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>LEVEL 1</td>
<td>Awareness</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>
</tr>
</tbody>
</table>

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 at 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. Risks not shared with Director unless there is a crisis.

LEVEL 2 - Basic Understanding

- Risks often not aligned to the objectives of the business area or Directorate.
- Awareness of 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, not 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 sought 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.

- 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 remain yet persuaded of the benefits, or rarely lead by example.
- Staff very unwilling to bring forward and expose problems and vulnerabilities unless instructed to. Perceived culture of ‘shooting the messenger’.
- Risk mitigation sometimes hampered by a lack of clarity in the articulation of individual risks.
- Team 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.

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 normally called on to support management teams, 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.
### 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, inline 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 to enable them to manage the risks.
- All information asset owners have received basic training and understand:
  - The nature, value, and benefits of the information assets they own.
  - The principles of risk management, and the risk interest in the data and systems they own.
- Information Asset Owners know who their risk co-owners are, and vice versa, and the SLAs know how to escalate IA risks within their business areas.

#### Risk worksho...f
- 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. Asset owners will typically ask what information is being requested and query which elements of the data they hold needs to be protected. Information that is passed on will be done so as safely as possible. Losses will be reduced, but not eradicated.
- SICs, G6, and G7 act as risk models and lead on risk management. Heads of Divisions/Site/Branch/Project/Programme regularly ask:
  - Have you been asked 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 undertaken, including information asset they are responsible for.
- Identify and manage risks that cut across delivery silos.
- Discuss risk each week with staff and up the line, monitor actions weekly and check they are sufficient.
- Communicate downwards what the top risks are.
- Escalate risks from Divisional level.
- Link up discussions of first - in - stop/stop 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 organizations.
- Send out 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.
- Practice "can do" attitude to problem solving.
- Leaders, managers, and staff learning the lessons from past mistakes.

#### Matrix for measuring progress
- We know what our top risks are, especially those affecting public protection and those sourced from the front desk.
  1. Risk exist on the database at divisional, directorate and 95% of them have recorded risks on the database. All divisions with responsibility for a geographic area have identified and recorded risk items which risk takes in account the risk shared with these bodies. This will include information asset risk register. Risks clearly articulated in all cases.
  2. Risk register, including information asset risks, are regularly updated and used at management meetings throughout the organization.
  3. A process is universally and visibly in operation for escalating risks from the team level - through divisional, public bodies, suppliers, contractors, partners, projects and programmes, to directorate level and strategic level. Such risks can be tracked through the risk database.
  4. Data to risks/measure are forensic, included on the risk database, and the extent of the risk is clearly articulated. The transfer is built to risks, including those in low priority areas, e.g. such as small information systems.
- Good risk behaviour — as well as good process.
- Risk is a standing item 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 last month, how mitigating actions are being progressed.
- Leaders and managers are visible, approachable and actively encourage staff to escalate risk. No one is blamed for escalating risks and good risk management is recognised positively in Performance Assessment agreements. 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 to promote good risk management behaviors and compliance with corporate standards throughout the business.
- Key staff (project managers, SICs, 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 tasks and risks have contingencies planned.
- Senior Board has been alerted to the risks including those identified on risk registers. Risks are discussed regularly (weekly) with Directors and are identified by all senior managers.
- The business has defined its risk appetite, including those relating to information asset risks, and plans are in place to ensure this.
- Risks that are mine 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 processes, especially those that are shared.
  - The process is poorly defined or compliance is infrequently checked.
  - Gaps exist between adjusting processes.
  - Data gets lost in the system.
  - The existence 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.
  - 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 attendant reporting requirements and are beginning to follow the published governance process and guidance. Business areas can show the following:
  - All are subject to accreditation, as a matter of course.
  - Where appropriate, Privacy Impact Assessments are used and effective contract mechanisms are used to apply all through, and information life and risks have been identified for all accredited in information systems.

### Level 4: Embedding

#### Knowledge and Skills
- In addition to the above, staff are more aware of those risks owned by or shared with partners, and can confidently discuss this point with partners.
- Ensure the Department communicates effectively and that it is subject to risk the public which arise in their area.
- Formally review the effectiveness of all aspects of their risk activity management.
- Senior management, including the Board, is actively engaged in risk management and broadcasting their horizons on risk through communication 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 materialise during the planning cycle and allow matters accordingly.
- Our people and workforces are increasingly plugged in to their partners.
- Share risk information with delivery and other business partners. Where risks are owned by others we are ready to challenge if appropriate and for where there is an appetite to share and support.
- Risk workshops shared with partners. We are beginning to come more comfortable sharing with partners, whereas in the past we wouldn’t. Discussions about risk are becoming increasingly more mature and widespread (and this is evidenced in minutes and notes).
- Three discussions underpin the escalation process and form part of both the informal and formal escalation process.
- Executive Board can be seen to be giving direction in the oversight and management of risk.

#### Metric for measuring progress
- At level 3 above, but risks is being cascaded and less noticeable as a separate activity — can show how the board is the primary body. Key elements from level 3 that are strengthened here are:
  - Risk engaged and cascading through public bodies, suppliers, contractors, partners, projects, and programmes.
  - Risk discussion takes place, as regularly as the need dictates, throughout the organization.
  - Escalated and de-escalated risks will be found at all levels. There is no single model that is right, though evidence will be through analysis of the information system. An effective system will potentially have risk discussion in the minutes and be backed up with audit reports showing the movement of risk through the business areas.

### 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 can point to evidence that their business processes include risk management activity can be taken account of in the account and financial priorities for that coming year.)
- Business Continuity Planning is in place, as required, so that:
  - All units, directorates and groups — where appropriate — have workable, up to date and tested BC plans in place.
  - The Divisional BC Plan is in place on the test procedures to be implemented on its BC plan.
  - The Divisional BC Plan is in place on the test procedures to be implemented on its BC plan.

#### Managing process, and information asset, risks as well as project risks and risks to organizational Units:
- Where not assessed at Level 3 above, process risks have been identified and mitigating actions are in place.
- To project the means that business areas will be expected to outline their key business processes and the associated risks — Process 3 will assess 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 their organization has effectiveness information risk management processes in place to manage the residual risks and the related, systems IA risks. *NB In this instance, this has been taken to mean the residual risks identified by the Accreditation process. Level 1 HMIC All Bodies.

#### Health and Safety improvements are on track for the Health and Safety improvement programme. (This metric for individual business areas to be marked on, but via the HM Health and Safety Subsidiary, not via risk coordinator.)

#### Compliance with information security management systems requirements - BS 27002 (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.
## Risk Rationalities: RM Framework and Processes

<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>Environmental analysis</td>
<td>Internal and external context analysis</td>
<td>A detection of internal, environmental, and external factors that significantly impact the organization’s objectives, risks, and controls have not been identified or evaluated.</td>
<td>The organization has an internal context analysis that covers strategic, regulatory, and operational factors.</td>
<td>An internal and external context analysis has been developed and documented.</td>
<td>An internal and external context analysis has been implemented and evaluated.</td>
<td>The organization has an internal and external context analysis that includes all relevant factors.</td>
</tr>
<tr>
<td>Risk Identification</td>
<td>Risk assessment</td>
<td>A process that involves identifying potential risks and developing mitigation or contingency plans.</td>
<td>The risk assessment process involves identifying the risk, assessing the probability and impact, and developing mitigation or response plans.</td>
<td>A process that involves identifying the risk, assessing the probability and impact, and developing mitigation or response plans.</td>
<td>A process that involves identifying the risk, assessing the probability and impact, and developing mitigation or response plans.</td>
<td>The organization has a comprehensive risk assessment process that includes all relevant factors.</td>
</tr>
<tr>
<td>Risk Analysis &amp; Measurement</td>
<td>Risk Treatment</td>
<td>Identification or potential risks is not being adequately addressed.</td>
<td>The organization is implementing risk treatment strategies to address identified risks.</td>
<td>The organization is implementing risk treatment strategies to address identified risks.</td>
<td>The organization is implementing risk treatment strategies to address identified risks.</td>
<td>The organization has a comprehensive risk treatment strategy that includes all relevant factors.</td>
</tr>
<tr>
<td>Risk Based Control &amp; Audit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Risk Framework

- **Risk Philosophy**: The board does not understand the need for risk management.
- **Risk Strategy and Policy**: The risk management policy has not been identified or accepted.
- **Approach to Risk**: No RM approach to dealing with uncertainties.
- **Risk Management Leadership and Commitment**: Management is not committed to establishing a risk management framework and has not assumed a leadership role in implementing it.
- **Environmental Analysis**: The internal and external context analysis has not been planned or implemented in a structured way by a core group of managers.

### Risk Rationalities: RM Framework and Processes

- **Process Mapping**: An analysis concerning the organizational processes has been neither carried out nor planned.
- **Staff Risk Perception and Evaluation**: The organization lacks a systematic approach to risk perception and evaluation.
- **Risk Identification**: The risk identification process has not been implemented.
- **Risk Analysis & Measurement**: Risk registers may not be complete or up-to-date.
- **Risk Treatment**: Mitigation Actions/Contingency plans do not exist where they are needed.
- **Controls**: There are no criteria in place to evaluate whether risk management practices are effective and efficient.

### Multidimensional Analysis and Reading Grid: RM Maturity

- **Stage (Level 1)**: No proactive, though the organization is facing situations and risk issues after they occur and it is not able to distinguish between positive and negative risk.
- **Stage (Level 2)**: Risk is identified but the organization is not taking proactive measures to mitigate it.
- **Stage (Level 3)**: Risk is identified and the organization is taking proactive measures to mitigate it.
- **Stage (Level 4)**: Risk is identified and the organization is taking proactive measures to mitigate it effectively.
<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>Outcomes and deliverables</td>
<td>No evidence of improved outcomes</td>
<td>There is limited evidence that risk management is being effective in at least most relevant areas</td>
<td>There is evidence that risk management is supporting delivery of key outcomes in all relevant and key areas</td>
<td>There is clear evidence of very significantly improved delivery of all outcomes and showing positive and sustained improvement in RM processes, which are seen to be managed effectively. The organization is doing well at managing risk in most areas.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Impact on work and personnel</td>
<td>No impact on work and staff</td>
<td>Low impact on top / senior management culture with reference to awareness of priorities and attention to results</td>
<td>MADM and Low Management approach through which key strategic goals are pursued is being aligned. Human resources management policies related to key and relevant areas have improved.</td>
<td>Full understanding of performance impact. Communication processes inside the organization have significantly improved and the organization is doing well at managing risk in most areas.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Benefits on the organization as a whole</td>
<td>No impact on the organization</td>
<td>Some improvement of effectiveness related to some stand-alone processes</td>
<td>Key activities and quality of services in all relevant areas have improved and duplication in both activities and services have been removed</td>
<td>All ineffective / duplicated services and activities have been removed. All project and activity effectiveness and quality has improved. Strong sense of teamwork exists across the organization.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk management integration</td>
<td>Linkage to corporate and operational planning</td>
<td>Programs operate independently and have no common framework, classifying overlapping activities and inconsistencies</td>
<td>Risk Management is not linked with strategic/operational planning process.</td>
<td>Risk Management is done as part of strategic/operational planning process throughout the organization, but it is not consistent. Risk management policies are not aligned.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use of RM information in decision making</td>
<td>Risk management information is not used in the decision making process</td>
<td>Information retrieved from the risk management process is used to assess the level of risk and set a threshold for business units and managers.</td>
<td>Information retrieved from the risk management process is used to assess the level of risk and set a threshold for business units and managers.</td>
<td>Information retrieved from the risk management process is used to assess the level of risk and set a threshold for business units and managers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integration with quality framework</td>
<td>No connection</td>
<td>Programs for compliance, quality management, process improvement and RM must operate independently and have no common framework, classifying overlapping activities and inconsistencies</td>
<td>The functions are aligned but not completely integrated.</td>
<td>The functions are completely integrated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connection with performance assessment system</td>
<td>No connection</td>
<td>Performance in managing risks is a residual factor considered in the organization assessment system.</td>
<td>Performance in managing risks is a residual factor considered in the organization assessment system.</td>
<td>Performance in managing risks is a residual factor considered in the organization assessment system.</td>
<td></td>
</tr>
</tbody>
</table>

**Risk Rationale: RM Framework and Processes**

<table>
<thead>
<tr>
<th>READING KEYS</th>
<th>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>Monitoring &amp; Review</td>
<td>RM system Monitoring &amp; Review</td>
<td>Risk management system is not in place.</td>
<td>A risk management system is not in place.</td>
<td>A risk management system is not in place.</td>
<td>A risk management system is not in place.</td>
</tr>
<tr>
<td></td>
<td>RM system Monitoring &amp; Review</td>
<td>A risk management system is not in place.</td>
<td>Periodic reviews to ensure that risk management system is effective and continue to support organizational performance is not envisaged.</td>
<td>Periodic reviews to ensure that risk management system is effective and continue to support organizational performance is not envisaged.</td>
<td>Periodic reviews to ensure that risk management system is effective and continue to support organizational performance is not envisaged.</td>
<td>Periodic reviews to ensure that risk management system is effective and continue to support organizational performance is not envisaged.</td>
</tr>
<tr>
<td></td>
<td>RM System in the Organization</td>
<td>The board does not feel the need to manage risk and the related function is not included in the organizational chart.</td>
<td>Top management / senior managers take the lead to ensure that a non-formal system is in place.</td>
<td>Top management / senior managers take the lead to ensure that a non-formal system is in place.</td>
<td>Top management / senior managers take the lead to ensure that a non-formal system is in place.</td>
<td>Top management / senior managers take the lead to ensure that a non-formal system is in place.</td>
</tr>
<tr>
<td></td>
<td>RM Internal culture</td>
<td>The focus is primarily on responding to crises and is reactive rather than proactive.</td>
<td>People tend to be risk-adverse: caution approach is taken to risk management overall (risk avoidance).</td>
<td>People tend to be risk-adverse: cautious approach is taken to risk management overall (risk avoidance).</td>
<td>People tend to be risk-adverse: cautious approach is taken to risk management overall (risk avoidance).</td>
<td>People tend to be risk-adverse: cautious approach is taken to risk management overall (risk avoidance).</td>
</tr>
<tr>
<td></td>
<td>Linkage to ethics and codes of practice</td>
<td>No ethics policy or guidelines in place. No direct statements of shared values or principles or attention to legal issues</td>
<td>Ethics policies and codes of practice are not aligned to the risk management process.</td>
<td>Ethics policies and codes of practice are not aligned to the risk management process.</td>
<td>Ethics policies and codes of practice are not aligned to the risk management process.</td>
<td>Ethics policies and codes of practice are not aligned to the risk management process.</td>
</tr>
<tr>
<td></td>
<td>Stakeholders</td>
<td>Stakeholders have been identified, but there is no formal communication or understanding of their information needs and/or risk tolerances</td>
<td>Communication with stakeholders is ad hoc and there is some understanding of their information needs and risk tolerances.</td>
<td>Communication with stakeholders is ad hoc and there is some understanding of their information needs and risk tolerances.</td>
<td>Communication with stakeholders is ad hoc and there is some understanding of their information needs and risk tolerances.</td>
<td>Communication with stakeholders is ad hoc and there is some understanding of their information needs and risk tolerances.</td>
</tr>
</tbody>
</table>

**Uncertainty Experts, People, Roles, Structures and Interactions**

<table>
<thead>
<tr>
<th>READING KEYS</th>
<th>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>RM Maturity in the Organization</td>
<td>The board does not feel the need to manage risk and the related function is not included in the organizational chart.</td>
<td>Top management / senior managers take the lead to ensure that a non-formal system is in place.</td>
<td>Top management / senior managers take the lead to ensure that a non-formal system is in place.</td>
<td>Top management / senior managers take the lead to ensure that a non-formal system is in place.</td>
<td>Top management / senior managers take the lead to ensure that a non-formal system is in place.</td>
</tr>
<tr>
<td></td>
<td>RM Culture</td>
<td>The focus is primarily on responding to crises and is reactive rather than proactive.</td>
<td>People tend to be risk-adverse: cautious approach is taken to risk management overall (risk avoidance).</td>
<td>People tend to be risk-adverse: cautious approach is taken to risk management overall (risk avoidance).</td>
<td>People tend to be risk-adverse: cautious approach is taken to risk management overall (risk avoidance).</td>
<td>People tend to be risk-adverse: cautious approach is taken to risk management overall (risk avoidance).</td>
</tr>
<tr>
<td></td>
<td>Ethical and Code of Practice</td>
<td>No ethics policy or guidelines in place. No direct statements of shared values or principles or attention to legal issues</td>
<td>Ethics policies and codes of practice are not aligned to the risk management process.</td>
<td>Ethics policies and codes of practice are not aligned to the risk management process.</td>
<td>Ethics policies and codes of practice are not aligned to the risk management process.</td>
<td>Ethics policies and codes of practice are not aligned to the risk management process.</td>
</tr>
<tr>
<td></td>
<td>Stakeholders</td>
<td>Stakeholders have been identified, but there is no formal communication or understanding of their information needs and/or risk tolerances</td>
<td>Communication with stakeholders is ad hoc and there is some understanding of their information needs and risk tolerances.</td>
<td>Communication with stakeholders is ad hoc and there is some understanding of their information needs and risk tolerances.</td>
<td>Communication with stakeholders is ad hoc and there is some understanding of their information needs and risk tolerances.</td>
<td>Communication with stakeholders is ad hoc and there is some understanding of their information needs and risk tolerances.</td>
</tr>
</tbody>
</table>
### Uncertainty: Experts, People, Roles, Structures, and Interactions

<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>
<th>Attributes / Performance indicators</th>
<th>Attributes / Performance indicators</th>
<th>Attributes / Performance indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Roles &amp; responsibilities of senior management</td>
<td>Corporate culture has no risk management accountability with process owners not defined</td>
<td>Staff accountability</td>
<td>Staff culture has little risk management accountability</td>
<td>Risk management responsibilities are formally stated in accountability agreements and/or governance documents and are communicated, applied, and evaluated at all levels of organizations</td>
<td>A formal process is in place whereby senior management assumes responsibility for the overall risk management strategy. Risks are identified by the management team and top-level reviews are conducted to ensure the strategy is effectively implemented.</td>
<td>A formal process is in place whereby senior management assumes responsibility for the overall risk management strategy. Risks are identified by the management team and top-level reviews are conducted to ensure the strategy is effectively implemented.</td>
<td>The management of risk is everyone’s responsibility</td>
<td>The allocation of suitable human resources for managing risks is systematically considered in the organization's operating budget and staffing plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human resources adequacy</td>
<td>No resources are envisaged to implement a RM system</td>
<td>Specialist support</td>
<td>Specialists are not available</td>
<td>An integrated and multidisciplinary center of excellence exists for risk management. There is a clear identification of risks, uncertainties, and functional risk issues and these are recognized externally.</td>
<td>That no key risks are overlooked. Merlinian/policy papers, methodological documents and information resulted from the RM system are disseminated. Clear communication protocols are in place at ensuring there is a clear understanding of the responsibilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal communication strategy</td>
<td>No internal communication flows about risk</td>
<td>Inter-RM information system</td>
<td>A specific pilot RM information system is being implemented as a part of other information systems</td>
<td>The management of risk is everyone’s responsibility</td>
<td>Each stage of the risk management process is tracked in a Web-based tool that is integrated with other corporate information systems.</td>
<td>The allocation of suitable human resources for managing risks is systematically considered in the organization's operating budget and staffing plan</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document management</td>
<td>Document management</td>
<td>Risk identification</td>
<td>The effects of risk events might be identified but not associated with their process sources</td>
<td>The organization establishes internal reporting mechanisms in order to support and encourage accountability and ownership of risk: internal reporting provides general information to interested internal audiences on the risk management processes in all key and relevant areas, without unnecessary detail</td>
<td>The management of risk is everyone’s responsibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Technologies, Support

<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>
<th>Attributes / Performance indicators</th>
<th>Attributes / Performance indicators</th>
<th>Attributes / Performance indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment</td>
<td>Managers tend to use their own individual approach, based on personal experience</td>
<td>Risk identification</td>
<td>The effects of risk events might be identified but not associated with their process sources</td>
<td>The organization establishes internal reporting mechanisms in order to support and encourage accountability and ownership of risk: internal reporting provides general information to interested internal audiences on the risk management processes in all key and relevant areas, without unnecessary detail</td>
<td>The management of risk is everyone’s responsibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk management tools &amp; techniques</td>
<td>New RM tools have been envisaged</td>
<td>Internal reporting &amp; reporting</td>
<td>Information about risk is not reported and used as a basis for decision making</td>
<td>Comprehensive and periodic internal reporting on both significant risks and risk management processes is provided regularly, at both executive (board of directors) and operational level (management). It contributes to strategic oversight, decision-making and improved operational decisions. Reliability and detail of risk information has significantly increased</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting system</td>
<td>Information about risk is not reported and used as a basis for decision making</td>
<td>Risk management</td>
<td>The organization establishes internal reporting mechanisms in order to support and encourage accountability and ownership of risk: internal reporting provides general information to interested internal audiences on the risk management processes in all key and relevant areas, without unnecessary detail</td>
<td>Risk management tools &amp; techniques are integrated with departmental management tools and techniques. Tools and models are assessed on a periodic basis and updated based on most relevant technology</td>
<td>The management of risk is everyone’s responsibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting system</td>
<td>Information about risk is not reported and used as a basis for decision making</td>
<td>External reporting</td>
<td>There might be some ad hoc reports provided on specific external request (e.g., public bodies, users of statistical information through citizen associations, media) about the effects of risk on disputed events after they have occurred or not</td>
<td>The management of risk is everyone’s responsibility</td>
<td>The management of risk is everyone’s responsibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reporting system</td>
<td>External reporting</td>
<td>Risk management tools &amp; techniques</td>
<td>New RM tools have been envisaged</td>
<td>The organization establishes internal reporting mechanisms in order to support and encourage accountability and ownership of risk: internal reporting provides general information to interested internal audiences on the risk management processes in all key and relevant areas, without unnecessary detail</td>
<td>The management of risk is everyone’s responsibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Training system

<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>
<th>Attributes / Performance indicators</th>
<th>Attributes / Performance indicators</th>
<th>Attributes / Performance indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td>RM Training and people’s competence</td>
<td>RM training program and activities are not envisaged. No understanding of risk principles or language. No information on RM competency requirements.</td>
<td>RM training and people’s competence</td>
<td>RM training and people’s competence</td>
<td>RM training and people’s competence</td>
<td>RM training and people’s competence</td>
<td>RM training and people’s competence</td>
<td>RM training and people’s competence</td>
<td>RM training and people’s competence</td>
<td>RM training and people’s competence</td>
<td>RM training and people’s competence</td>
</tr>
<tr>
<td>DESCRIPTORS</td>
<td>STAGE (LEVEL 1)</td>
<td>STAGE (LEVEL 2)</td>
<td>STAGE (LEVEL 3)</td>
<td>STAGE (LEVEL 4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<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</td>
<td>An Internal Communication plan and a team responsible for communicating about</td>
<td>Adequate and efficient communication plan and tools to share RM knowledge,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>have been implemented (e.g., knowledge sharing systems such as wiki platforms,</td>
<td>organization’s policy and ownership have been defined. Meetings with the</td>
<td>information and practices with all internal stakeholders; and to promote</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>sharepoint sites)</td>
<td>organizational divisions involved are organized. Other tools to share RM</td>
<td>co-operation and dialogue are in place (e.g., regular internal meetings,</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>information are face-to-face discussion, Reid delivering sessions</td>
<td>workshops and seminars, web info sessions, internet site regularly updated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>about RM issues, RM newsletter, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RM external communication instruments and tools</td>
<td>No specific external means for communicating about risk are envisaged</td>
<td>Some external tools to share knowledge among a core group of selected stakeholders about risk may be used</td>
<td>Specific external tools to communicate with stakeholders about how the</td>
<td>Adequate plan and tools to communicate with all external stakeholders and to promote co-operation and dialogue are in place (e.g., annual meetings, annual report, workshops and seminars, internet site regularly updated about RM issues, RM newsletter, etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Resources</td>
<td>No resources are envisaged to implement a RM system</td>
<td>Financial resources made available to manage risk are very 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 organisation’s risk framework and a budget to iron specific risks relating to key and relevant areas</td>
<td>The allocation of suitable resources for managing risk is systematically considered in the organisation’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>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>