Focus on: Risk management maturity model

In order to pursue the continuous improvement of the risk management system, the most advanced statistical organizations, have introduced methods to analyze the maturity of their risk management models, defining assessment grids, composed of variables representing the main components of the system itself.

CASE STUDIES:

UK, Office for National Statistics (ONS)

ONS has developed a model to analyze and measure the level of its maturity risk management system significantly advanced.

It consists of 5 levels of maturity, each of them is described by the following variables:

1. Knowledge & Skills;
2. Behaviors;

<table>
<thead>
<tr>
<th>Level</th>
<th>Knowledge and Skills</th>
<th>Behaviors may include...</th>
<th>Metrics – for measuring progress</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LEVEL 1</strong></td>
<td>Staff, managers and leaders are aware that risk management is something that should be done, but do not understand why or how. Have received but not fully read and understood communications material on risk.</td>
<td>Staff, managers and leaders are not yet taking action to identify and control risk across the organization or in high risk areas. Training gaps are known and being addressed. Staff has to decide for themselves what level of risk taking is acceptable.</td>
<td>1. No risk champions or other indicators of a risk management culture. May have heard of the concept, or be able to identify with it, probably in the context of project management. Risk registers may have been produced, but will have been done for them, by ‘experts’ or as a one-off. 2. It may have a coordinator who is ‘a voice in the wilderness’. 3. Risk appetite not defined - excessive risk aversion in some places and excessive risk taking in other places. 4. Risk not shared with Director unless there is a crisis.</td>
</tr>
<tr>
<td>Awareness</td>
<td>Risks often not aligned to the objectives of the business area or Directorate. Awareness of the need for good risk management – but may not have fully bought in to the concept. Understanding the theory and processes behind formal risk management, but it may think of risk as a compliance tool, risk as a tool for real business improvement. Understanding activity to date, including senior management, strategic risks and existence of risk policy statement, risk framework, guidance and training programmes. Understanding who to contact for further support. Training is taught by, and for, key people. Understanding some of the key risks to the organization and to their area. Understanding there are formal procedures that need to be implemented, but not yet implemented them all.</td>
<td>Possible attendance at introductory risk training courses and key staff will probably have read ONS risk policy statement or practical guidance. If applied, risk management has been a time-consuming, mechanistic process. Often involves a junior team member creating a risk on the risk database, which is collecting dust and rarely updated. Risks often materialize which should have been foreseen and recorded on the risk register. Staff has participated in collating or drafting reports (e.g. strategic risks). Senior management are not yet persuaded of the benefits, or rarely lead by example. Staff very unwilling to bring forward and expose problems and vulnerabilities until instructed to. Perceived culture of ‘shooting the messenger’. Risk mitigation sometimes hampered by a lack of clarity in the articulation of individual risks. Blame culture apparent, with people too scared to say ‘no’. Staff has to decide for themselves what level of risk taking is acceptable leading to excessive risk aversion in some places and excessive risk taking in other places.</td>
<td>1. Normally have risks recorded at divisional and probably at directorate levels, plus at least 50% of directorates have them. 2. Risk registers will typically be mechanistic and compliance-focused documents, which are updated on request of overseers (e.g. the center). 3. Risk not normally a standing item at management, project, programmes or divisional board meetings. 4. Organizations will have a nominated risk champion. Organizations will have risk coordinator, who is departmental ‘expert’. 5. Some staff have been on risk management training. Corporate center regularly called on to support management, units, projects, programmes or departmental boards within the directorate. 6. No evidence of a systematic approach to escalating risks from team/divisional levels. Risks escalated from the team/divisional levels on an exceptional basis for example, as the result of a crisis or externally generated event such as media interest. 7. Strategic and Directorate risks have either not reduced in severity over the last two quarters or reductions in severity cannot be traced to the actions taken by the risk owner / business. 8. Risks in the database are not clearly articulated in all cases and / or risk owners have not been allocated. 9. Mitigating Action and Contingency plans do not exist where they are needed. 10. Risk appetite not defined.</td>
</tr>
<tr>
<td><strong>LEVEL 2</strong></td>
<td>Basic Understanding</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Level 3: Application

#### Knowledge and Skills
- Staff, managers and leaders know how to identify, assess, address, monitor and report risk in a consistent, structured manner, in line with Organizational guidance.
- Real ownership for risk and actions exists.
- Management at all levels in the organization have a clear understanding of how risk should be managed and they act in accordance with this.
- Management at all levels have visibility of the work they oversee, and have the skills to interpret and challenge what they see in order to expose risk.
- Key staff are aware of the need to manage risks with partners and have the skills and knowledge needed to manage these risks.
- All information asset owners have received training and understand:
  - The nature, value and benefits of the information assets they own.
  - The principles of risk management, and
  - the risks inherent in the data and systems they own.
- Information Asset Owners know who their risk coordinators are, and vice versa, and the IS&IT know how to escalating IA risks within their business areas.

#### Behaviors may include
- Risk workshops have been held to kick start the process. Staff are implementing basic risk management processes.
- Staff are using basic risk information to inform decision-making, e.g. information asset owners will typically risk why information is being requested and query which elements of the data they hold needs to be passed on. Information that is passed on will be done so in as far as is possible. Losses will be reduced, but not eradicated.
- SCL.8 and GD.7 act as risk models and lead on risk management. Heads of Directions/Unit/Branch/project/programme regularly ask:
  - Have you been to see for yourself how this risk is managed?
  - Has the risk severity changed in the last week?
  - What level of severity are you testing to manage this risk down to?
  - What has been done about this risk in the last week?
  - Have you discussed this risk with your Director?
- Managers:
  - Send a message to staff that they can be confident escalations will be acted upon.
  - Escalations are only considered, including information asset risks they are responsible for.
- Identify and manage risks that cut across delivery silos.
- Discuss risk each week with their staff and up the line, monitor actions weekly and check they are sufficient.
- Communicate downward what the top risks are.
- Escalate risks from Delivery level.
- Link to discussions of finance, strategy and stop/slowdown projects to reduce risk as well as cope with budget.
- Demonstrate we really have an appetite for setting priorities – and stopping / slowing down the non-priority areas.
- Learn about good risk management from other organisations.
- Send a message that we are still ambitious but need to reduce our risk exposure.
- Ensure we do not blame people for escalating risk.
- Check regularly that processes are well controlled.
- Preventive “can do” attitude to problem asking.
- Leaders, managers and staff learning the lessons from past mistakes.

#### Metric – for measuring progress
- We know what our top risks are, especially those affecting public protection and those sourced from the front line.
  - Risk exist on the database at directorate and 95% of them have recorded risks on the database.
  - All details with responsibility for agency either have identified and recorded emerging risks which risk take of and the risks shared with these bodies. This will include information asset risk registers. Risks clearly articulated in all areas.
  - Risk registers, including information asset risks, are regularly updated and used at management meetings throughout the organization.
  - A process is universal and visibly in operation for escalating risks from the team level down through divisions, public bodies, suppliers, contractors, partners, projects and programmes, to directorate level and strategic level. Such risks can be tracked through the risk database.
  - Risks to data/information are foreseen, included on the risk database, and the extent of the risk is clearly articulated. The business is alert to risks, including those in low priority areas, e.g. such as small information systems.
  - Good risk behaviors – as well as good process.
  - Risk is being seen at management meetings throughout the organization. Managers regularly discuss risk with their staff – what the key risks are, what has changed since last week or month, how mitigating actions are being progress.
  - Leaders and managers are visible, appropriate and actively encourage staff to escalate risk. No one is blamed for escalating risks and good risk management is recognised positively in Performance Agreement assessments.
  - But staff are held to account for failing to escalate a risk or to take mitigating actions.
  - There is a risk champion and they support staff, and also promote good risk management behaviors and compliance with corporate standards throughout the business.
  - Key staff/project managers, SICLs, business and strategic support staff have been trained in risk management to the appropriate level and can explain the benefits to other staff, which they do on a regular basis. Likewise, Information Asset Owners have all been trained in Risk management and can identify and escalate risks to their assets where necessary.

Planning for risks over the long term as well as the short term:
- All risks and red risks have contingency plans in place.
- Senior Board has been alerted to the risks including those identified on risk registers. Risks are discussed regularly jointly with Directors and are identified in management reports.
- The business has defined its risk appetite, including those relating to information asset risks, and plans are in place to ensure this.
- Risks that arise to five years away are identified and mitigating actions or contingency plans are in place.
- Managing process, and information asset risks, as well as project risks and risks.
- Risks on the database identify process risks, especially those that contribute to:
  - The process is poorly defined or compliance is infrequently checked,
  - gaps exist between adjoining processes,
  - data gets lost in the system,
  - the priority of a process is not clear or is in dispute,
  - the process has been improved, but a legacy of old cases remains,
  - there is a backlog of work, and
  - there are interactions between processes that are owned by different people.
- Information asset owners are aware of the criticality of their information assets and the attended requirements and are beginning to follow the published guidance on governance and guidance. Business areas can show the following:
  - all are risk subject to accreditations, as a matter of course, where appropriate, Privacy Impact Assessments are used and effective contract mechanisms are used to apply to data, and the information assets have been identified for all accredited in-service information systems.

### Level 4: Embedding

#### Knowledge and Skills
- In addition to the above, staff effectively share those risks owned by or shared with partners, and can confidently press this point with partners.
- Ensure the Department communicates effectively on significant risks to the public which arise in their area.
- Formally review the effectiveness of all aspects of their Risk management activity.
- Senior management, including the Board, are actively engaged in broadening their horizons on risk through participation in internal events and training.
- The organization is increasingly seen as an example of best practice across government.
- All information asset owners and managers are aware of the importance of managing information assets effectively and appreciate the benefits of doing so and the risks if they get it wrong.

#### Behaviors may include
- Open communication internally on risk. Assessments of the effectiveness of risk management being undertaken.
- Longer term risks are integrated into the strategy and business planning functions. Business planners are beginning to think about whether enough resource has been allocated to the potential risks that may materialize during the planning cycle and allocates accordingly.
- Our people and workforces are increasingly plugged into our partners.
- Share risk information with delivery and other business partners.
  - Where risks are owned by others we are ready to challenge if appropriate and if we perceive there are inappropriate risks being ignored or not taken seriously.
- Staff are being trained in the management of risk.
- Risk workshops shared with partners, we are beginning to become more comfortable sharing with partners, where in the past we wouldn’t.
- Discussions about risk are becoming increasingly more mature and widespread (and this is evidenced in minutes and notes).
- These discussions underpin the escalation process and form part of both the internal and external escalation process.
- Executive Boards can be seen to be giving direction in the oversight and management of risk.
- Risk management of risk escalation is beginning to be shown.

#### Metric – for measuring progress
- At LEVEL 3 above, but risk is becoming mainstreamed and less noticeable as a separate activity – can show evidence of this across the business – quality of risk lifecycle. Key elements from level 3 that are strengthened here are:
  - discussing, handling and escalation (metric 5 below), strengthening metric 2, 3 and 5 above),
  - strategic risks (metric 6 below, strengthening metric 12 above), and
  - Process risk management (metric 6 below, strengthening metric 15 above).

We know our top risks are 1. We also share or discuss our critical risks amongst ourselves (cross-cutting risks) and in our key partnerships (ICDLs, with partners and suppliers, where appropriate, and we can evidence this. In practice, the means business areas can evidence that their top processes, (where shared, see metric 6 below), their top programmes and projects (as agreed between us and the business areas) and any other significant bilateral or multilateral understandings) are covered above, but agreed, assurance can be given that the top risks are discussed and shared appropriately, supported by mapped and repeatable processes.

Good risk behaviors – as well as good process.
- Risk management has been established and judged to be effective and this can be shown through assurance and governance reporting. (In practice, this means that business can show through its governance mechanisms and/or external assurances.
- Risk awareness and management of the risk escalation process. In practice this means that all of the parts of the organisation can show that there is a robust network and hierarchy for escalating risk with the “flagship” up and down the line as the lens of this framework i.e. discussions on risk take place, as regularly as the need dictates, throughout most of the organisation. Escalated and de-escalated risks will be found at all levels. There is no single model that is right, though evidence will be there through analysis/overview of management info. An effective system will explicitly have risk discussion in the minutes and be backed up by audit reviews showing the movements of risk through business areas hierarchically.

Planning for risks over the long term as well as the short term:
- Evidence of risk being taken account of in the business planning and resource allocation/budget setting process throughout the planning period. (Assumed as part of the business planning cycle, each business area will be able to evidence that resources have been allocated to the risk management activity can be taken into account in the business and financial priorities for that coming year)
- Business Continuity Planning is in place, as required, that:
  - All units, directorates and groups – where appropriate – have supportive, up to date and tested BC plans in place, and
  - The Domestic BC Plan is on track against the prescribed timescale targeted BS 25999. (This sub metric for individual business areas to report on, and if necessary within BS 25999)
- Managing process, and information asset, risks as well as project risks and risks to organisational Units:
  - Where not assessed at Metric 2 above, process risks have been identified and mitigating actions are in place. (To practice the means that business areas will be expected to outline their key business processes and the associated risks – PDU will ask if all significant threats have been identified and if they have, whether they are being adequately mitigated)
  - All information systems that are critical to the business have been identified and subject to Accreditation and therefore organisation has effective information asset risk management processes in place to manage the residual risks and the related, systems IA risks.
  - No in this instance, this has been taken to mean the residual risks identified by the Accreditation process. Level 4 HMG All Models
- Health and Safety improvements are on track against the Health and Safety Improvement programme. (This metric for individual business areas to be marked on, but via the HO Health and Safety Sub-Committee, not via risk coordinators)
- Compliance with information security management systems requirements – BS 27001 (not formal accreditation).
ITALIAN NATIONAL INSTITUTE OF STATISTICS (ISTAT)

ISTAT has developed a model that considers all components of the framework and risk management process described in the guidelines; each component is articulated on 4 levels that represent the specific maturity level, based on the statements deriving from the analysis of the practices collected through the surveys and from the comparison among the most relevant international risk management standards.

Some descriptors have been made up for the purpose of illustrating in greater detail the different topics connected to the core areas. These allow the items to be allocated among four maturity levels characterized by reference to attributes / performance indicators, consisting of potential / typical features.

The grid highlights, for each descriptor reflecting the extent to which each risk management competency or capability is defined and controlled, three elements or Reading-keys used both in the survey design and in the processing phase:

1. Risk rationalities (processes) that corresponds to the organizations’ efforts to translate uncertainty into manageable and communicable conceptualization of risks, and the definitions of activities and tasks to deal with them.
2. Uncertainty experts (roles) that refers to the actors - their experience, background and interactions -, organizational units or structures to which the organization assigns the responsibility for risk management.
3. Technologies (support) that denotes the complex sets of practices, procedures and tools enacted to accomplish the management and control of risks.

Coherently with this framework, core areas / items are graded using a four-point scale, designed taking into account that each maturity level is a defined position in an achievement hierarchy establishing the attainment of certain risk management capabilities.
<table>
<thead>
<tr>
<th>READING KEYS</th>
<th>ITEMS / CORE AREAS</th>
<th>DESCRIPTORS</th>
<th>STAGE (LEVEL 1)</th>
<th>STAGE (LEVEL 2)</th>
<th>STAGE (LEVEL 3)</th>
<th>STAGE (LEVEL 4)</th>
<th>Attributes / Performance Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading Keys</td>
<td>Environmental analysis</td>
<td>Multidimensional analysis and reading grid: RM maturity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Risk Framework

#### Safety culture

- **Attitude towards uncertainty (Risk Philosophy)**
  - No proactive though the organisation is facing situations and uncertainty issues arise.
- **Mandate**
  - The board does not drive the need for managing risk.
- **Risk strategy and policy**
  - The need for a risk strategy and related management policy has not been identified and accepted.
- **Approach to RM**
  - No risk approach to addressing uncertainties.
- **Management and commitment**
  - Management is not committed to addressing risk management and has not assumed a leadership role in implementing it.

### Environmental analysis

- **Internal and external context analysis**
  - An internal and external context analysis has been planned or is to be carried out.

### Environmental analysis

- **External and internal context analysis**
  - An internal and external context analysis has been planned or is to be carried out.

### Risk Rationales: RM Framework and Processes

#### Process Mapping

- **Risk assessment**
  - No attempt is made to identify risks or develop mitigation or contingency plans.
- **Risk treatment**
  - Risk registers are typically mechanical and compliance-focused documents, which are up dated on request of management.
- **Risk related control & audit**
  - Risk registers include mechanisms and compliance-focused documents, which are up dated on request of management.

### Environmental analysis

- **Risk treatment**
  - Mitigation Actions and Contingency plans do not exist where they are needed.

### Environmental analysis

- **Controls**
  - Controls are used on all high basis to respond to risk and a changing environment.

### Environmental analysis

- **Risk based control & audit**
  - Controls are used on all high basis to respond to new risks and a changing environment.

### Environmental analysis

- **Multidimensional analysis and reading grid: RM maturity**
  - Opportunity approach: a common and consistent definition of risk exists and risk assessment is applied throughout the organisation.
  - Open and proactive approach: risk that considers both threat and opportunity.
  - Risk-based approach to high-level goals is used at all levels.
### Risk Rationales: RM Framework and Processes

#### Reading Keys
- **Core Areas:** Items / Core Areas
- **Descriptors:** Stages (1-4)
- **Attributes/Performance Indicators:** Attributes / Performance Indicators

#### Stage (Level 1)
- **Attributes:** No evidence of improved outcomes
- **Descriptors:** Risk discrimination ability
- **Implications:** There is limited evidence that risk management is being effective in all relevant areas.
- **Actions:** There is evidence that risk management is failing to deliver improved outcomes. Identified risk management processes are not aligned to the operational strategy.

#### Stage (Level 2)
- **Attributes:** No impact on work and staff
- **Descriptors:** Impact on work and personnel
- **Implications:** There is limited evidence that risk management is being effective in all relevant areas.
- **Actions:** There is evidence that risk management is failing to deliver improved outcomes. Identified risk management processes are not aligned to the operational strategy.

#### Stage (Level 3)
- **Attributes:** Risk management information is not used in the decision making process
- **Descriptors:** Use of RM in decision making
- **Implications:** Risk management information is not used in the decision making process.
- **Actions:** Informations derived from the risk management process is used to assess the level of strategic/operational alignment by business units, managers and employees.

#### Stage (Level 4)
- **Attributes:** No connection
- **Descriptors:** Integration with quality framework
- **Implications:** The functions are not aligned and not completely integrated.
- **Actions:** The functions are not aligned and not completely integrated.

### Risk Rationales: People, Roles, Structures and Interactions

#### Reading Keys
- **Core Areas:** Items / Core Areas
- **Descriptors:** Stages (1-4)
- **Attributes/Performance Indicators:** Attributes / Performance Indicators

#### Stage (Level 1)
- **Attributes:** Risk management systems are not in place
- **Descriptors:** RM systems Monitoring 
- **Implications:** A risk management system is not in place.
- **Actions:** A framework to measure progress in implementing risk management in place.

#### Stage (Level 2)
- **Attributes:** No decentralization of information
- **Descriptors:** RM culture
- **Implications:** People tend to be risk adverse: caution approach is taken to risk management.
- **Actions:** RM is done prospectively and a culture of control is being disseminated.

#### Stage (Level 3)
- **Attributes:** No ethics policy or guidelines in place
- **Descriptors:** Linkage to ethics and value
- **Implications:** Organization may have an ethics, compliance and code of conduct strategy.
- **Actions:** Ethics and values policies are included.

#### Stage (Level 4)
- **Attributes:** Risk management systems are not in place
- **Descriptors:** Risk management systems are not in place.
- **Implications:** A risk management system is not in place.
- **Actions:** A framework to measure progress in implementing risk management in place.
<table>
<thead>
<tr>
<th>READING KEYS</th>
<th>ITEMS / CORE AREAS</th>
<th>DESCRIPTORS</th>
<th>STAGE (LEVEL 1)</th>
<th>STAGE (LEVEL 2)</th>
<th>STAGE (LEVEL 3)</th>
<th>STAGE (LEVEL 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Attributes / Performance indicators</td>
<td>Attributes / Performance indicators</td>
<td>Attributes / Performance indicators</td>
<td>Attributes / Performance indicators</td>
<td>Attributes / Performance indicators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Role: corporate culture has no risk management with process owners not defined</td>
<td>Specialist: senior management recognizes accountability with process owners well defined</td>
<td>A formal process is in place whereby senior management assumes responsibility for the overall risk management process. Risks are identified by senior management on a collective basis, and plans of action developed.</td>
<td>Risk management responsibilities are formally stated in accountability agreements and/or governance documents and are communicated, shared, and maintained at all levels of organizations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Staff accountability: senior management accountability not well defined</td>
<td>Staff accountability: senior management accountability well defined</td>
<td>The management of risk is everyone’s responsibility.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Human resource availability: resources are not available</td>
<td>Human resource availability: resources available</td>
<td>The allocation of suitable human resources for monitoring activities is centrally coordinated in the organization’s operating budget and staffing plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specialist: risk analysis not available</td>
<td>Specialist: risk analysis available</td>
<td>An integrated and multidisciplinary centre of excellence exists for risk management. There is a cross-functional integration between specialists and staff. Specialists have a broad understanding of strategic, operational and functional risk issues and are recognized externally.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Communication: no internal communication flows about risk</td>
<td>Communication: internal communication flows about risk</td>
<td>Open, transparent, inclusive and two-way communication is facilitated through regular and frequent information exchange.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Document management: no risk management information system has been envisaged</td>
<td>Document management: risk management information system has been envisaged</td>
<td>A specific risk IT system is being implemented as a part of other information systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk identification: risk events might be identified but not associated with their process sources</td>
<td>Risk identification: risk events and their sources are well defined</td>
<td>The effects of risk events might be identified but not associated with their process sources.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk assessment: risk assessment models and techniques have limited scope</td>
<td>Risk assessment: risk assessment models and techniques have wide scope</td>
<td>Techniques have limited focus in specialized areas (financial risk, IT risk management).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk reporting: risk reports are not used in a structured manner</td>
<td>Risk reporting: risk reports are used in a structured manner</td>
<td>Risk identification and reporting processes are well documented. Risk reports are used in a structured manner.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk control: risk controls are not implemented</td>
<td>Risk control: risk controls are fully implemented</td>
<td>Risk controls are implemented and monitored. Risk management information systems are well coordinated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk communication: risk communication is not effective</td>
<td>Risk communication: risk communication is effective</td>
<td>The communication establishment facilitates internal and external communication. Risk communication is effective.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk training: risk training is not provided</td>
<td>Risk training: risk training is provided</td>
<td>Risk training is provided and risk awareness is raised.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Risk monitoring: risk monitoring is not effective</td>
<td>Risk monitoring: risk monitoring is effective</td>
<td>Risk monitoring is effective.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TECHNOLOGIES: SUPPORT**

- **Risk identification**: Unstructured or informal qualitative methods since the know how required could not be available from the staff. Historical data review, semi-structured interviews, project planning.
- **Risk assessment**: Structured qualitative methods (e.g., Delphi method, scenario analysis, etc.) are used to determine what risks need to be addressed.
- **Risk control**: A wide range of qualitative and quantitative tools is used for risk management. Knowledge transfers occur between risk specialists and managers to balance benefits and limitations of available tools and models.
- **Risk communication**: Comprehensive and periodic internal reporting on both significant risks and risk management processes is regularly provided, at both executive (board of directors) and operating level (management). It contributes to strategic insights, decision-making, and improved organizational decisions. Reliability and detail of risk information has significantly increased.
- **Risk training**: A specific training program for risk management is provided and personal running RM metrics in all key and relevant areas is equipped with necessary skills, guidance, and learning tools. Most people have relevant skills & knowledge to manage risks effectively. Risk skills gap is being addressed.
- **Risk monitoring**: All staff at all levels receive regular and appropriate guidance and training to identify risk and address issues, and risk management processes are well documented. Risk information is disseminated to others at all levels through regular and ongoing training.

**Human Resources**

- **Human resource availability**: Resources are not available.
- **Human resource availability**: Resources are available.
- **Human resource availability**: Resources are well defined.
<table>
<thead>
<tr>
<th>READING KEYS</th>
<th>ITEMS / CORE AREAS</th>
<th>DESCRIPTORS</th>
<th>STAGE (LEVEL 1)</th>
<th>STAGE (LEVEL 2)</th>
<th>STAGE (LEVEL 3)</th>
<th>STAGE (LEVEL 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Communication system</td>
<td>RM Internal communication instruments and tools</td>
<td>No specific internal means for communicating about risk are envisaged</td>
<td>Some internal tools to share knowledge among a core group of people about risk have been implemented (e.g. knowledge sharing systems such as wiki platforms, SharePoint sites)</td>
<td>An Internal Communication plan and a team responsible for communicating about organization’s policy and ownership have been defined. Meetings with all the organizational divisions involved are organized. Other tools to share RM information are face-to-face discussion, real-time sharing sessions</td>
<td>Adequate and efficient communication plan and tools to share RM knowledge, information and practices with all internal stakeholders and to promote co-operation and dialogue are in place (e.g. regular internal meetings, workshops and seminars, webcasts, webinars, email updates, etc.)</td>
</tr>
<tr>
<td></td>
<td>Financial Resources</td>
<td>Financial resources adequacy</td>
<td>No resources are envisaged to implement a RM system</td>
<td>Financial resources made available to manage risk are limited and shared with other pilot programmes</td>
<td>A specific RM budget is provided but not yet adequate. It includes primary financial resources such as the allocation of staff to support the implementation of the organization’s risk framework and a budget to incur specific risks related to key and relevant assets</td>
<td>The allocation of suitable resources for managing risk is systematically considered in the organization’s operating budget; senior executive management discusses target maturity levels for each critical component of RM and a decision is made about the necessary investments. This includes the costing of opportunities for improved processes or additional programmes and resources to implement, monitor and review the framework</td>
</tr>
</tbody>
</table>