Risk Management in Istat: from the project to the process
Management System Network

- Values and ethics
- Organizational culture
- Effectiveness and efficiency
- Leadership and relationship
- Quality and integrity of data

Methods and procedures standardization supporting changes

Staff and Organization Assessment

Quality Analysis & Process Management

Change Management

Performance Evaluation

Planning & Control

ICT

Audit & ICT Governance

Risk Management

Internal Audit

ICT

Training & Communication

Governance

Internal Audit

Control Systems Checks

Organizational culture

No overlapping !!

☑ Quality of services and products

☑ Supporting decision-making processes

☑ Enhancement of transparency
Risk Management approach in ISTAT

**OBJECTIVES**
- Setting up objectives
- Selection of priorities
- Objectives/processes

**PROCESSES**
- Process mapping
- Economic value
- Process objectives

**RISKS**
- Risk analysis
- Risk assessment
- Risk treatment

**CONTROLS**
- Controls in processes
- Controls/objectives vulnerabilities
- Control assessment

**LEVEL OF RISKS IN PROCESSES**

**INTERNAL CONTROL RELIABILITY**

**RESPONSE ACTIONS**

**MONITORING**

“BASE” Approach
“ADVANCED” Approach
“PRO” Approach
Risk Management System in Istat: from the project to the process

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Project launched</td>
<td>Approach trial</td>
<td>Experimental phase</td>
<td>Experimental phase</td>
<td>Full implementation</td>
<td>Developments</td>
</tr>
<tr>
<td>• Analysis and comparison of practices and models</td>
<td>• Survey on Risk perception</td>
<td>• Creation of risk registers</td>
<td>• Revision of risk registers</td>
<td>• Integration w/ operational planning</td>
<td></td>
</tr>
<tr>
<td>• Identification of appropriate approach</td>
<td>• Pilot and rollout of risk management approach</td>
<td>• Risk assessment</td>
<td>• Identification of risk treatments</td>
<td>• Risk treatment monitoring</td>
<td></td>
</tr>
<tr>
<td>• Establishing ISTAT’s RM model</td>
<td>• RM training and dissemination</td>
<td>• RM training and dissemination</td>
<td>• RM training and dissemination</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The project developed following some parallel but related paths:

1. **Organization**: Both the President and the Directorate General endorsed and sponsored the project. A business unit was involved in implementing and coordinating risk management system.

2. **Training and dissemination** program in order to improve management culture and promote a common language and understanding throughout the organization.

3. **All Risk Management process has been implemented**

4. **Information System has been developed to support the process**

5. **Change of perspective**: Bottom-up/Top-down mixed approach
Risk Management System architecture in Istat

Risk Definitions and Standards used in Istat’s RM system

Among the others (more than 60!), Istat selected:

- **ISO 31000:2009**: Risk Management Principles and Guidelines
- **ISO/IEC 31010:2009**: Risk assessment techniques
- **COSO Model 2004/2013**, a multidimensional standard that develops along three sides of the cube: 1) **Objectives**; 2) **Organization**; 3) **Process**.

The selected Model defines:

- **Enterprise Risk Management** “... a process effected by an entity’s board of directors and management, applied in strategy setting and across the enterprise, designed to **identify potential events** that may affect the entity, and **manage risk** to be within its **risk appetite**, to provide **reasonable assurance** regarding the **achievement** of entity objectives.”

- **Risk**: “the effect of uncertainty on objectives, where an effect is a deviation from what is expected (positive and/or negative), often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence”.
Risk Profile and Risk Complexity

**Risk Profile** is the set of risks that could affect all or part of an organization. It results from a comprehensive process that: concerns risk information from several sources; reflects recommendations from managers; envisages a risk questionnaire, revised guidelines, clearer definitions of risk sources and communication strategy.

**Risk Profile** takes into account:

- **Risk Appetite**, which could be expressed either qualitatively or quantitatively, maybe in terms of ranges, and explored going through the impacts of past events and the reactions of key stakeholders (customers, employees, regulators, ..).

- **Risk Attitude** (Existing Risk Profile). If an organization is particularly effective in managing certain types of risks, it may be willing to take on more risk in that category, conversely, it may not have any appetite in that area.

- **Risk Acceptance**, which refers to the maximum potential impact of a risk event that an organization could withstand. Often, appetite will be well below acceptance.

- **Risk Perception**, which describes how people perceive risks according to their values and interests

- **Risk Tolerance**, which is the level of variation that the entity is willing to accept around specific objectives.

- **Risk Retention** considers stakeholders’ conservative return expectations and a very low appetite for risk-taking.
Step 1: Survey on Risk perception

Istat launched a survey on risk perception involving Top and Executive Managers, carried out through a questionnaire:

- composed of about 70 questions and divided into four sections:
  1. **Internal control environment** and organizational culture;
  2. **Objectives** of the organization and Risk Management;
  3. **Identification and classification** of risk factors;
  4. "Cataloging" risks

- investigating four dimensions:
  1. the risk perception compared to the activities of each manager;
  2. the risk perception in the Institute as a whole;
  3. the maturity of the control environment in the structure leaded by each manager;
  4. the maturity of the control environment in the Institute as a whole
Step 2: Risk Identification

Organizational Risks have been identified using a Framework representing: activities, descriptions, impacts and proposals of treatment.

To describe risks some criteria have been taken into account:

- Risks must be linked to the objectives
- Pay attention to the risks with generic impact on the objectives, but not relevant for the results
- In identifying the risks, do not confuse them with the impacts
- Avoid defining risks with assertions that are only the opposite of the objectives
- The definition of a risk should understand the cause and consequences

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Uncertain organisational factor that, if it occurs, prevents the accomplishment of results</td>
</tr>
<tr>
<td>Criticality</td>
<td>Real hindering event that determines an actual situation of management inefficiency and/or operational</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preventive action</td>
<td>Action finalised to prevent the possible occurrence of a critical event, or to eliminate or reduce the damaging effects before they occur</td>
</tr>
<tr>
<td>Subsequent action</td>
<td>Action aimed at removing or reducing the effects of the damaging event, after its occurrence</td>
</tr>
<tr>
<td>Improvement action</td>
<td>Remedial action responding to a critical event that produce problematic situations or negative effects on the organization</td>
</tr>
</tbody>
</table>
## Istat’s Risk Register

### Examples of risk register pertaining to "Organization":

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk</th>
<th>Effect</th>
<th>Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Failure to observe the measures of personal data protection</td>
<td>Inadequate levels of security in data access</td>
<td>Training; Plan of monitoring compliance with the provisions for the protection of personal data processing</td>
</tr>
<tr>
<td>Resources</td>
<td>Access by unauthorized personnel (internal and external) to the data processing center and the network of the Institute</td>
<td>Possible alteration or tampering of computer equipment by unauthorized personnel</td>
<td>Introduction of a registration process of physical access to the operating rooms; Dissemination of safety instructions and procedures that must be followed in an emergency within the operating rooms; Monitoring and updating access rights.</td>
</tr>
<tr>
<td>Organization</td>
<td>Process steps too dependent on the skills owned by only one person</td>
<td>Impossibility of implementing some steps of data production processes</td>
<td>Development of a procedure for some data production processes to enlarge widespread competencies</td>
</tr>
<tr>
<td>Personnel</td>
<td>Difficulty of turnover related to specialized expertise for monitoring the quality of collection, processing and data analysis</td>
<td>Delays and problems in various stages of the production process</td>
<td>Periodic execution of procedures for staff mobility</td>
</tr>
<tr>
<td>Technology</td>
<td>Software tools not sufficiently tested for lack of technical support</td>
<td>Reputational collapse; Low quality of statistical data</td>
<td>Securing computer systems. Measures aimed at ensuring the reliability and continuity of services provided by software</td>
</tr>
</tbody>
</table>

### Examples of risk register pertaining to "Statistical Production":

<table>
<thead>
<tr>
<th>Risk</th>
<th>Treatment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay in updating repositories to make balancing data</td>
<td>Mapping and re-engineering the collecting data process for the estimation of a table chart-supply use</td>
</tr>
<tr>
<td>Delay in receiving internal / external sources</td>
<td>Risk Analysis aimed at removing obstacles to the data collecting process through internal and inter-institutional agreements</td>
</tr>
<tr>
<td>Lack of timeliness in the preparation of data files by the competent departments</td>
<td>Mapping and re-engineering the production process of the national accounts relating to the production and value-added services non-market at current prices</td>
</tr>
<tr>
<td>Lack of formalized procedures (supporting documentation, methodological notes, data quality control)</td>
<td>Improving communication and developing information-sharing initiatives</td>
</tr>
<tr>
<td>Delay in receiving data concerning financial accounts and investments with regard to both sector and sub-sectors of Public Administrations</td>
<td>Reviewing and monitoring agreements in place</td>
</tr>
<tr>
<td>Reduction of the amount of data collected at the local level</td>
<td>Execution and tender’s award to provide tablet to municipal detectors of consumer prices</td>
</tr>
<tr>
<td>Delay in the computerization of procedures for the acquisition and processing of data</td>
<td>Activating the control system and correcting data through models used by other NSIs</td>
</tr>
<tr>
<td>Transmission of questionnaires poorly filled out because of lack of competence</td>
<td>Monitoring procedures of collection data by the local Authorities</td>
</tr>
<tr>
<td>Discontinuities in the collection mode and in the data stream</td>
<td>Reviewing organizational process to manage replacements of those involved in data collection</td>
</tr>
<tr>
<td>Difficulties in managing archives and data delivery aligned with new tax regulations</td>
<td>Continuous staff training and making up working groups including statistics and informatics</td>
</tr>
</tbody>
</table>
Main priorities Areas

Some areas were identified as particularly exposed to risks:

1. Management and administrative procedures: obsolescence, non-compliance, waste of resources, inefficiencies in sharing and disseminating information;

2. Recognition and quantification of project costs in order to properly deploy the available resources;

3. Integration among the management systems to support decision making and sector plans;

4. Tendering procedures: requirements, preparation of specifications (technical and legal), tender’s award;

5. Technical management of contracts and their qualitative and quantitative supply monitoring
Results

- Risks and organisational criticalities:
  more than 96% of the total (100% in the Prioritization Areas)

- About 78% are criticalities, i.e. inefficiencies in management processes solved by organisational improvement (over 80% in the P. A.)

- About 4% are problems different from organisational risks (i.e. statistics, ICT, exogenous factors, human resource policies)

<table>
<thead>
<tr>
<th>Risks</th>
<th>All Areas</th>
<th>Prioritization Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N.</td>
<td>%</td>
</tr>
<tr>
<td>TOTAL</td>
<td>359</td>
<td>100,0%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Nature</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Risks</td>
<td>65</td>
<td>18,1%</td>
</tr>
<tr>
<td>Criticalities</td>
<td>279</td>
<td>77,7%</td>
</tr>
<tr>
<td>Others</td>
<td>15</td>
<td>4,2%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>22</td>
<td>6,1%</td>
</tr>
<tr>
<td>Compliance</td>
<td>6</td>
<td>1,7%</td>
</tr>
<tr>
<td>Operatives</td>
<td>310</td>
<td>86,4%</td>
</tr>
<tr>
<td>Reporting</td>
<td>13</td>
<td>3,6%</td>
</tr>
<tr>
<td>Exogenous</td>
<td>8</td>
<td>2,2%</td>
</tr>
</tbody>
</table>
The risks were assessed by the same personnel who contributed to identify them, using the Control & Risk Self Assessment (C&RSA) method to measure the risk’s likelihood and impact on the organization. **2 factors were considered to assess the risks**

1. **Impact**: 2 variables (each weighted at 50% of the impact) were considered among:
   a) Organization (i.e. delay in producing output, extra workload); b) Reputation (internal and external), c) Economics (higher costs)

2. **Likelihood** (50% overall rating): number of occurrences in a significant sample of events, e.g. occurred in the last 12 months

The **multiplication** of the factors determined the overall value of the risk

- Low gravity (green area): about 24% of the critical events
- Highest priority (red area): about 18% of critical events;
- Careful monitoring (yellow area): about 58% of the critical events, with different gradation
Step 4. Risks Treatment

466 organisational response actions (231 in *Priorities Areas* – “P.A.”)

<table>
<thead>
<tr>
<th>Treatment</th>
<th>All Areas</th>
<th>Prioritization Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TOTAL</strong></td>
<td>466</td>
<td>231</td>
</tr>
<tr>
<td>Risks and Criticalities</td>
<td>V.A.</td>
<td>%</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td>450</td>
<td>100,0%</td>
</tr>
<tr>
<td>Types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preventive</td>
<td>36</td>
<td>8,0%</td>
</tr>
<tr>
<td>Subsequents</td>
<td>6</td>
<td>1,3%</td>
</tr>
<tr>
<td>Improvement</td>
<td>261</td>
<td>58,0%</td>
</tr>
<tr>
<td>To deepen</td>
<td>83</td>
<td>18,4%</td>
</tr>
<tr>
<td>Others</td>
<td>64</td>
<td>14,2%</td>
</tr>
<tr>
<td>Responsibilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal</td>
<td>170</td>
<td>37,8%</td>
</tr>
<tr>
<td>External</td>
<td>44</td>
<td>9,8%</td>
</tr>
<tr>
<td>Cross-cutting</td>
<td>172</td>
<td>38,2%</td>
</tr>
<tr>
<td>Not attributable</td>
<td>64</td>
<td>14,2%</td>
</tr>
</tbody>
</table>

- 58% of the proposals refers to organisational or production improvement (about 62% in the p.a.);
- Nearly 38% of the actions are internal (about 44% in the p.a.);
- Over 38% of the actions requires the collaboration of different structures (about 39% in the P.A.)
From the Bottom-up to the Top-Down approach

- From 2015 on, the previous bottom-up approach is being integrated with a top-down one in order to enhance quality and significance of the information contained in the registers.

- Operational risks are identified by accountable managers and then gathered in strategic categories (corporate risks), in order to be assessed, treated and monitored.

Among the others, Corporate risk selection takes into account the following criteria:

- Ability to monitor a risk response action by means of specific indicators;
- Organizational sustainability of the risk treatment proposed;
- Cross-cutting quality of the risk response actions proposed;
- Belonging of risks to one of the “priority intervention areas”.

Corporate risks are specifically monitored by appropriate output and performance indicators.
Top-Down approach: «Corporate» risks

In 2015, the critical events (Risks and Criticalities) in the Catalog were 111, compared to 209 at the end of 2014 and 359 of the experimental phase; among these, about 18% fall under the category "Corporate".

The risk treatments have significantly been reduced; in fact, in early 2015, the response actions in the Catalogue amounted to 128, compared to 254 at the end of 2014 and to 450 of the experimental phase. About 19% correspond to those proposed for mitigating “Corporate“ risks, monitored by appropriate output and performance indicators.
Top down approach: Roles and accountabilities

1) All **staff** are responsible for an effective management of risks including identification of any potential risks;

2) Risk management is driven by the **organizational units**;

3) An **Office** is dedicated to the coordination of the management process and risk analysis, adopting an unbiased perspective against any other structures and supporting the highest level of decision making;

4) The **Risk Manager** is responsible for: collaborating with Top Management both in identifying high risk areas related to strategic and business processes and in planning treatments to mitigate corporate risks;

5) The **Advisory Board**, composed by the top managers (operating in the most risky areas), defines the Risk Management policy;

6) **Chief Statisticians and Governing body** define the strategies also on the information coming from the RM System;

7) The organizational model envisages an **Internal Auditing office** for reporting to the Governance on the adequacy of RM process and the compliance of mitigating actions.

*Fabrizio Rotundi*
Where we are going to

**Implementing three levels of Controls:**

- **first control line:** Management (*risk owner*), responsible for verifying and mitigating risks, monitors controls on the ongoing activities
- **second control line:** Risk Management Office, whose task is to facilitate, monitors and supervises the ERM process
- **third control line:** Risk-Based Internal Auditing, independent, provides reasonable assurance on the ERM effectiveness as well as the activities of the first and second line of control

**Improving the Risk Management System:**

- Connecting Risk Management System to GAMSO
- Designing a set of Key Risk Indicators tailored for GSBPM standard
- Adopting the Model for Fraud risks
- Improving ERM supporting software
- Fostering link with Performance Evaluation
- **Improving Quality through Risk Management**
- Moving to a centralized organizational Model
- **Deeper integration (Internal controls & Management information system)**
The information system RiskInIstat has been implemented to manage risks via web with the main objective to let Management edit and view the necessary information, in an intuitive and immediate way.

It gives the possibility to update the catalogs, showing how much the objectives has been realizing at different stages of the ERM process,

provided that “RELIABLE” information is uploaded !!!
Thank you for your attention !!!

Fabrizio ROTUNDI
rotundi@istat.it
fabrizio.rotundi@gmail.com