The different business objectives and the specific structure of any organization prevent the possibility of adopting a single monolithic enterprise risk monitoring process suitable to control all its operations. Starting from the resources involved and the basic actions performed by each internal process, it is possible to correlate them with the rules (concerning procedures and processes) issued to pursue the business strategy (alignment to objectives). The organizational structure is the glue that keeps fluid relationships between the processes (communication), improves the implementation level of the rules (operations) and permits to measure the effectiveness of the actions (controls). The risk is a function depending on the ability to manage all these variables.

Here, a two-step approach is proposed to manage the enterprise risk. The first step is the bottom-up implementation of a practical method to face the treatment of the operative risk. The second step is the management of the overall risk (strategic included), under the perspective of different frameworks, by the measurement of the maturity level. This involves the adoption of a suitable internal control framework and the search for key actions that heavily impact the business objectives (top-down).

The first method/tool is finalized to issue a risk treatment plan (RTP)\(^1\) with all the details necessary to meet the needs of the operations. This is the final document of a process, starting with establishing the context, scope and the risk evaluation criteria. Then, for each resource (e.g., asset, process), any risk having an impact on the business objectives is identified, analyzed and evaluated. Finally, all is summarized in a plan, the RTP, with the activities (e.g., controls, countermeasures) implemented to mitigate the identified risk. This plan complies with the requirements of the International Organization for Standardization (ISO) concerning risk assessment and treatment.

The second method/tool is undertaken to manage the enterprise risk assessment (ERA) as the basis for all the high-level risk frameworks adopted. This is the process to evaluate the level of implementation of the internal rules (maturity) and the chance that something negative may happen. This information is automatically transformed in a risk evaluation at any level of the organization. Considering all the rules established in the organization and, putting these in relationship with the risk framework checklists, the level of the risk for any relevant resource affected by the rules enforced is easily assessed under the various perspectives of control.

The RTP is recommended for the management of the operative risk to provide an analytic approach with a high level of detail. The ERA, on the other hand, is intended to build an executive scenario for

---

Has been the risk monitoring manager at Magneti Marelli for more than four years. Previously, he was responsible for information and communications technology operations and resources in the APAC region (China, Japan, Malaysia) and, before that, was the worldwide information security officer for more than seven years. For internal risk monitoring, he developed the described methodology, merging an operative risk analysis with a consequent risk assessment driven by the maturity level of the processes. Also, he designed the cybermonitoring tool. Sbriz was also a consultant for business intelligence systems for several years. He can be contacted directly at https://it.linkedin.com/in/luigisbriz or his current contact information can be found at http://sbriz.tel.

© 2019 ISACA. All rights reserved. www.isaca.org
top management with a qualitative approach and a synthetic view of the phenomena under analysis. It is a modular solution but, if both are used, integration is possible using the outcomes of RTP as input for ERA, reducing the overall need for data entry. Here, in part one of this two-part series, the first method described is aimed only at operational risk.

Organizational Structure

Starting from zero, a good way to define an organizational structure suitable to govern risk monitoring is the merger of all the organizational structures built for the monitoring/reporting systems of the internal processes or departments. This permits the identification of the minimal significant entity able to make decisions or transform products or manage resources. Where there is a source of decisions, it is necessary to include an analysis node for the risk monitoring system.

An entity is the basic organization unit used for the monitoring of business performance. Typically, it is the intersection of product family, legal entity and location, which enables at least a consolidation of business, geographic or legal aspects. For example, in a large organization with multiple locations, it is quite easy to define the location of a plant or a logistics warehouse or a research and development center or a shopping center as a basic decision-making unit of the organization.

A feature of the entity is its ability to make its own decisions and, thus, to impact the business objectives. It is characterized by its own internal organization with its own objectives. This organization must have identified the position accountable for achieving the entity objectives (e.g., a local general manager); one or more risk analysts (e.g., process leaders, personnel leading ISO certification processes or internal controllers); and team leaders to govern the projects, tasks, actions or activities.

In addition, to complete the organizational structure, two other factors have to be managed in the risk monitoring system:

- **Departments**—Internal functions having accountability over one or more processes

- **Roles**—Positions established to govern and manage the organization and its parts

With this information, it is possible to issue a responsible, accountable, supportive, consultive, informed (RASCI) matrix to clarify how the game is played (figure 1). A syntactical organization requires a minimum of four categories of players (roles).

The main role is the risk assessor in charge of either the coordination of the risk assessment for the site or the risk analysis for the local certification schema. The resources’ owners are involved by the risk assessor in the self-assessment process or in the risk treatment plan issuing. The risk certifier is any position having charge of the consistency control of the assessments at the department level for a product family or for a geographical area. The risk manager is appointed at the headquarters level to organize the risk management process and to perform the onsite audits.

Establishing the Context

Before starting the process, the entity should establish its context in relationship to the expected objectives, its known issues and its ability to achieve the intended outcomes of its management system(s). Three sets of information and action are needed to meet these purposes:

1. Describe the enterprise mission, values and processes, and identify internal and external issues influencing its objectives.
2. Select the interested parties and identify their needs and expectations.
3. Define the boundaries of the management systems and the applicability of the requirements considered in the analysis.

A three-part form enables the required information to be gathered. An example of a web page screenshot is shown in figure 2.

The first and third columns ("context" and "scope") are text fields proposed to be filled in with a predefined narrative (precompiled template of text) with the topics that will have to be personalized. The usage of this template of text in the data entry allows users to easily fill in the forms without
Roles, Responsibilities and Their Interactions

<table>
<thead>
<tr>
<th>Responsibilities</th>
<th>Risk Manager</th>
<th>Risk Certifier</th>
<th>Risk Assessor</th>
<th>Resources' Owner</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk frameworks management</td>
<td>A / R</td>
<td>C</td>
<td>I</td>
<td></td>
<td>Risk process organization; methodological addressing; framework change management</td>
</tr>
<tr>
<td>Organization structure updating</td>
<td>S</td>
<td>A / R</td>
<td>I</td>
<td></td>
<td>Entity organization management; intrinsic value management</td>
</tr>
<tr>
<td>Performing risk self-assessment</td>
<td>C</td>
<td>C</td>
<td>A</td>
<td>R</td>
<td>Performing the local risk self-assessment of the ERA checklist</td>
</tr>
<tr>
<td>Remediation plan implementation</td>
<td>I</td>
<td>S</td>
<td>A</td>
<td></td>
<td>Implementation of the remediation plan; application of any corrective action</td>
</tr>
<tr>
<td>Risk assessment monitoring</td>
<td>A / R</td>
<td>S</td>
<td>S</td>
<td>S</td>
<td>Consistency checking of the risk assessment process; system control; check on the deadlines</td>
</tr>
<tr>
<td>Risk assessment checking</td>
<td>C</td>
<td>A / R</td>
<td>S</td>
<td>S</td>
<td>Offline checking of the assessed statements with remote interviews and documentary analysis</td>
</tr>
<tr>
<td>Risk assessment auditing</td>
<td>A / R</td>
<td>I</td>
<td>S</td>
<td>S</td>
<td>Onsite auditing of the assessed statements with interviews, observations and independent tests</td>
</tr>
</tbody>
</table>

Responsible—Person who carries out the project/task
Accountable—Person who is ultimately accountable for the process/project being completed appropriately
Supportive—Person who provides resources or plays a supporting role in implementation
Consulted—Person who provides information and/or expertise necessary to complete the project
Informed—Person who needs to be notified of results but needs not necessarily be consulted

The business context is completed by a strengths weaknesses opportunities threats (SWOT) analysis

Forgetting relevant topics. The central column, “interested parties,” is managed by a helper (pop-up form with a standard catalog of interested parties) enabled to the selection and change (figure 3) of a typology (generic interested party) to issue a customized interested party. Each customized item is well coded to be able to correlate the single interested party with a dedicated risk profile for a subsequent automatic evaluation of its severity (weight) during the risk calculation. The profile is hidden to the end user, and it is used only by the processing and consolidation algorithm. It is then named and changed with the narrative proposed by the system to easily describe it and declare its relevance.
to emphasize the critical factors for the achievement of the business objectives (figure 4). The technique used to build the four lists (catalogs) of SWOT, at the entity level, is the same as that used for the interested parties. From each catalog, the items included are selected from standard typologies (template) and then customized. Each typology selected is automatically coded and kept linked with the original typology to allow constant access to its profile (set of attributes useful for calculation reasons). The profile allows the use of personalized weighting during the calculations to identify its nature (and, therefore, how to manage it) and build the network of relations with the enterprise risk assessment (ERA) tool described in the second part of this article.

Consider the following example to understand the need to always keep the relationships between categories and custom objects. Suppose the W7.1 code is the category weakness of the loss or disclosure of generic personally identifiable information (PII). The related selected and customized item W7.1.1 will be in consequence identified as a potential issue regarding a privacy data breach. So, if the privacy ISO/IEC 29134:2017 standard was adopted, a privacy impact assessment (PIA) could be automatically built, collecting all the custom objects having a link with the selected category PII and, in case of greater severity, also include the items classified as sensitive personal identifiable information (SPII) identified by the code class W7.2.

Of course, other kinds of information must be considered before analyzing the risk to resources and their activities. The resource-activity pair is the basic item on which to finalize the risk analysis. Before starting, the elements used to describe the environment will have to be encoded in some catalogs to reduce the typos or inconsistencies during their reuse. Specific lists must be managed for:

- Departments or equivalent organizational units accountable for one or more processes or assets
- Roles equivalent to accountable positions into the organizational charts
- Human resources (HR) involved in the management of the activities finalized to protect/manage the resources
- Activities (i.e., controls, countermeasures, actions) in place or planned to contrast the risk affecting the resources
- Resources (i.e., assets, processes, competencies) having impact on the business objectives that need specific actions for their protection

There are some considerations about the following catalogs. Human resources (figure 5) are linked at least to a department and to an internal position (role) to demonstrate the organization's commitment and qualify the eligibility to maintain leadership to manage the assigned task. The catalog is used primarily to identify people having accountability in some process (key user), and this means reducing the list size and probably even occasionally changing it. There are two categories
of key users: the risk owners, i.e., individuals accountable and able to analyze the risk factors and treat them, and the task managers who will have the accountability to lead an action/activity following a plan.

The activities (figure 6), also called controls, countermeasures, tasks or actions, have a dual significance and may be either an operation required by the process for its execution or a mitigation control to reduce potential risk to a resource. An activity is always linked to a responsible party (selected from the catalog of the human resources) and evaluated in terms of the

---

Figure 4–SWOT Analysis

<table>
<thead>
<tr>
<th>SWOT</th>
<th>Helpful to achieving the objective</th>
<th>Harmful to achieving the objective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STRENGTHS:</strong> activities that could be useful in achieving the objectives. We can control these things that are good now. The expectation is to implement a process of continuous improvement.</td>
<td><strong>WEAKNESSES:</strong> activities that might hinder the achievement of the objectives. We can control these things that are bad now. The need is to strengthen all the processes involved.</td>
<td></td>
</tr>
<tr>
<td>S1.1 Our values: Our mission, vision and values declared in our policies and well communicated to all the interested parties.</td>
<td>W1.1 KPI misaligned with objectives: Misalignment of procedures with business objectives or customers’ retirements</td>
<td></td>
</tr>
<tr>
<td>S4.1 Governance: Governance organization and policies aligned to the best standards and practices</td>
<td>W2.1 Loss of information: Loss of information or unauthorized access or unauthorized disclosure of information</td>
<td></td>
</tr>
<tr>
<td>S5.2 Internal organization: The code of conduct and procedures are spread to all interested individuals after a training session</td>
<td>W3.1 Process improvement: Training program misaligned with business objectives</td>
<td></td>
</tr>
<tr>
<td>S6.1 Technology by process: Methodologies continually updated; knowledge aligned with best practices, fast product development</td>
<td>W4.1 Customer care: Inability to manage customer demand and its expectations</td>
<td></td>
</tr>
<tr>
<td>S6.2 University relationships: University</td>
<td>W5.1 Performance: Technologies or machineries or equipments not aligned to business objectives</td>
<td></td>
</tr>
<tr>
<td>S7.1 Procedures: Widespread use of KPIs in all of the company processes with continual monitoring, analysis and improvement</td>
<td>W7.1 Loss or disclosure of SPI: Loss or disclosure of Sensitive Personal Information</td>
<td></td>
</tr>
<tr>
<td>S8.1 Innovation: R&amp;D centers spread on all the production countries</td>
<td>W7.2 Loss or disclosure of PII: Loss or disclosure of Personally Identifiable Information</td>
<td></td>
</tr>
<tr>
<td>S9.1 Employees: Employees’ competence and motivations (employees satisfaction checked)</td>
<td>W8.1 Competitors analysis: Analysis of competition is not adequate to correctly measure the performance of our competitors in the market</td>
<td></td>
</tr>
</tbody>
</table>

---

Figure 5–Risk Owners and Task Managers

Risk Owners and Task Managers registry

<table>
<thead>
<tr>
<th>Department</th>
<th>Responsible name</th>
<th>Role</th>
<th>Risk Owner</th>
<th>Task Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>EH&amp;S</td>
<td>Here name of EHS manager</td>
<td>EH&amp;S manager</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Finance</td>
<td>Here name of CFO</td>
<td>CFO</td>
<td>✓</td>
<td>×</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Here name of HR manager</td>
<td>HR manager</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ICT</td>
<td>Here name of ICT manager</td>
<td>ICT manager</td>
<td>✓</td>
<td>×</td>
</tr>
</tbody>
</table>
progression of the work and the risk of not being able to complete it. A new activity can be included either as duplication of an already existing one (fast and easy) or selecting a new one from the standard catalog of activities. The standard catalog includes generic activities already preconfigured for an easy customization, and it is linked to a hidden risk profile to automatically manage its severity in the risk evaluation.

The business resources (figure 7) are any asset or process or competence to which impairment or misuse might affect the achievement of business objectives. The resource is described in terms of a name and description, an owner department to place it in its position within the organization, its list of critical issues (selected from the catalog of its SWOT), an eventual definition of a maximum tolerable downtime (MTD) or recovery point objective (RPO)\(^5\) (if the resource is impacted by the continuity management), the reference to a procedure describing its handling, and its interested parties list. New resources are inserted from a duplication of an already existing one or selection of a new one from the standard catalog of resources. The standard catalog is analogous to that of the activities; every referenced resource is linked to its specific risk profile to properly customize the risk evaluation.

Risk Analysis and Treatment

The risk analysis, evaluation and treatment are carried out in a single form combining a resource with its set of potential issues (its personal SWOT), its interested parties, the eventual continuity parameters (MTD, RPO), its controls and already-set countermeasures. Each row in figure 8 represents one risk (pair made of a resource with a set of issues).

The overall process to assess and treat a specific risk for a resource is summarized in the following steps:

1. Customize the SWOT list inherited from the resources master file to better identify the specific potential risk represented in the row.
2. Select relevant controls/countermeasures from the activities list. The system automatically splits the list in current controls if the activity status is completed, or otherwise, if not, in countermeasures column.
3. Define the eventual target for the confidentiality, integrity and availability (triple CIA) of data or availability only for a service, or otherwise the security baseline levels (default) will be selected.
4. Complete first evaluation of the impact and likelihood considering only the already completed activities.
5. Complete second evaluation of the impact and likelihood considering also the countermeasures as completed. The aim is to reach the status of acceptable risk, eventually adding new actions (countermeasures) to contrast the potential risk.

6. Optionally add a clear description of the consequences (outcomes of events affecting business objectives) and an explanation of the impacts of residual risk.

7. Identify the risk owner accountable to monitor the risk evolution by selecting the name from the human resources master file.

8. Eventually customize the interested parties involved in this risk and automatically derived from the resource master file.

Management Review

With the risk analysis and treatment completed, the data entry is nearly finished. One last piece of information required is the updating of the executive summary of the works carried out since the last analysis provided by the risk assessors. General considerations about potential risk and severity are inserted in the risk assessor summary to focus the attention of top management on these factors (figure 9).

When the report is presented to top management for approval, a cover sheet as a meeting note is automatically added to summarize the critical resources, which includes resources with relevant risk and also the countermeasures relating to critical issues.

The management review continues by entering the addresses to prioritize the actions, and it is concluded by approving the analysis, the evaluation and the consequent plan (figure 10). During the discussion, at any time, it is possible to directly edit any previous form and get the cover immediately updated. After approval, the plan is then automatically frozen and it is issued a reference number to identify it. The history of the last five plans' revisions is retained for possible comparisons.
Also, with the approval, the system prepares the data entry for a new plan review, keeping the current analysis and allowing its change. The cycle can restart from any previous step: review an action, a risk, the list of the resources, change a task and so on. People can do what they need and in the sequence they want.

Documents Issued

Approving the RTP, two documents are immediately ready to be issued: an overall report including the comprehensive risk analysis and the subsequent RTP and a detailed snapshot of a single risk on a page called risk card. The RTP report uses a few sections (a tab for each card) to divide and organize all the information, as shown in figure 11.

The following is a brief description of the tabs available:

- **RTP cover**—Synthetically exposes the critical resources and activities with the risk assessors and the management addresses. The history completes the cover.

- **Establishing the context**—Summarizes the mission and vision of the business, the internal and external risk factors, and the interested parties, and defines the boundaries of the management systems. The SWOT analysis provides the list of the issues, helpful or harmful, internal or external, that can affect the business objectives.

- **Risk criteria**—Provides the standard risk matrix adopted and its variations, automatically utilized, if there are confidentiality, integrity, availability objectives above or below the baseline.

- **Privacy impact assessment**—Provides the risk analysis of the resources having an issue linked with privacy. It is made up of resources with an issue (weakness) such as PII or SPI, and it is aligned to the requirements of ISO/IEC 29134:2017 and GDPR.

- **Business impact analysis (BIA)**—Provides the risk analysis of the resources having an issue linked with continuity of the data system. It is made up of resources having a declaration of MTD or RPO below the maximum selectable.

- **Risk treatment plan**—Provides the risk analysis of the resources without any issue relating to privacy or continuity of the data system (separately described). It is made up of all the resources not already included in PIA and BIA tabs.

This document shows only the latest review issued. Reviewing is a cyclical task with a frequency aligned at a minimum to the reviewing cycle of the business objectives or immediately after an incident or to prepare for a significant change. A feature of the review is the possibility to close it only if all the risk factors are in a status of acceptable, otherwise the new version will not be issued. Part two of this series will show how to reuse these outcomes (and other data) to feed a different methodology to monitor the enterprise risk.
Endnotes


2 McCallister, E.; T. Grance; K. Scarfone; Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), National Institute of Standards and Technology, USA, April 2010

3 Op cit ISO/IEC

4 Northeastern University, “What is Sensitive Personal Identifying Information (PII)?” USA, https://www.northeastern.edu/securenu/sensitive-information-2/sensitive-information/


6 Ibid.