should be integrated with the management and budgetary processes. Specifically, the information provided in a treatment plan should include:
   a. The reasons for selecting the treatment options, including expected benefits;
   b. Who is accountable for approving the plan and who is responsible for implementing it;
   c. The actions proposed;
   d. Resource requirements, including contingencies;
   e. Performance measures and constraints;
   f. Reporting and monitoring requirements;
   g. Timing and schedule.

Lastly, responsibilities related to the treatment phase should be clearly assigned, specifying who is accountable for the management of particular risks (or categories of risk), for implementing treatment strategies, and for the maintenance of risk controls. For this, the board should ensure that management considers and implements appropriate risk responses: responsibility for treatment is usually assigned to the management level (directors-general, heads of divisions: project managers) and assigned to staff, where appropriate. Management should also identify and note in the ‘risk register’ those actions selected as treatment, and should show to the board how such risk responses improve the performance of the organization. Risk owners, according to their respective roles in the project or process, are indicated to set risk treatment plans, even though at this stage responsibilities vary according to the kind of risks (either corporate or operational). For example, senior managers are responsible for corporate risks, their mitigation strategies and action plans. The operational risk responsibility relies on the divisional levels which the program is assigned to.

c) **Risk treatment monitoring**: in designing response actions, it is important that the controls put in place are proportional to the risks. Risk analysis assists such a process by identifying those risks requiring attention by the management. Risk control actions will be prioritized in terms of their potential to benefit the organization. Effectiveness of internal control is determined by how much the risk will be either eliminated or reduced by the control measures proposed. The latter need to be measured in terms of potential economic effect if no action is taken, versus the cost of the action(s) proposed, and invariably require more detailed information and assumptions than are promptly available. Every response action has a related cost, and it is important that the treatment offers value for money in relation to the risk controlled by it. In this regard, options in addressing risk (“TREAT”) can be further analysed into four different types of related/associated controls:

- **PREVENTATIVE CONTROLS.** These are designed to limit undesirable outcomes. The more an undesirable outcome should be avoided, the more appropriate preventative controls should be implemented[1]. Most of controls implemented in organizations tend to belong to this category.
- **CORRECTIVE CONTROLS.** These are designed to correct undesirable outcomes that have occurred, and provide a way to achieve some recovery against loss or damage[2]. Contingency planning is an important element of corrective control.
- **DIRECTIVE CONTROLS.** These are designed to ensure that a particular outcome is achieved, and are particularly important when avoiding an undesirable event – typically related to Health and Safety or to security – is crucial[3].
- **DETECTIVE CONTROLS.** These are designed to identify occasions of occurrence of undesirable outcomes. Their effect is, by definition, “after the event” so they are only appropriate when the resulting loss or damage can be accepted[4].

d) **Residual risk measurement**: If a residual risk persists even after treatment, a decision should be taken about whether to retain this risk or to repeat the risk treatment process. For residual risks that are deemed to be high, information should be collected about the cost of implementing further mitigation strategies.

**EXAMPLE OF RISK TREATMENT PLANNING**
## RISK TREATMENT - SCHEDULE

| PROPOSING DEPARTMENT | ____________________________ |
| VALIDATING DEPARTMENT | ______________________________ |
| RESPONSIBILITY        | ______________________________ |
| KIND OF TREATMENT     | ______________________________ |
| RISK DESCRIPTION      | ...................... |
| PROCESS               | ...................... |
| PHASE                 | ...................... |
| CAUSE                 | ...................... |
| ENABLING FACTORS      | ...................... |
| TIMETABLE             | ...................... |

## RISK TREATMENT - MONITORING

| OBJECTIVES         | ...................... |
| OUTPUT INDICATORS  | ...................... |
| CONTROL PROCEDURE  | ...................... |

## RISK TREATMENT – ACTION PLAN

<table>
<thead>
<tr>
<th>PHASE</th>
<th>UNIT</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Q1. Following risk identification and assessment in your organization, is any treatment of the risks put in place?

R1. “Yes. risk treatment of most significant risks is assigned to managers, and followed up (annually or bi-annually by the board of directors). The less significant risks are treated as a part of normal operations. The risk treatment of moderate or higher risks is taken to the department’s management team for approval. The treatment is assigned to a person responsible for implementing the treatment as a part of normal operations or if that is not possible a separate implementation plan is to be prepared”.

Source: Finland, Survey on risk management practices

R2. “Yes. Risk is weighted and asset owners have to set up a plan to reduce risks that are measured above a certain level”

Source: Iceland, Survey on risk management practices

R3. “Yes. Treatments are identified as part of the risk identification process - a template is completed by Heads of Division twice a year, and individual directorate risk registers and a corporate risk register are created. Ownership of the risk is assigned and the process is reviewed twice a year by the senior management committee with the individual Head of Division. The project management system also facilitates risk identification and management, and the project team review the project regularly. Risk management treatments can involve human resource solutions”.

Source: Ireland, Survey on risk management practices

R4. “Yes. Treatment of the risks is the main result of risk analysis. The results are known as control activities. In some cases control activities have been established as a result of previous experiences, well before any formal risk analysis. However only a full analysis can give a reasonable security that everything that counts has been considered and that the institution are prepared to face the consequences.”

Source: México, Survey on risk management practices

R5. “Yes, in accordance with the system procedure on the risk management approved by the NIS President (Decision no. 1038/2011). The audit reports on risk management are taken into consideration to propose treatment actions”.

Source: Romania, Survey on risk management practices

Q2. Please indicate which kinds of risks are being managed through the risk management process, while specifying connections and differences in treatment:

R1. “Approach in treatment depends on greater or lower influences of CBS in reducing risk to an acceptable level. Regarding the risk treatments, most of identified and assessed risks have been classified into two categories: risk reduction and risk avoidance or in combination”.

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

Q3. Please describe the methodology used in identifying and monitoring the risk treatment, while specifying the organization roles involved:

R1. “The methodology used by INEGI is based mainly on the international standard ISO 31000 about risk management, ISO/IEC 27000 about information security, some elements of COSO ERM (enterprise risk management), and also from the standard of the European Federation of risks (FERMA). The first version of the methodology was released in 2010, and the present version has been the result of the institutional experience of its use”.

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

Q4. With reference to RM, Internal Controls and Internal Audit System within your Organization, please describe the connection/integration between these ones in detail, while specifying: how risk treatment actions are monitored functions, roles and accountabilities involved in the monitoring of the risk treatment actions...

R1. “As for the risks, each head of an administrative unit is responsible to identify, analyse, evaluate and determine the actions of treatment.

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

Q5. Please describe who sets priorities for risk treatment actions and how:

R1. “On a corporate level, the board of directors sets the priorities. On a process level, the process owner sets the priorities”.

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

Q6. Following risk identification and assessment in your organization, is any treatment of the risks put in place?

R1. “Yes. Directors/division chiefs (risk owners) propose response actions validated by the risk manager/fraud and corruption prevention manager. These actions are selected on a priority basis (risk strategic area, risk value, feasibility), and then entrusted to the executives. Managers propose the response actions; the governance select the actions after defining their significance (prioritization); the framework is populated by the internal representative network. The validated and selected response actions are designed, carried out and monitored under the responsibility of the managers (directors/division chiefs); the framework is filled in by the representative network with the monitoring information”.

Source: Italy, Survey on risk management practices
Examples of preventative controls include restriction of action to authorized persons only, for example, permitting only those suitably trained and authorized to handle media enquiries prevents releasing of inappropriate comments to the press.

For example, drawing up contract clauses to allow recovery of overpayment. Insurance can also be regarded as a form of corrective control as it facilitates financial recovery against the actualization of a risk.

For example, requiring that staff are trained to get certain skills before being allowed to work unsupervised.

Examples of detective controls include “Post Implementation Reviews” which detect lessons to be learnt from projects, for application in future work, and monitoring activities which detect changes to be responded to.