8. Risk management maturity model

In order to enable benchmarking between implementation levels of risk management in organizations, researchers, public agencies, professional associations and standards bodies tried to define their own risk management model[1]. This type of tool contains the fundamental elements of effective risk management processes, and depicts the evolutionary scale from a basic approach to an embedded and holistic one. It allows NSOs to gauge progress in developing the necessary risk management capabilities, and to assess the effectiveness of risk handling and impact on delivering successful outcomes. It also promotes a common language and understanding. A phased approach allows the NSO: to measure where it currently is; to set goals for where it wants to go; to plot a path to get there, focusing its efforts for improvement on areas of identified weakness. Furthermore, a maturity model can serve as a recognition program[2] within the organization: attainment of a maturity level can be considered as a performance indicator.

Moreover, given that:

- There is no optimum maturity level that would be considered as appropriate for every organization (it depends on its external context, size, internal culture, people, history, complexity of the organizations’ activities, etc.)[3]; and
- The same entity could present heterogeneous levels of maturity with reference to different organizational areas (any risk management linked processes and activities can be more developed than others);

To facilitate deeper understanding of risk management, a multidimensional analysis and reading grid is proposed (Figure 5, see the full version in the Annex). It takes into account inputs from different sources: collection of actual cases of implementation of risk management systems, among statistical organizations (practices); selected case-studies, reporting certain significant experiences of NSOs; existing maturity models which are reported in the scientific and technical literature, also belonging to heterogeneous fields.

The grid has been developed by abstracting the principles of capability maturity modelling observed in the practices analysed, and through literature review. Its structure is a matrix where each of the cells is populated with a competency or capability. First, some core areas/items representing consistent sets of significant features have been identified. As a second step, specific descriptors have been developed for the purpose of illustrating in greater detail the different topics connected to the core areas. Descriptors allow the items to be allocated among four maturity levels characterised with reference to attributes/performance indicators, consisting of potential/typical features that reflect the extent to which each risk management competency or capability is defined, institutionalised and controlled. The multidimensional grid has been designed as a diagnostic tool instead of a prescriptive model for implementation. Its approach builds on the assertion that the quality of an organization’s risk management process should improve with time, with additional value being provided at each step toward increased maturity.

The grid also highlights, for each descriptor, three elements or reading-keys used both in the survey design, and in the processing phase. The data collected is analysed according to a theoretical paradigm/protocol named ‘The Template’[4]: The first element, risk rationalities (processes) correspond to the organizations’ efforts to translate uncertainty into a manageable and communicable conceptualization of risks, and the definitions of activities and tasks for dealing with them. It reflects the main purpose around which any organization bases its risk strategy (i.e. the improvement of compliance, performance, company value, etc.). The second element, uncertainty experts (roles), refers to the actors - their experience, background and interactions - organizational units or structures to which the organization assigns the responsibility for risk management. The third element of analysis, technologies (support), denotes the complex sets of practices, procedures and tools enacted to accomplish the management and control of risks.

The maturity of an organization’s risk management system can be categorized into clusters, that range from having no formal process, to fully integrated into all aspects of the entity. Risk management capability is a broad spectrum, ranging from the occasional informal application of risk techniques to specific projects, through routine formal processes applied widely, to a risk-aware culture with proactive management of uncertainty. In view of this, core areas/items are graded using a four-point scale, designed to take into account that each maturity level is a defined position in an achievement hierarchy, which establishes the attainment of certain risk management capabilities. This hierarchy is based on different stages of progressively mature organizational behaviour. It was judged that having more levels would increase the amount of ambiguity and misunderstanding, without giving sufficient additional refinement to aid usability and clear framing with respect to a specific NSO’s context. In determining its target risk maturity level, an organization needs to consider the model as progressive: so where a competency has been achieved in a previous level, it is assumed to also have been achieved in the next level. The boundaries are defined by the ends of a continuum between an immature state to that of a mature organization. The multidimensional grid has been designed to be scalable, flexible and adaptable to accommodate changes in an organization’s size, structure or regulatory context. It represents a live map which may be updated and integrated when necessary, to reflect new inputs, standards, governance regimes and so on.
At LEVEL 1:

- There are no risk management processes in place. The organization does not feel the need for managing risk, and does not use structured approaches for this purpose: it is not carrying out pre-planning activity, but is reacting to situations and risk issues after they occur with no proactive thought.
- The organization is not able to distinguish between positive and negative risk.
- Management processes are repetitive, with no attempt to learn from the past and to prepare for future threats.
- There might be a belief that most important risks are known.
- The effects of risky events might be identified, but not linked to goals, and risk events are not associated with their process sources.
- No attempt is made to develop mitigation plans.
- There is no culture of control, but one of resistance to change prevailing. There is emphasis on protecting physical and financial assets.

To move from Level 1 to Level 2, the organization needs to recognize the value of risk management, and to became aware of its potential benefits. To this end, a disruptive event or external factors – such as stakeholders' influence, government pressure, etc. – may trigger a more proactive approach towards risk, and an awareness that some form of structured system needs to be put in place to deal with uncertainty.

At LEVEL 2:

- Top management are aware of the need to manage uncertainty and risk, and have made basic resources available to improve.
- A risk strategy has been identified, and a risk management policy has been drawn up.
- Key people are conscious of the need to assess and manage risks, and they understand risk concepts and principles.
- Some stand-alone risk processes have been identified, and the related risk mitigation activities are sometimes identified but not often executed.
- Risk management mainly focuses on past events.
- Corporate culture has little risk management accountability, with process owners not well defined or communicated.
- Risk culture is enforced by policy still interpreted, nevertheless, as compliance.
- A pilot training programme has been implemented, and a core group of people have the skills and knowledge to manage risk.
- Programs for compliance, quality management, process improvement and so on still operate independently, and have no common framework, causing overlapping risk assessment activities and inconsistencies.
- Controls are mainly based on departments and finances.
- Consistent planning and tracking of performance is missing. Qualitative risk assessments are unused or informal.

Summarizing, although the organization is aware, at some level, of the potential benefits of managing risks, there is no effective widespread implementation process, and it is up to an interested individual manager to pursue good practices. There is limited evidence that risk management is being effective in at least the most relevant areas.

At LEVEL 3:

- Organizational processes are identified, and risk ownership is clearly defined and well communicated to all staff.
- Authorities, roles and responsibilities are identified, and appropriate resources allocated.
- Agreement exists on a risk framework, and operating guidance is available.
- Senior managers take the lead to ensure that approaches for addressing risk are being developed and implemented in all key and relevant areas.
- Events are associated with their source processes.
- Emphasis is on developing a series of proactive action plans, to deal with events that may impact the organization and its stakeholders, to better respond to identified issues, and to consider measures reducing the likelihood of undesirable events and their consequences.
- More weight is given to preemptive planning.
- Qualitative assessment methods are used to determine what deeper needs exist for use of quantitative methods, analysis, tools and models.

This phase provides the opportunity to increase awareness for a large portion of the organization. There is clear evidence that risk management is being effective in all relevant areas. By the end of this stage, a culture of risk management is taking hold within the organization, and includes the management of opportunities.

At LEVEL 4:

- The management of risk is everyone's responsibility, and the risk management system is enforced at every level: it is embedded in all organizational processes and strategies, and is a formal part of goal setting and achievement.
- Accountability is embedded into all processes, support functions, lines and locations, as a way to achieve goals.
- A risk-based approach to achieve goals is used at all levels.
- A terminology and classification for collecting risk information is fully implemented.
- Risk and performance information is collected from all areas, to identify dependencies and root cause indicators' frequency; moreover, it is actively used to improve all organizational processes.
- Mitigation measures are determined, and a method to quantify effectiveness is understood.
- Risk mitigation is integrated with assessment (carried out with quantitative analysis, tools and models supporting qualitative methods) to monitor effective use.
- Measures ensure downside and upside outcomes of risks and opportunities are aggressively managed.
- Standardized evaluation criteria of impact, likelihood and controls' effectiveness are used to prioritize risk for follow-up activity.
- Frontline employees' participation and documents risk issues' or opportunities' significance are promoted.
- Process owners regularly review and recommend risk indicators that best measure their areas' risks.
- The results of internal adverse event planning are considered to be a strategic opportunity.
- Career development and compensation include incentives for effective risk management.
- The organization measures the effectiveness of managing uncertainties and seizing risky opportunities.
- Deviations from plans or expectations are measured against goals.
- A clear, concise and effective approach to monitoring progress toward risk management goals is communicated regularly with business areas.
Level 4 is viewed as an iterative continual improvement phase, where risk management system feedback loops permanently encourage learning from experiences in order to achieve excellence. A proficient level is characterized by specific features, such as: organizational resilience and commitment to excellence; risk management as an inseparable part of decision making and day-to-day operations; risk management as an objective in all senior management performance agreements; risk capability continually reinforced and sustained by top management; leaders regarded as exemplars; organization selected as an example of good practice by others; good record of innovation; sound risk management arrangements established to manage risks together with all partners.

Figure 5. Extract from a Multidimensional analysis and reading grid: Risk management maturity
QUESTION MARK BOX

Q. With reference to the risk measurement phase, does your organization use different techniques concerning risk classification (IT, financial, compliance, etc.)?

R1. “Yes. This varies considerably depending on the type of risk and the risk maturity of the business area. Typically corporate areas are more risk mature, usually by virtue of having a long standing responsibility for supporting the organization to manage a specific type of risk”.

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

Q. Comments or observations:

R1. “The risk management system is still being developed, and we anticipate moving along the maturity model as the system is further developed”.

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

Q. Has the level of staff awareness of risks and/or risk management been evaluated during the implementation of the risk management process in your organization?

R1. “Yes, during the starting phase. A survey involving the management was carried out in order to evaluate and measure the risk perception and the maturity of the internal (within the single organizational divisions) and external (among divisions within the organization) control systems.

Source: Italy, Survey on risk management practices

R2. “Review of risk maturity and understanding is part of the design of the risk management framework but has not yet been developed”.

Source: New Zealand, Survey on risk management practices

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

R1. “Both organization and individual performance assessment. Risk management is an objective in all senior management's performance agreements – there are considerations being made to roll this out to the whole organization's employees. The organization has a risk policy and process guide, which sets out the process to which the entire organization adheres daily. The risk maturity level is a measure against which we record our progress, as well as management information being presented in the monthly Performance Report to Directors”.

Q. In your organization, the information derived from the risk management process has been used to: Understand causes of low performance (organizations and/or individual) and review change processes:

R1. “Somewhat Agree. This is done, but the organization is developing its risk maturity and is not quite embedded yet, but the risk management team has a plan to ensure this continues to mature over the next 12 months”.

Q. In your organization, which development phase is the risk management process currently in?

R1. “Some areas are very mature, others have opportunity for improvement, though in general it’s a very good standard”.

Q. What are the strengths of the risk management system in your organization?

R1. “Introduction of risk targets and reassessment of risk appetite. New risk database and new risk policy have all helped maturity and risk literacy”.

Source: UK, Survey on risk management practices

---


[2] By using a recognition program the organization can incentivize its stakeholders to continually improve resilience and performance.


[4] The Template shared during the Workshop of the Modernization Committee on Organizational Framework and Evaluation, held in Geneva on 14 to 17 October 2014, takes into account the most used and well known international standards, such as Enterprise Risk Management Conceptual Framework (ERM): Internal Control-Integrated Control, developed by Committee of Sponsoring Organizations (Co.S.O.), and ISO 31000:2009 (Risk Management – Principles and guidelines).