



***RETHINKING AND RESHAPING ORGANIZATIONAL SYSTEMS  
IN TIME OF CHANGES: THE PROCESS OF RISK MANAGEMENT  
IN ITALIAN NATIONAL INSTITUTE OF STATISTICS***

## Summary

1. Introduction: Risk Management in public sector .....	3
2. Istat's Risk Management Project .....	5
3. The project of Risk Management in Istat.....	6
4. The Risk Management process .....	8
5. The results.....	11
6. Current risk frame .....	15
7. Monitoring operations: the results from the first half of 2013.....	17
8. Process management tools: the software web-based application "RiskinIstat" .....	19
9. Development and dissemination of Risk Management System (from 2014 on) .....	20

### Authors:

Prof. Alessandro Hinna, University of Rome, Tor Vergata

Fabrizio Rotundi, ISTAT, Head of Risk Management Office

Eleonora Rocchi, ISTAT, Risk Management expert

Katia Ambrosino, ISTAT, Risk Management expert

Danila Scarozza, University of Rome, Tor Vergata, Researcher

Thanks also to Angela Leonetti for her contribution in reviewing and enriching the article

## 1. Introduction: Risk Management in public sector

In several countries, the Public Administration Reform that has been taking place in the last ten years, has been characterized by the effort to increase productivity, ability and quality, despite the cuts in available financial and instrumental resources. In this frame, governments have set a legal background for the development of an internal control system in public sector organizations, while relevant institutions have made their contribution to promote risk management frameworks and to establish a certain set of rules and methodologies which have been at the margin to the “typical” accounting practice.

However, apart from the regulatory initiatives and often superficial efforts to implement a risk management framework, little has been done to concretely establish an overall internal public sector control system on risk management basis. Some of the reasons behind this pattern are related to public sector’s inherent reluctance to accept innovations or changes, to the natural differences between the private and the public sectors and their objectives, or to the comparatively limited practical and theoretical knowledge of risk management implementation in the public sector entities.

Despite the explosion of risk management in private sector, until 1980s government and public administrations did not appear to have pressures to change and to implement risk management practices. It is only since the early 1990s that there have been several attempts to adopt certain aspects of ‘good practices’ in public management: private sector initiatives to improve risk and internal control systems have been mirrored by similar promptings for change in the public sector, where risk management is now seen both as an important dimension of good governance and as a tool to aid the achievement of strategic objectives.

In general terms, the awareness of the need for formal frameworks for risk management in public management is boosted by several factors, including:

- the ease of access to data and applications and the expansion of relations with stakeholders, combined with the speed of economic change, make the risks intersected of each other in a complex and difficult way to manage;
- the exponential increase of regulatory activity makes the compliance with laws a talked-about subject, so, on the one hand, public administrations must meet a series of, often complex, obligations, contained in administrative laws, on the other, the responsibility of business leaders has become direct and personal;
- the increasing "globalization", which obliges many national governments to take into account the corresponding Community, international or other national institutions (for example, ISTAT and Eurostat), which implies the need to manage risks beyond the boundaries of the State of origin;
- the increased visibility of citizens, which increasingly exposes public administrations to reputational damage or loss because of easily disseminating news and multiplicity

of information sources.

The new level of uncertainty solicit public administrations to introduce innovative forms of operative systems: the traditional decision-making and control systems are rationally based, and reduce the individual decisional process to a mere formal procedure that automatically matches the problem with a predetermined solution set by rules and regulations, while with the new approach the duties of people involved in decision-making must change, they cannot be exclusively technical ones, but they must involve interaction with other actors. The technical duties are inadequate to support decisional processes that are (by this time) not only experimental, i.e. directed to the production of political efficiency (oriented to the result, not to the process), but also conflictual, directed in turn, towards the production of acceptable policies resulting from the intermediation among the different internal and external actors.

In public administration cultural frame, a risk management system can be considered a “new” system of specific organisational rules and can be experienced by organisational participants ‘legalistically’, allowing defensive compliance strategies. As a final result, while the risk management system might support the actor in managing the complex issue of tasks uncertainty increasing degree, the risk management support can represent an “exit strategy” to not manage the uncertainty and a “defensive” strategy to avoid individual or collective responsibility.

All these peculiarities reveal that risk management in the public sector entities requires a more accurate approach, together with additional dedication and resources, which sometimes are unavailable and it is important to emphasize that, in order to achieve the maximum of risk management potential in the organization, the adopted system and framework must be more specific and incorporated into the specific organization frame.

## 2. Istat's Risk Management Project

The goal to define a management system based on the evaluation of available assets and resources, aimed at managing risks and criticalities that hinder the statistical processes, has been strengthened by the need to meet the principles and criteria recommended by the European community<sup>1</sup>.

The impulse to establish a Risk Management system in Istat not only comes from these requirements but also from the necessity to strengthen people's sense of belonging, to review activities and available human capital, to govern uncertain situations and emergencies. In such a context and due to lack of resources, the Institute has consequently been facing a deep cultural change; such an approach has gradually modified, and is still modifying, mentality, developing provisional and managing capacity, enabling management to move from planning and control activities based on a fragmented, informal and occasional approach to considering events not only as risks but also as opportunities and challenges.

According to the aims of the analysis, among the other public entities that have put in place a risk management process<sup>2</sup> in Italy, the National Institute of Statistics was selected as a case study because of its uniqueness, having completed the experimental period and chosen to use the risk management system as a tool for the analysis and the administration of the organization. In particular:

1. the risk management project has begun before the Italian legislative reform on internal controls systems, which now obliges public administrations to use information from risk management systems to support management control systems and to treat the high severity risks, such as fraud and bribery;
2. the ERM process has been applied to organizational risks in order to avoid overlapping with other control systems already in use;
3. all operational activities needed during the pilot phase and the final implementation of the System have been completed, and the ERM process is now effective, from the analysis of the control environment to the identification, evaluation and risks treatment;
4. the implementation of the process is continuous and multidirectional, and was accompanied by communication, training and planning activities.

Moreover, Istat is also planning a progressive introduction of Internal Audit concerning organizational processes and the effectiveness of controls and risk treatments.

<sup>1</sup> The (EU) Regulation 223/09 required the improvement of the statistical processes, pushing the application of innovative management systems for improving quality and saving cost and time.

<sup>2</sup> In particular, the following public entities have been analyzed: Banca d'Italia; INPS, National Institute of Social Security, Ragioneria Generale dello Stato, Regione Lombardia, Università Alma Mater di Bologna.

### 3. The project of Risk Management in Istat

The Project for introducing an organizational Risk Management system in Istat started in 2009. Figure 1 shows a summary of its evolution.

**Figure 1.- Istat's Risk management Action Plan**

2009	2010	2011	2012	2013...
Project launched	Approach trial	Experimental phase	Experimental phase	Full implementation
<ul style="list-style-type: none"> <li>Analysis and comparison of practices and models</li> <li>Identification of appropriate approach</li> <li>Establishing of Istat's RM model</li> </ul>	<ul style="list-style-type: none"> <li>Pilot and rollout of risk management approach</li> <li>RM training and dissemination</li> </ul>	<ul style="list-style-type: none"> <li>creation of a risk register</li> <li>risk assessment</li> <li>RM training and dissemination</li> </ul>	<ul style="list-style-type: none"> <li>revision of a risk register</li> <li>identification of risk treatments</li> <li>RM training and dissemination</li> </ul>	<ul style="list-style-type: none"> <li>Integration w/ operational planning</li> <li>Risk treatments monitoring</li> <li>Risk-based audit plan</li> </ul>

The project at first focused on the analysis and comparison of best practices, models and frameworks used worldwide in order to be able to choose the more appropriate one according to Istat's needs and goals. After selecting the most suitable approach, based on the concept of Enterprise Risk Management, fuller documentation was presented to political bodies establishing and describing the specific risk management model framework and process to set up fit to Istat's needs, together with the planned steps for the implementation of a Risk Management system in Istat. The abovementioned documents were officially adopted by the Institute.

The project developed following three parallel but related paths:

1. *Organization*, that is the definition and structure of the main actors involved in the implementation of the risk management approach, which should facilitate the integration with other core business and activity control processes and offices.

Considering that the success of the project strictly depended on the collaboration and participation of all the subjects of the System, in order to guarantee concrete progress and acceptance of the implementation of the RM approach, Istat's President and the Directorate general assured their commitment to the project. They endorsed and sponsored it adopting an active and participating role throughout all the phases of the implementation process.

Secondly, to provide strong backing, coordination and support for the implementation of the risk management system in Istat, a specific role was assigned to an office whose tasks include:

- giving support for establishing risk management policies and appetite, defining roles and responsibilities, and setting goals for implementation;
- providing a framework for risk management implementation, setting risk categories and measures related to likelihood and impact;

- giving support in identifying, assessing and managing risks and responses;
- assisting operational managers in reporting risk information up and across the organization;
- establishing a common risk management language, facilitating the developing and improving of a risk management culture and promoting risk management competences throughout the organization;
- monitoring risk management progress, reporting to the President, the Board and the Directorate General on progress and recommending action as needed.

At last, for risk analysis, identification and assessments, all managers, offices' representatives and people involved in particular activities across Istat were involved in order to ensure the efforts to implement ERM to be embedded within Istat's core business activities and the risk culture to be communicated throughout the organization.

2. *Training and dissemination* of RM culture and approach to management and all staff, in order to improve management culture and promote a common language and understanding throughout the organization. In particular, a dedicated training program for managers and staff has been developed and continuing communication and information across the organization is guaranteed, too. For example, several risk management seminars have been held, periodic reports addressed to top managers and political bodies were prepared to describe developments, results and analysis, specific policies and procedures have been established and published, the RM office participated in working tables among public institutions regarding risk management issues, composed by national and international entities and companies with a particular focus on research and statistics Institutes, and a web-site, in Italian and English, has been constantly updated in order to provide an effective and efficient tool for sharing knowledge and available information on risk management. In addition, during 2013, a web-enabled software will be developed as a supplementary instrument to reduce burden for reviewing risk catalogues, monitoring treatments and reporting results.
3. The RM *process*, that is the operational activities needed to implement the RM approach, starting from the pilot and rollout phase to the full implementation of the system. The experimental phase lasted three years and was made out of four steps:
  - Phase 1: analysis of the environmental context;
  - Phase 2: creation of a risk register by means of event identification and analysis;
  - Phase 3: risk quantification and assessment;
  - Phase 4: risk responses identification and planning;

The approach has been finally fully implemented during 2013 and 2014. Therefore, future challenges lie in other two phases:

- Phase 5: continuous monitoring and periodic reviewing to address risks;
- Phase 6: monitoring of risk treatments and of the ERM processes for guaranteeing their effectiveness.

#### 4. The Risk Management process

The entity's internal environment is the foundation for all other components of enterprise risk management, providing discipline and structure. The internal environment influences how strategy and objectives are established, business activities are structured and risks are identified, assessed and acted upon. It influences the design and functioning of control activities, information and communication systems, and monitoring activities. The internal environment comprises many elements, including an entity's ethical values, competence and development of personnel, management's operating style and how it assigns authority and responsibility. That is why the first step consisted in the analysis of the internal environment by means of a questionnaire (Phase 1 - *analysis of the internal environment*).

The survey was submitted through a web application to about 30 top managers and it regarded their perception of the dynamics and severity of risk factors that could affect the activities of single offices or of the entire Institute. Among the possible methodological options evaluated for the topographic analysis of risk perception in Istat, the selected questionnaire is based on an international standard (ISO 31000:2009, AS / NZS 4360:1999, A & O) and modeled according to the definitions of an EU framework (PD ISO / IEC Guide 73:2002 and standards FERMA - Federation of European Risk Management Associations).

The Survey is made up of more than 60 questions and focuses on:

1. the level of attention given to risk management when programming and monitoring the main activities of the Directorates and the Institute;
2. the alignment of the current tools used for programming and control with the risk management system;
3. finding, although in simplified form, the factors that may cause injury, distinguishing among internal risks, external risks and cross sectional risks.

The questionnaire uses heterogeneous expressions and different types of responses, in order to keep constant the level of attention by the respondent; and it sometimes uses subjective terms such as "substantially", "normally", "total", etc. as the survey is used to detect perception,...

During the second Phase (*creation of a risk register by means of event identification and analysis*), threats, vulnerabilities and the associated risks are identified. It comprises in building risks catalogues through the recognition of risk issues or assets (the general areas or activities that need to be managed) as well as potential effects or consequences if the risk were to occur and other general information regarding the critical events identified, such as if risk factors are internal or external and responsibility. This additional information is very useful because in order to be able to treat a risk it is necessary to understand its nature and causes so to evaluate whether to manage or accept it according to opportunity and

convenience of the response. During pilot and rollout phase, all efforts concentrated in identifying and analyzing the strategic organizational risks that concern general census and ICT activities. This first experience has been very useful for improving and revising the methodology and the techniques applied across the entire organization during the following experimental phase. Afterwards, the work proceeded following two additional gradual steps: during the first part of the experimental period, information regarding risks was gathered in a very flexible and open minded way; then, when risk management concepts and the model had been set and it had been somewhat learned by all actors, the catalogues have been revised applying the framework and the methodology in a stricter way. In particular, in order to adapt the ERM risk management model to Istat's characteristics, the catalogues registered not only risks but also "criticalities" so that Istat's risk management database now contains these two types of critical issue. Risks are all those organizational events whose happening is eventual and that might exposure the organization's objectives to danger; a "criticality" is an actual and existing problem that determines inefficiencies. As mentioned before, these activities were carried out with the cooperation of Directors, managers and employees involved in the risky activities through interviews and several meetings and continuous feedback, just as any other phase of the process.

Identified risks need to be assessed employing a combination of both qualitative and quantitative methodologies, in order to form a basis for determining how they should be managed, prioritize them and give them an economic value (Phase 3 - *risk quantification and assessment*).

Risks quantification and assessment is done considering the likelihood and impact of events as established by the Control and Risk Self-Assessment (C&RSA) method, whereby senior managers evaluate risks and controls with the help of the Risk Management Office. Risks are assessed considering two perspectives, which are likelihood, the possibility that a given event will occur, and impact, the effect that the event could provoke. Risks are ranked and then mapped on a likelihood/impact matrix, in order to show results of the assessments and help managers visualize and distinguish between areas of interventions depending on the different levels of risk exposition.

The risk likelihood/impact assessment permitted to: *a)* focus attention on critical and relevant risks; *b)* guide the development of strategies for risk management; *c)* align objectives with risk management; *d)* allocate proper resources to manage risks according to their severity; *e)* reduce probability that severe risks are not expected; *d)* create synergies among different offices and processes for sharing best practices.

This method might be affected by subjectivity and discretion but it was functional in sharing the framework and allowing involvement in the implementation of Risk Management: the success of the project strictly depends on the collaboration and participation created across the organization, first of all of process owners. The C&RSA method should be applied to both "residual risks", the portion of the risk that is left after a risk control has been conducted, and "inherent risks", risks related to the nature of the activity. At this stage, Istat

concentrated on inherent risks and plans to expand assessment to residual risks in the next future.

Having identified and evaluated the risks, the next step involved the identification of alternative appropriate actions for managing these risks, the evaluation and assessment of their results or impact and the specification and implementation of treatment plans (Phase 4 - *risk responses identification and planning*).

According to risk assessment results, senior managers devise action plans to address risk issues, whether they are low, high, or acceptable risks, select risk responses (avoiding, accepting, reducing, or sharing risk), defining specific treatments, timing, responsibilities and eventually, when possible, costs. More than one option can be considered and adopted either separately or in combination to avoid the risk by deciding to stop, postpone, cancel, divert or continue with an activity that may be the cause for that risk; to modify the likelihood of the risk trying to reduce or eliminate the likelihood of the negative outcomes; to try modifying the consequences in a way that will reduce losses; to share the risk with other parties facing the same risk; to retain the risk or its residual risks.

In the event that available resources (e.g. the budget) for risk treatment are not sufficient, the Risk Management action plan sets the necessary priorities and clearly identify the order in which individual risk treatment actions should be implemented.

Treatment plans are necessary to describe how the chosen options will be implemented. The treatment plans should be comprehensive and should provide all information needed about: proposed actions, priorities or time plans, resource requirements, roles and responsibilities of all parties involved in the proposed actions, performance measures, reporting and monitoring requirements. Monitoring will be accomplished, on experimental basis, through ongoing management activities but also by means of separate evaluations and internal auditing techniques. In fact, although every part of the organization is responsible for managing risks in each specific area of activity, risk control and monitoring should be operated in an integrated, holistic approach to ensure alignment with the organization-wide objectives and strategies.

Risk management is not a standalone activity and needs, in order to be effective, to be integrated with other organizational processes and systems, such as strategic and operational planning and other audit activities. This type of effort has started in 2012 as managers were asked to include in the operational annual plan of their offices also the most relevant risk treatments and they will be monitored also through the management control system. This activity helped to pinpoint key action plans and valuable risk treatments.

## 5. The results

### *The risk and control perception*

The survey on risk perception explored the most representative dimensions of managers' organizational behavior when the critical events occur. The information obtained was processed to highlight the incidence of risk factors on planning and organizing the activities of each single structure and of the Institute's goals. For this purpose, Istat selected four dimensions, which are most representative of the attitude of managers with respect to critical events. They describe:

1. the *perception of risk compared to the activities of the manager*: measured by the content of those responses that determine “whether” and “how much” the risk affects the planning and management of the manager's activities within the structure of belonging;
2. the *perception of risk compared to the Institute*: related to the connection between the existence of risk and the achievement of the strategic objectives of the Institute;
3. the *maturity of the control environment headed by the respondent*: depending on the individual property to apply the risk management system adopted by the Institute;
4. the *maturity of the control environment of the Institute*: its value derives from answers to questions that investigate the ability of the Institute to implement and support a system of risk assessment;

Each of these dimensions corresponds to a set of answers, not necessarily placed in sequence, that highlight the character and the criteria used by the manager when converting the perception of risk into organizational behavior.

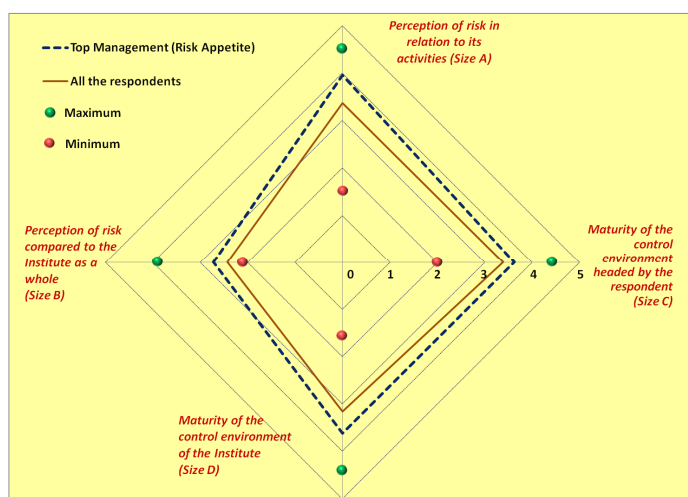
Considering that the information collected shows managers' opinion and that individual perception is itself a particularly skittish phenomenon depending on environmental trends that affect the one's field of competence, the analysis was strictly qualitative and no statistical significance nor quantitative measurement of the phenomenon was attributed to data. In addition, given the variability and subjectivity of risk perception, the results of the analysis of the responses showed a trend in behavior and do not establish a psychological profile or aptitude of the manager.

To facilitate data understanding and interpretation, the four behavioral dimensions have been represented using a radar chart, in which the value placed on each vertex is the average of the values declared by the manager in the set of questions that express the meaning of the relative dimension. Depending on the risk profile to be analyzed, the results of the survey can be differently interpreted.

Specifically were examined 3 situations:

- I. The risk perception by management, highlighting the outliers;
- II. The risk perception by management, by level of responsibility;
- III. The risk perception by management, by area of activity (technical and administrative).

### The risk perception by management, highlighting the outliers



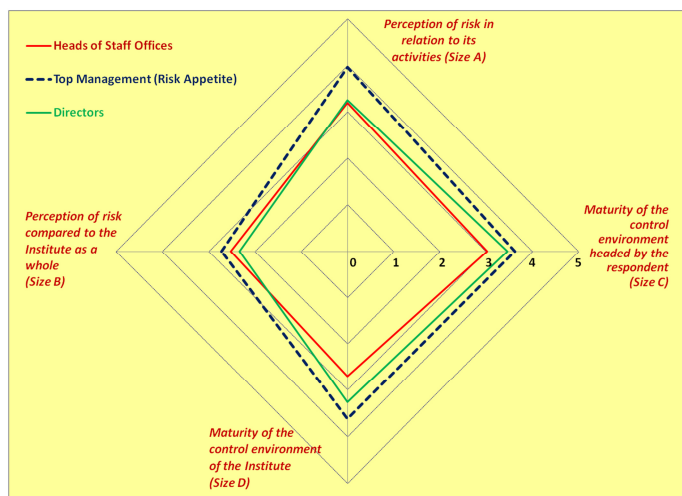
**Figure 2 – Representation of the average of management profile**

Figure 2 compares the average rating given by all the executives involved in the survey (brown line) with the profile of the top management (dashed blue line), including General Director and Chief of Departments, who, in the current theoretical framework, is the level of acceptance of risk consistent with corporate strategies (risk appetite) and shows

outliers, i.e. the maximum values (green bubbles) and minimum values (red bubbles), recorded for each dimension.

The graph shows that the risk is considered an important component in planning activities (Size A), for all groups of respondents considered, even though there is a more favorable approach by apical managers (value of 4 to a maximum of 5) compared to all respondents (value of approximately 3.5). On the other hand, both groups show a moderate mistrust in considering the risks an essential planning element to achieve the strategic objectives of the Institute (Size B). Again, however, it should be noted an attitude more inclined to consider the risk as an important factor for the Institute's activities, by the top management, although the gap between the two values is not so large as in the case of A. In addition, for this dimension, even the maximum value recorded (bubble green equal to 3.8 points) is by far divergent from the average. We note, however, a positive general judgment about the maturity level of the control environment, both for the single structure of belonging and the Institute (Dimensions C and D: values slightly higher 3 out of a possible 5), such that it is allowed a positive development of the risk management system, based on the current organizational configuration. Even for these two dimensions, the orientation of the apical Leadership is demonstrated more favorable than that of all the respondents, although the gap between the two values is more pronounced about the overall vision of the Institute (Size D).

### 1. The risk perception by management, by level of responsibility



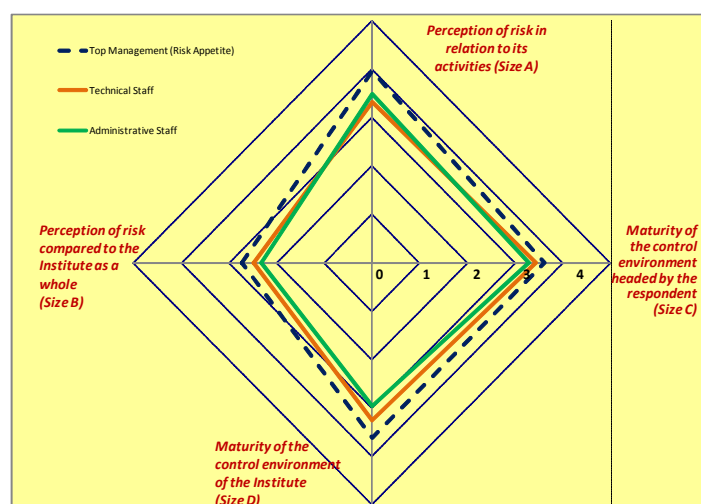
**Figure 3 – Mean profile for senior management by level of responsibility**

Figure 3 shows the average profiles of senior management, divided by level of responsibility, including Top Management, i.e. General Director and Chiefs of Department (blue dotted line), Directors (green line) and Heads of Staff Office (red line) in order to highlight 'how' and 'how much' they manages the organizational risk, according to the level of responsibility. The average rating of top management, considered the highest level of tolerance permitted, shows a particular attention to consider the risk as the base element for the activities planning. In fact, from the graph, the value assigned by top management to A and B dimensions, is the highest among the three levels of responsibility, with a value respectively equal to about 4 and more than 2.7, on a scale of values ranging from 1 to 5. Moreover, these values are also higher than the average, in fact, the maturity assessment of the control environment for C and D sizes is higher than that expressed from the other categories of management (average value equal to more than 3.6).

Comparing the Directors profile (green line) with the top management's risk appetite (dashed blue line), are observed two fairly homogeneous approaches in assessing Size C, whereas are much less homogeneous in the evaluation of the other three dimensions (A, B and D).

The Heads of Staff Offices (red line) show, on the other hand, a more moderate assessment of criticality as part of the its own activities planning. In fact, they attribute a lower value to the control environment's maturity, where is implanted the Risk Management System (Size D), than the other classes of senior management. Risk management, instead, is considered an important component for activity planning under its own responsibility (size A, average about 3.2 points).

## II. The risk perception by management, by technical and administrative sectors



**Figure 4 – Technical and administrative management profile**

Figure 4 shows the average profiles of the legal-administrative structures (green line) and of the technical structures (orange line) compared with that of *top management* (blue dotted line).

Analyzing the technical and administrative senior management's average profiles, all 4 dimensions converges to values lower than the

*top management* (representative of the Institute of *Risk Appetite*). The legal and administrative structures, on the one hand, pay attention on the risks identified within the structure of belonging (Size A, mean value greater than 3.5 points on a scale 0 to 5), on the other hand, are less positive with risks related to the activities of the Institute as a whole (Size B, average value of about 2.5 points on a scale from 0 to 5). Also with regard to the control environment maturity (C and D sizes), legal and administrative structures are more confident in the approach of their structure than in that of the organization as a whole (Size C, value close to 3.5; Size D, value equal to about 3 points, on a scale of 0 to 5). The technical structures reveal the same level of attention to the risks identified on the statistical production Directorates and on the Institute as a whole for all the dimension A, B, C, D; the average is around 3.5 percentage points. The comparison between the administrative and technical-scientific profile shows a more favorable judgment, by researcher, to make risk management an essential factor to get the activities successfully (size B, C and D). Finally, risk management is more important for the administrative top management, referring to the planning and monitoring activities.

## 6. Current risk frame

The activities programmed have been completed under tight timelines, thus the experimental phase was finished by the end of 2012, permitting to set up all preliminary activities needed for the next phase aiming at full implementation.

All data collected was put into a database in order to store all information, analyze it easily and be able to create different kinds of reports. The database is going to supply base information for the application that is being developed and that will allow all managers, at different levels and with different access, to view and administer directly their own critical events.

All catalogues have been revised and updates to consider the objectives and activities planned for 2013, improving the distinction among organizational risks and criticalities and the others, which are not managed by the model, and the description of action plans, which are more realistic and detailed. Of course, as in the experimental phase, Istat attempted to optimize all efforts and information collected, and tried to analyze from different point of views also the critical events that are not managed by the model but that nevertheless might be useful for organizational progress, avoiding to waste a rich heritage gathered through confrontation with a wide range of managers. For example, the lack of human resources or competences has been included in the database in a special category, in order to signalize worries and difficulties linked to excessive workloads due to absence of employees turnover in the Italian public sector.

Hence, the critical events identified for 2013 are 350, with a total of 450 treatments; of these, 90 have been formally integrated in Istat's annual operational plan.

Among identified critical events, about 38% are "internal", that is, they can be managed by the structure that documented it, and about 38% are "cross-cutting", that is, they can be treated with the cooperation of other organizational units, meaning that, compared to 2012, the analysis concentrated much more on the efforts that each one can do to reach their own objectives and limited the necessity to involve other offices or to transfer responsibility for risk management.

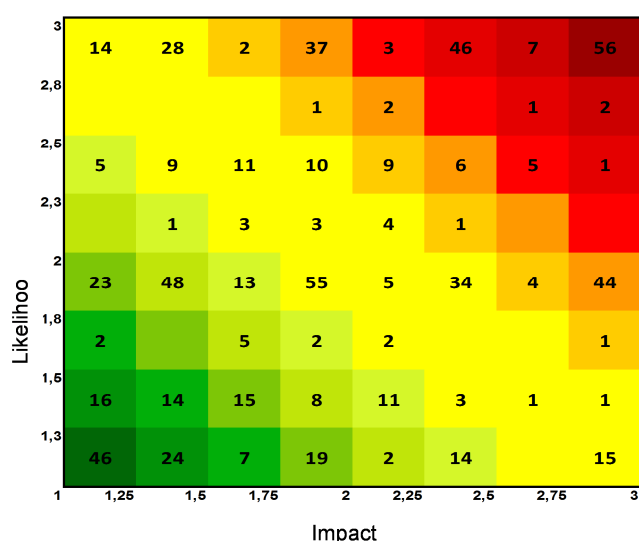
This information is particularly significant, because the simultaneous participation in operative objectives of different business units, belonging to different areas of the Institute, requires a relevant effort during the planning phase. In fact, the manager that leads a structure, who is asked to cooperate by a manager belonging to another structure, must be informed immediately so that she/he can program all supporting activities. The sharing of process and activities among several units represents an important starting point in order to improve also the organizational design evidencing the need to enrich the traditional bureaucratic model with some other mechanisms. Obviously, both new organizational mechanism and monitoring tools should facilitate horizontal integration and communication systems and decision-making processes should also improve. Respecting COSO ERM

framework, each critical event was also classified according to the four objective categories (Strategic, Operations, Reporting, Compliance) to which Istat added a fifth one, Endogenous, to group those risks that depend exclusively on events that are independent and external to the organization (2% of identified risks). About 86% of critical events are Operational and might therefore compromise the effective and efficient use of resources because, for example, they are related to inappropriateness and obsolescence of managerial or administrative procedures. The strategic events, which are lined up with strategic objectives and aligned with and supporting the mission of the organization, are about 12%.

The detailed planning of risk treatments programmed by the structures and the integration of part of these in the operational plan, represent the additional step accomplished in the transition between the experimental and the full implementation phase. The about 90 risk treatments that have been included in the operational plan, have been chosen according to priority, eventual previous risk evaluation, attention to detail and consequentiality among objectives, critical event, generated effects and actions.

Among the selected 90 corrective actions, more than half refers to managerial or administrative actions addressed to both the revision and the control of existing procedures at Istat. In most cases, these actions aim to improve, in a cross-organizational way, working processes and activities. All treatments programmed by the units and that have not been integrated in the operational plan of the Institute, will have to be developed during the full implementation of the multi-annual program of risk management and will be monitored directly by the Risk Management Office.

**Figure 5 – Risks evaluation matrix (experimental phase results)**



Evaluation according to C&RSA has been applied to critical events identified during the experimental phase by Directors and managers and were then allocated into the likelihood/impact matrix: each box shows the number of critical events with that particular combination of likelihood and impact evaluation range (figure 5). According to this kind of analysis, 24% of critical events are located in the “green area”, that is the low exposition area, while 18% are in the red high exposition area, which refers to

top priority critical events that require close attention. The yellow medium exposure area includes the majority of the critical events (about 58%), those that nonetheless need a constant monitoring and managing. The events with a higher probability and higher impact are about 8%, as the ones with lower likelihood and lower consequences.

## 7. Monitoring operations: the results from the first half of 2013

In September 2013 the monitoring of response actions to organizational risks and threats referred to the first half of the year was brought to an end. According to the ERM process, Istat offices provided final data concerning the step of risk treatment applied to action proposals both contained (*Risk Management* goals) and not included in PAA 2013.

Information received was later transferred to the new Risk Management application launched at the end of October 2013. This application supports risk and threat catalogue management in Istat, in fact, starting from the planning for 2014 it is possible for users to access online at the address <http://riskinistat.istat.it/risk/> and directly update and monitor information contained in the relevant registers.

During monitoring operations, whose results are described as follows, it has been possible to: 1) collect final data on the trend of critical events and response actions connected to them; 2) detect total and partial outputs and the activities carried out during the first half of the year; 3) update and revise general information contained in the catalogues.

Comparing data from the first monitoring of response actions to risks and threats with 2013 planning data (cfr. Tables 1 and 2), we can find a decrease in the sum of critical events contained in the Istat catalogue (from 359 to 295) equal to 17% approximately, that results in a decrease of their treatment actions equal to 20%. This trend comes from the revision of contents of the pertaining register made by the offices together with monitoring operations, in order to make catalogues consistent with *Risk Management* system.

Looking at summary Tables 1 and 2 in detail, we notice that in comparison with the planning step the catalogues at present contain organizational critical events, risks and threats only, not considering IT and statistical problems and the ones concerning lack of human resources, that are not included in the ERM model used by Istat.

From data analysis we find that criticalities (threats) – in other words, problems causing real inefficiency in management operations – are much more (82% approximately) than risks (18% approximately), that is, organizational negative events which can occur or not. This information underlines that, even if Istat is going towards a better assimilation of the “risk culture” according to ERM guidelines, its governance has chosen not to neglect real inefficiency problems in administration at all, thinking it appropriate to act on them directly, just for making the best use of the resources invested in developing ERM project in the last three years.

**Table 1 – Critical events: summary of monitoring information and comparison with planning data**

<b>Planning: 2013</b>				
Critical Events	All Areas		Prioritization Areas	
	N.	%	N.	%
<b>TOTAL</b>	<b>359</b>	<b>100,0%</b>	<b>170</b>	<b>100,0%</b>
<b>Nature</b>				
Risk	65	18,1%	33	19,4%
Threat (criticality)	279	77,7%	137	80,6%
Others	15	4,2%	0	0,0%
<b>Type</b>				
Strategic	22	6,1%	6	3,5%
Compliance	6	1,7%	2	1,2%
Operative	310	86,4%	155	91,2%
Reporting	13	3,6%	6	3,5%
Exogenous	8	2,2%	1	0,6%

<b>Monitoring: first half of 2013</b>				
Critical Events	All Areas		Prioritization Areas	
	N.	%	N.	%
<b>TOTAL</b>	<b>295</b>	<b>100,0%</b>	<b>171</b>	<b>100,0%</b>
<b>Risk</b>	<b>52</b>	<b>17,6%</b>	<b>32</b>	<b>18,7%</b>
Solved	12	23,1%	8	25,0%
Unsolved	31	59,6%	24	75,0%
Not available	9	17,3%	0	0,0%
<b>Threat (criticality)</b>	<b>243</b>	<b>82,4%</b>	<b>139</b>	<b>81,3%</b>
Solved	31	12,8%	20	14,4%
Unsolved	186	76,5%	114	82,0%
Not available	26	10,7%	5	3,6%

Furthermore, monitoring and revision actions highlight that approximately 60% of treatment actions concern *priority intervention areas* – the most critical areas in which risks and threats that are particularly relevant for the organization remain.

Data analysis concerning treatment action *responsibility* highlights that approximately 90% of response actions are carried out by the same management office which suggested them, both on its own and together with other offices; comparing these data with planning ones points out that response actions involving external responsibility are lessened of 25%.

As far as planned response actions progress is concerned (cfr. Table 2), we find out that by the 2013 first monitoring approximately 2/3 of them are still running, while 17% of them are already brought to an end.

In the following tables and charts, monitoring information contained in offices' registers (critical events, response actions) is fully reported.

**Table 2 – Response actions: monitoring information and comparison with planning data**

<b>Planning: 2013</b>				
Response actions	All Areas		Intervention Areas	
	N.	%	N.	%
<b>Risks and Threats**</b>				
<b>TOTAL</b>	<b>450</b>	<b>100,0%</b>	<b>231</b>	<b>100,0%</b>
<b>Type of action</b>				
Preventive	36	8,0%	24	10,4%
Subsequent	6	1,3%	3	1,3%
Improvement	261	58,0%	143	61,9%
To deepen	83	18,4%	42	18,2%
Other	64	14,2%	19	8,2%
<b>Responsibility</b>				
Internal	170	37,8%	101	43,7%
External	44	9,8%	22	9,5%
Cross-cutting	172	38,2%	89	38,5%
Not ascribable	64	14,2%	19	8,2%

<b>Monitoring: first half of 2013</b>				
Response actions	All Areas		Intervention Areas	
	N.	%	N.	%
<b>Risks and Threats**</b>				
<b>TOTAL</b>	<b>357</b>	<b>100,0%</b>	<b>210</b>	<b>100,0%</b>
<b>Responsibility</b>				
Internal	175	49,0%	101	48,1%
External	33	9,2%	11	5,2%
Cross-cutting	149	41,7%	98	46,7%
<b>State of action</b>				
Finished	62	17,4%	38	18,1%
Ongoing	199	55,7%	122	58,1%
Not started	9	2,5%	9	4,3%
Postponed	22	6,2%	20	9,5%
Transferred	2	0,6%	1	0,5%
Cancelled	7	2,0%	6	2,9%
Not available	56	15,7%	14	6,7%

## 8. Process management tools: the software web-based application “RiskinIstat”

Istat’s risk and threat catalogue, updated and improved during monitoring step according to a *ratio* closer to the ERM guidelines, represents the starting point of 2014 planning, that is run *on line* by the **RiskinIstat** software application.

This web-based and purpose-made application allows risks to be managed quickly and efficiently either avoiding involved persons/offices from being excessively charged or assuring a safer data treatment and processing and a clear and well-timed reporting.

The RiskinIstat application, designed in 2012 and carried out during the following year, is fully running from autumn 2013, so finalizing the risk analysis and response actions planning experimentally started up in 2010. The main purpose of Risk information system is to allow Istat’s Top Management to easily and immediately entry and view all information needed to manage risks in their offices, so ensuring the update of risk catalogues, objective fulfillment and different steps of Risk Management process.

To do that, the application has been built like a pyramid which provides for different functions in any step according to users’ role and position.

*Update, Validation/Assessment and Monitoring* are the three steps of the process.

## 9. Development and dissemination of Risk Management System (from 2014 on)

In 2013 Risk Management has been fully adopted by Istat's administration and is aiming at gradually reaching a perfect integration with the rest of management and quality improvement systems.

This process follows two paths and acts on different levels:

- on one side, it manages risks effectively and efficiently in order to ensure data and processing safety and provide clear and well-timed reporting. The whole operation is backed up by the application RiskinIstat that allows to entry and view the information needed for managing risks and threats. All this ensures to keep the risk catalogue and Risk Management objectives situation updated, in any of its different steps;
- on the other side, it integrates with other management and internal audit systems as:
  - statistical production and process mapping quality Audit;
  - the project Stat2015 which represents the mainframe of innovations that Istat is going to adopt in methodology, technology, subject and organization for 2013-2015 years;
  - Risk Assessment activity concerning National Accounts statistics, according to Eurostat's demands.

Risk management process in Istat has been supported by a proper training for the Top Management and human resources involved in the System implementation. This training is aimed at increasing organizational culture and disseminating Risk Management inside Istat.

Several partnerships among Universities and public bodies (Università di Roma Tor Vergata – Tor Vergata University of Rome – and Scuola Nazionale dell'Amministrazione – National School of public Administration) have also been started in order to detect possible joint research paths on risk management in the public sector.

Moreover, in 2013 Istat's practice in risk management has been selected as best organization practice among international and European public bodies to participate in conferences arranged by the most important new public management associations, such as the European Academy of Management (EURAM), the European Group of Organizational Studies (EGOS) and the Academy of Management (AOM), and the UNECE Conference of European Statisticians.

As regards, instead, future prospects of Risk Management System, a further development area is concerning the interconnections with anti-corruption activities in the public sector (ex L. 190/2012).