GUIDELINES ON RISK MANAGEMENT PRACTICES IN STATISTICAL ORGANIZATIONS

THIRD DRAFT

November, 2016

Prepared by:

In cooperation with:

This page has been left intentionally blank

TABLE OF CONTENTS

List of Reviews **5**
FOREWORD **7**
The guidelines 7
Definition of risk and risk management 9
SECTION 1: RISK MANAGEMENT FRAMEWORK **13**
1. Settling the risk management system **15**
1.1 Risk management mandate and strategy 15
1.2 Establishing risk management policy 17
1.3 Risk management approaches 21
1.4 Adopting an integrated risk approach connected to statistical quality management 24
2. Risk management resources ..... **28~~28~~**
2.1 Risk organizational culture ..... 28~~28~~
2.2 Training ..... 29~~29~~
2.3 Delivering roles and responsibilities ..... 30~~30~~
3. Risk management process (see Section 2) ..... **32~~32~~**
4. Monitoring and reporting ..... **33~~33~~**
4.1 Monitoring and review of the framework ..... 33~~33~~
4.2 Establishing reporting mechanisms ..... 34~~34~~
SECTION 2: Risk management process ..... **39~~39~~**
1. Communication and consultation ..... **41~~41~~**
1.1 Internal communication ..... 42~~42~~
1.2 External communication ..... 44~~44~~
2. Context analysis ..... **46~~46~~**
2.1 Establishing the context ..... 46~~46~~
2.2 Process mapping ..... 47~~47~~
3. Risk assessment ..... **49~~49~~**
3.1 Risk identification ..... 50~~50~~
3.2 Risk analysis and measurement ..... 54~~54~~
3.3 Risk weighting ..... 58~~58~~
4. Risk treatment ..... **59~~59~~**
4.1 Risk treatment actions ..... 60~~60~~

4.2 Risk treatment process ..... 62~~62~~
5. Monitoring and control ..... 68~~68~~
5.1 Monitoring and review ..... 68~~68~~
5.2 Key risk indicators ..... 69~~69~~
6. Risk based control and audit ..... 71~~71~~
7. Risk management information system ..... 74~~74~~
8. Risk management maturity model ..... 77~~77~~
9. Lessons learned ..... 85~~85~~
9.1 Strengths and weaknesses when implementing a risk management system in NSOs 85~~85~~
9.2 Cluster 1: Mandate to manage risks and Risk Policy ..... 87~~87~~
9.3 Cluster 2: Risk management procedure and the role of risk management office ..... 89~~89~~
9.3 Cluster 3: Risk management integration with other functions ..... 90~~90~~
9.4 Cluster 4: Risk management process ..... 92~~92~~
9.5 Cluster 5: Risk management supporting processes ..... 95~~95~~
9.6 – Risk management integration into ongoing activities ..... 97~~97~~
Acknowledgements ..... 99~~99~~

List of Reviews

First Draft (April 2016) – Risk management guidelines presented during the "Workshop on risk management practices in Statistical Organizations", held in Geneva on 25-26 April 2016.

Second Draft (July 2016) – Review of risk management guidelines after the "Workshop on risk management practices in Statistical Organizations", according to the observations and suggestions received by the NSOs participating in the Survey.

- The following paragraphs/chapters have been revised: Foreword: "what risk is and why risk management is relevant" statements added (page 9-11);
- Risk Nomenclature and definitions: meaning of risk Plan clarified (page 17);
- Risk appetite: risk Appetite and risk Profile issues implemented (page 18-20).
- Risk management commitment: paragraph revised as required (page 20);
- Risk management approach: example of "mixed approach" clarified (Fig. 2, page 23);
- Internal control according to a risk-based approach: relationships between internal controls and risks clarified (page 24-26);
- Integration with GAMSO: proposal to align GAMSO and risk management process added referring to the integration between risk and quality management (page 27);
- Roles and Responsibilities: responsibility of he "governing board" clarified (page 31);
- Monitoring and Review of the Framework: the importance of periodically reviewing the risk management maturity level underlined (page 34);
- Review Audit Report: the importance of the audit report in aligning risks with internal controls underlined (page 37);
- Communicating risks: the importance of documenting risk communication in the risk management /Internal communication Plan underlined (page 42-44);
- Establishing the context: the importance of risk maturity assessment in order to successful implementing a risk management policy underlined (page 46-47);
- Risk treatment: the differences between mitigation actions and contingency actions clarified (page 61);
- References: the standard ISO 27000 "*Information technology - Security techniques Information security management systems – Requirements"* quoted in "References"

The following paragraphs/chapters have been included/added:

- Risk management approaches: paragraph on risk management approaches (top-down, bottom-up) implemented (page 21-22);.
- paragraph on risk identification modified (page 50);
- Risk management Maturity Model paragraph added (page 76);

- Risk Appetite: UK case study added (page 9-11, Annex);
- Risk Maturity Model: UK Case study added (page 29-34, Annex);
- Risk Maturity Model combining both international standards and analysis of surveys on risk management practices results added (page 35-42, Annex)

Third Draft (October 2016) – Risk management guidelines integrated with the analysis of results from the III Survey "What was most successful, What was most Difficult, What not to do when implementing risk management in NSOs' experiences" (July – September 2016).

The following chapters have been included/added:

a) Lessons Learned (page 85): new chapter on analysis of 3rd survey on risk management practices results.
b) Summary table of 3rd survey on risk management practices results: (page 36-48 Annex).

FOREWORD

The guidelines

These Guidelines are intended to help the implementation of a risk management system in statistical organizations.

In order to identify practices specific to the particular features of National Statistical Offices (NSOs), the first step of analysis has concerned the collection of actual cases of implementation of risk management systems at internationally. In 2015 two surveys were carried out, in order to analyse to what extent risk management systems are adopted among the NSOs who are members of the United Nations Economic Commission for Europe (UNECE) – as well as among countries and international organizations not belonging to the UNECE, and yet participating in the Commission's activities.

Data collected through the first survey has been pre-analysed according to a theoretical paradigm – named "The template" – shared through a research paper during the "Workshop on modernization of Statistical production and services", held in Geneva on 19 -20 November 2014. The template takes into account the most relevant and useful standards such as Enterprise risk management Conceptual Framework (ERM): Internal Control – Integrated Control, developed by the Committee of Sponsoring Organizations of the Treadway Commission (Co.S.O.) and ISO 31000:2009 (risk management – Principles and guidelines).

The countries involved in the second survey were selected according to the following criteria: long-term positioning within the most developed areas; representativeness related to the geographical area (EU/not EU countries); compliance with acquired standards and practices.

From a methodological point of view, it should be highlighted that the selection carried out is not based on a performance ranking. Rather, it aims at focusing on the most relevant features required for a high-quality risk management practice, because information from the respondents will contribute to define a global framework, inferred from each system.

The Guidelines don't aim at detecting a *best practice* according to international risk management standards, but to those practices most adjustable to the NSOs' organizational context, with a view to reproducibility[1]. Their goal is therefore to provide both a theoretical

[1] The notion of reproducibility refers to the transferability of standard features, regardless of any difference in the organizational context; that implies the possibility for other organizations to adopt the same model.

and practical tool for helping the NSO modernization process, given that implementation of a risk management system will contribute to greater focus on controlling statistical quality.

This draft consists of two sections, whose index complies with risk management standard ISO31000/2009:

- Section 1 investigates the risk management system; and
- Section 2 focuses on the risk management process.

The Sections 1 and 2 include **Question Mark boxes** that consistently report some answers to the questions contained in the first and the second surveys.

Each paragraph includes key words ("tags") to make topic findings easier within the Guidelines.

The Guidelines also comprise:

- **Annexes** which show a more practical approach to the different domains of risk management, describing two categories of examples:
  - Focus points on risk management core topics;
  - Case-studies, describing significant experiences of some NSOs on particular features of the risk management systems;
- **References**, concerning the main sources of the Guidelines;
- **Glossary**, with the definition of the main relevant terms of the Guidelines.

Definition of risk and risk management

Risk management is an organizational model aimed at developing the quality of management processes; it stands out by analysing the events that have never materialized within the organization.

Unlike most managerial systems, risk management doesn't overlap with other internal controls because it represents a different perspective that cuts across planning and control, performance evaluation system, audit, quality and so on.

Therefore, risk management helps the organizations bring about a higher level of quality of services and products because it supports the decision-making processes, preparing for the difficulties that could hinder the achievement of the strategic goals.

In a few words, the main objective of risk management concerns protecting and strengthening:

- Values, ethics and sense of belonging
- The entity's tangible and intangible assets
- Growth of organizational culture
- Leadership and relationship
- Effectiveness and efficiency of processes
- Resources for strategic priorities
- Stakeholder's satisfaction

That means that risk management could be considered to be a tool to effectively manage an organization; in fact, it deals with risks and opportunities affecting the creation or the preservation of an entity's value. risk management is defined by the Co.SO. Model[2] as: "*a process, effected by an entity's board of directors, management and other personnel, applied in a 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*".

The definition reflects certain fundamental concepts; in particular, risk management is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite

[2] Committee of Sponsoring Organizations of the Treadway Commission (COSO) - Internal Control - Integrated Framework, 1992,2004,2013

- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories

This definition is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries, and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.

Risk management examines the events that have negative impact; they represent the risks which can prevent value creation or erode existing value.

There are many risk definitions in the literature and in the standards most recognized at the international level; the standard ISO 31000:2009 defines risk as: "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 (including changes in circumstances) and the associated likelihood of occurrence" and the uncertainty is "the lack of information about the understanding or knowledge of an event, its consequences and likelihood".

In fact, the concept of risk is more complex than the combination of likelihood and effect; it comprises some issues considered by the cognitive analysis relating to the organization, including:

- Risk Profile: set of risks that may affect all or part of an organization;
- Risk Appetite: total amount and type of risks that an organization decides to pursue, maintain or adopt
- Risk Perception, which describes how people perceive risks according to their values and interests
- 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 Capacity, which is the maximum level of risk that an organization can assume without violating the regulatory burden;
- Risk Retention, which considers stakeholders' conservative return expectations and a very low appetite for risk-taking.
- Risk Tolerance, which is the level of variation that the entity is willing to accept around specific objectives.

All of these issues should be considered to assess the overall risk level of the organization.

Therefore, the identification of the "enabling factors" and the "causes" related to a risk, could contribute significantly to specifying the context in which the risk can occur, allowing risk owners, to adopt the necessary preventive measures.

While the enabling factor represents an organizational/social/environmental circumstance which facilitates a behaviour that could result in a risk, the cause is the reason why the action has been undertaken. Therefore, the root-cause analysis can help organizations distinguish risks that could be effectively tackled from those which can only be partially dealt with.

Regarding the definition of a risk, some issues should be taken into consideration[3]:

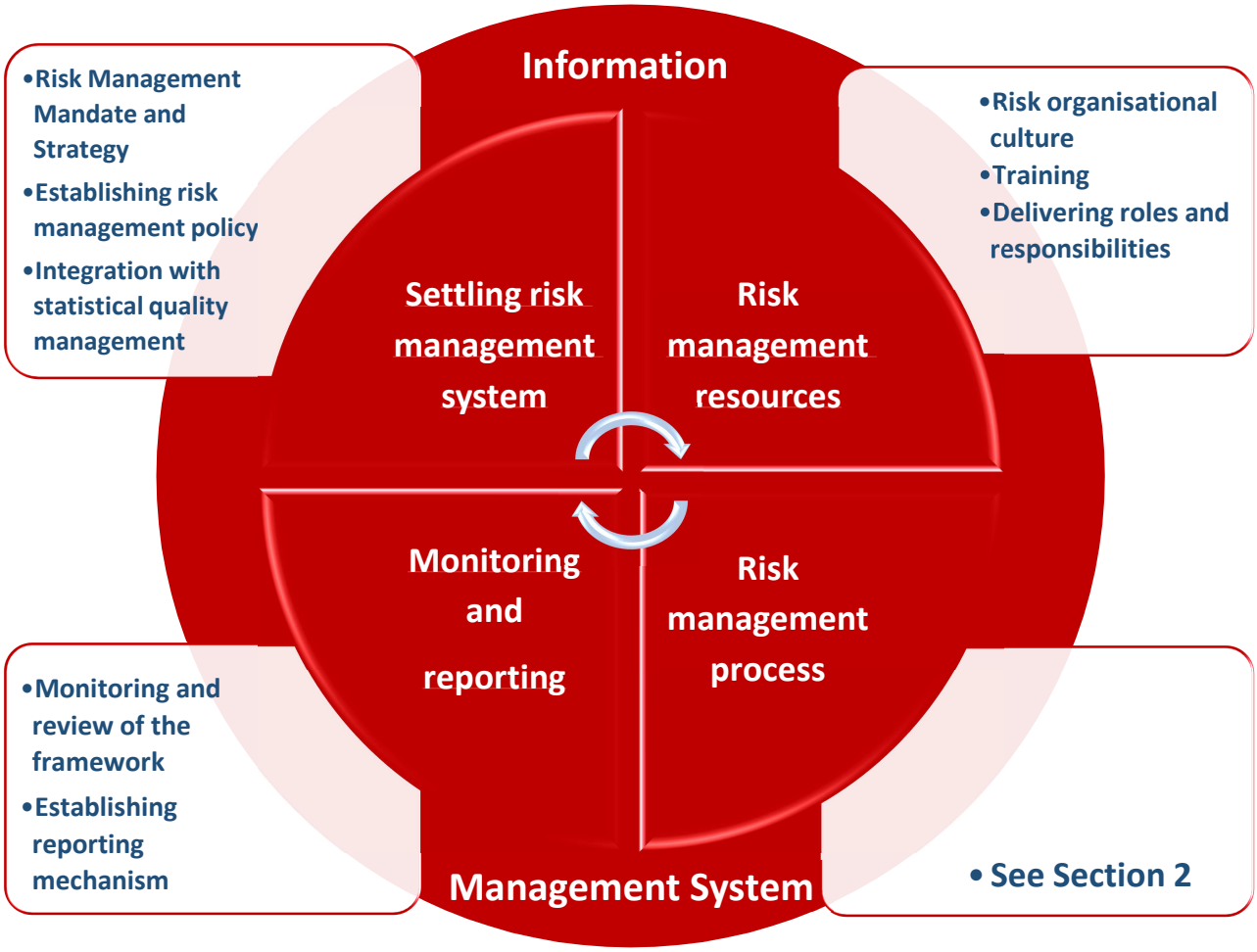
- A risk statement should be a clear, meaningful and concise statement that describes the risk. *Example: Increased difficulties in reaching household survey respondents could adversely impact the quality of our data.*
- The statement should describe the event, and the potential impact of that event on the achievement of the organization's objectives. *Example: There is a risk that (event)....and the consequences are (impact)...*
- A good risk statement should also include the possible causes (drivers). *Examples: There is a risk that (event)...because of (cause)...and the consequences would be (impact)...; Given that...there is a risk that...with the potential impact of....*

Before any risk treatment is put in place, the event involves an "inherent risk", ontologically related to the activity that could determine the event itself; once the mitigating action has been put in action, all that's left is the "residual risk", whose value can be equal to, greater or less than the "inherent risk".

[3] Source: "Statistics Canada's Updated Operational Risk Exercise 2014", Statistics Canada - Statistique Canada

This page has been left intentionally blank

SECTION 1: RISK MANAGEMENT FRAMEWORK



This page has been left intentionally blank

1. Settling the risk management system

A risk management framework (system)[4] provides the infrastructure for delivering, maintaining and governing risk management throughout the organization. As a part of this framework, an organization should set up:

a. A risk management mandate, that is the board's statement for setting the direction and priorities for risk management, and through which "who does what" is established, and the proper authorization and necessary resources are given. This is the main expression of the governance of risk, through which the organization's board engages stakeholders in locating the different responsibilities for managing risks.
b. A risk strategy, that points out how risk management supports the organization's overall strategy and related objectives. It takes into consideration the external and internal context, focusing in particular on key stakeholders' demands.
c. A risk policy that provides a clear and concise outline of the organization's requirements for risk management within the organization's overall approach to governance. It includes the risk appetite statement, the human resources training program for supporting the risk management process, as well as a definition of risk assessment criteria.
d. An integrated risk approach supports quality management in improving statistical data integrity and quality, through identification, analysis and treatment of risks inherent to statistical and over-arching processes.

1.1 Risk management mandate and strategy

TAGS: Philosophy; Mandate; Scope; Plan.

A risk management strategy includes definition of the risk management scope and plan, as well as the discussion of risk management philosophy.

I. Risk philosophy

[4] The AS/NZS 4360:2004 standard uses the following definition of risk management framework: "*set of elements of an organization's management system concerned with managing risk*". Within this draft the clauses "RM framework" and "RM system" are being used as synonyms.

A risk management philosophy is the set of shared beliefs and attitudes that characterise how risk is considered in any organizational activities. It affects how risk management components are applied, including how risks are identified, the kinds of risks accepted, and how they are managed.

When the risk management philosophy is not developed, understood, or fully embraced by the staff, an uneven application of risk management across business units, functions, or departments is likely. Even when the philosophy is well developed, cultural differences among units resulting in variation in enterprise risk management application may still be found.

Therefore, risk philosophy, risk appetite and risk strategy should always be kept aligned, as one reflects the other. To this purpose it's necessary to "measure" risk perception by the management staff – as some managers may be prepared to take more risk, while others are more conservative – as well as the risk maturity of organizational context, since this latter could be more or less resilient in facing risk.

II. Mandate

A mandate in risk management expresses itself through an official statement/document, that clearly indicates the risk management strategy and objectives, the people accountable for them at all levels, and authorizes such people to use proper resources for achieving their assigned objectives.

Defining and communicating this statement testifies an organization's commitment to implement a risk management system.

Box 1 - An example of mandate among NSIs

"*Minimizing any significant risks arising during activities and services, through the application of effective risk management principles and practices. The organization will bear an acceptable level of risk, but only after weighing up the likelihood, consequences and cost of an adverse event occurring against the availability of resources to eliminate or manage the risk*".

Source: Australian Bureau of Statistics – Accountable Authority Instructions

III. risk management scope

Defining the scope of a risk management strategy means that all staff are made aware of the relevance of risk in achieving their objectives, as well as specific training for such staff is envisaged. It also means that a common approach to risk management is shared across the organization, including a common risk language.

IV. risk plan

To implement a risk management system, a risk plan is needed that includes:

- Risk management objectives (strategic as well as operational ones);
- Risk management activities, to be undertaken within a proper timeframe, to help the organization achieve its strategic objectives;
- Resources required, including people, knowledge and budget;
- Decisions regarding risk communications, internal and external.

It describes how the risk management strategy progress will be monitored, reviewed and reported.

Regarding the activities to be undertaken, several of them are crucial, whether resulting from an extended program or from a "quick" one through a "prototypal release" of the risk management system. The resources that an organization will invest in implementing such a system are also crucial, to determine the quality and progress of results.

1.2 Establishing risk management policy

TAGS: Risk appetite; Risk Profile; Top management; Commitment; Stakeholder.

To achieve consistency in risk management activities across the organization, the risk management policy should contain a high level overview and description of the risk management process.

The main features of the policy are:

- Definition of corporate risk appetite: the board and senior managers set the risk tolerance level by identifying general boundaries against unacceptable exposure to risk. The corporate risk appetite is then used to shape tolerance levels down the organization (see below);
- Implementation of a risk management standardized process at all levels, to ensure that risk management is an inherent part of how core-business is run (see Ch. 4);
- Top management involvement in risk management framework design (see below);
- Stakeholders' empowerment (see below and see also Section 2, Ch. 1);
- Definition of risk criteria (see Section 2, Ch. 3);

- Definition of a hierarchy of risks (see Section 2, Ch. 3);
- Implementation of a risk management unit/office (see Ch. 2);
- Definition of human resource training policy to support risk management process (see Ch. 2);
- Establishing a communication system (see Section 2, Ch. 1);
- Establishing a reporting system (see Ch. 4).

I. risk Appetite and risk Profile

Any organization intending to implement a congruous risk management system should define a Risk Appetite Framework (RAF), which is a framework connecting risks to the mission and strategic objectives, and so translating strategy into quali-quantitative variables. With reference to the risk profile (the "set of risks that may affect all or part of the organization") and consistently with the overall strategic plan, such a framework defines the leaning toward risk (risk tendency), tolerance thresholds, risk limits, risk governance, as well as any processes needed to outline and implement them.
An organization cannot consider risk as simply resulting from likelihood-per-impact in order to treat it: its management depends on the component variables involved in determining risk appetite, or "the amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time". Risk Appetite level mostly depends on the kind of activity performed, the products and services offered, and the regulatory and environmental contexts in which the organization operates.
The variables expressing risk profile-risk appetite ratio are as follows:

- Risk perception, which describes how people perceive risks according to their values and interests;
- 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, or 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 capacity, which is the maximum level of risk that an organization can assume without violating the regulatory burden;
- Risk retention, which considers stakeholders' conservative return expectations and a very low appetite for risk-taking;
- Risk tolerance, which is the level of variation that an organization is willing to accept around specific objectives.

While risk appetite is linked to strategic objectives, risk tolerance is mainly connected to the operational ones since through the latter the governing body sets up the maximum deviation allowed by risk appetite.

Figure 1: From the risk profile to the risk appetite definition

The Risk Appetite Framework (RAF) is a methodological scheme aimed at determining the organization's risk appetite level, through an evolving, iterative process, that helps the organization outline the amount of risk it is willing to take, in order to achieve its objectives according to the business strategy.

When outlining risk appetite, all strategic activities (planning, detection of financial and human resources, portfolio project selection, etc.) are determined according to risk-based thinking and criteria. It's up to the governing body to draw up the RAF through a statement (RAS – Risk Appetite Statement), comprising an official document that sets out risk objectives, as well as the ways to monitor their achievement and cascading them through the organization's operational processes.

In particular, the RAF should state:

- The types of risks an organization intends to take;

- For each kind of risk, any possible tolerance threshold and operational limit, under both normal and critical (at organizational/financial level) circumstances;
- Any procedures and/or actions to start if it becomes necessary to lead risk level back to either the objective or the limits established, especially if risk level reaches the tolerance threshold;
- The role of actors involved in defining and implementing the RAF (board, managers, auditors, operational units);
- Timing and procedures to monitor and update the RAF;
- Rules for sharing the RAF contents with all actors, both internal and external, involved in its definition and implementation.

Those organizations who effectively adopt a risk Appetite Framework are able to integrate it within their own decision-making processes, and strive to internally communicate and disseminate its contents, starting from the top management.

In defining its own risk appetite level, an organization should set up a template to identify tolerance thresholds for any activity area; for example, the template will show whether a particular activity within each area has a low, medium or high risk level and then, respectively, a high, medium or low tolerance level.

The RAF should contain any elements to be taken into consideration in order to determine the tendency to risk, for example, through designing a matrix in order to assess the risk tendency level for each activity, to be made by the respective risk owners.

A different level of risk appetite can therefore be outlined for the top strategic risks, as well as specific behaviours consistent with a pre-determined level of risk tendency; for this a matrix to support the decision-making processes can be laid down, in order to align the individual approach with the risk policies established by the top management: risk adverse; risk minimising; cautious; open to risk; or risk-taking.

II. Risk management commitment

Risk management design should be mostly contributed to by top management with the assistance of middle/low management and technical staff (for example, through mixed working groups). Particularly during the start-up phase, every organizational level should be involved in order to collect inputs and needs (for example, through *ad hoc* interviews). Employees know best the most typical and recurring risks in their area, and should be both encouraged and engaged to regularly give information about them.

Risk management goals should not only be clearly defined and communicated by top management, but also discussed within each of NSO's units. Each unit should have a contact person who is entitled to coordinate all the risk management activities, in cooperation with his/her colleagues, including the head of unit.

III. Stakeholders' empowerment

It is very important to establish and maintain proper risk frameworks, that ensure cooperation with stakeholders in achieving common objectives (e.g. the public's trust in the quality of official statistics; protection of confidentiality related to respondent data, etc.). An organization should regularly circulate information, as well as continuing dialogue about risk management with internal and external stakeholders, in order to ensure that everybody understands the basis upon which decisions are made and the reasons why particular actions are required.

For this purpose, the organization needs to:

- Periodically review interfaces;
- Check whether communication is correctly understood, and all communication channels are effective;
- Set up clear communication protocols in order to ensure there is a common understanding of the respective responsibilities;
- Implement a consultative team approach, to help properly define the internal and external context, and ensure risks are identified effectively; to put different areas of expertise together when analysing risks; to ensure different views are properly considered in evaluating risks; and to assure appropriate change management during risk treatment;
- Develop a communication plan for both internal and external stakeholders, at the earliest stage of the risk management process;
- Encourage, acknowledge and appreciate unsolicited views;
- Provide periodic feedback to show how well what was promised or projected has been actually performed.

For further information see Section 2, Ch. 1.

1.3 Risk management approaches

The coordination of the risk management process should be centralized: the risk office analyses and draws up information related to each process phase, and proceeds with strategic planning, in coordination with the organization's board.

The risk committee, with the risk manager playing the role of coordinator, sets up the criteria to select the most relevant information coming from the risk management information system (selective approach). Significant risks in terms of impact or strategic level

are reported by the office supporting the risk manager on a regular, specific and exceptional basis. The risk manager gives directions on translating strategies into risk management objectives, and monitors their achievement by divisions/offices and managers within their own competence. The risk manager therefore finalizes the information received, by adapting it to the organizational context (down to the any single office level), in order to correct possible deviations from strategic priorities.

Risk register development involves detailing organizational risks (corporate as well as project and operational ones), and setting up specific risk registers on particular topics (work health and safety, fraud, IT security, environment, etc.).

Three kinds of approach can be followed for involving management and stakeholders in identifying risks:

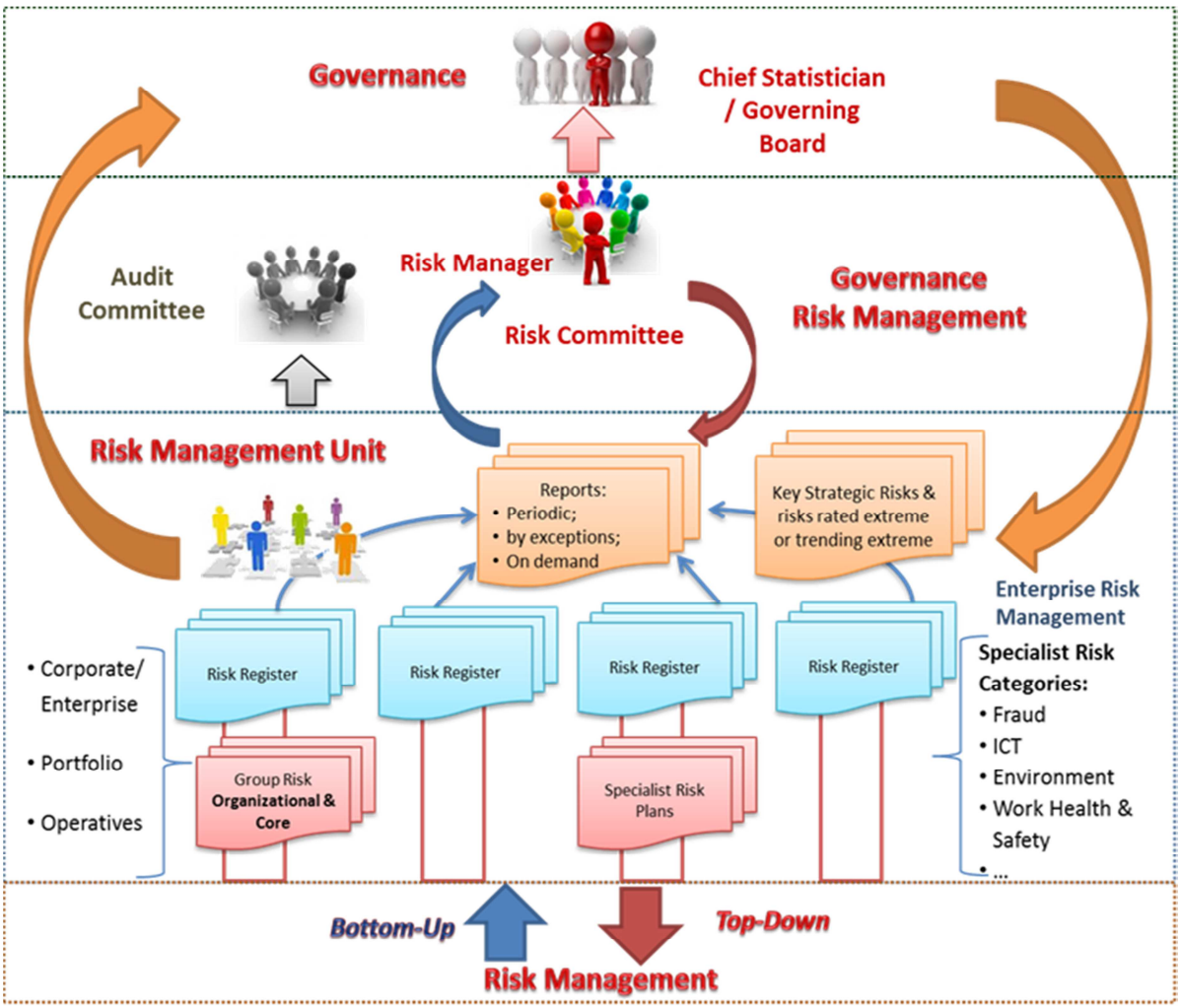
- **Top down-approach**: the decision-making process is centralized at governance level. This approach can show two modes: a) Full top-down mode, where the business units' risks are listed at department level, meaning that heads of unit cannot add risks themselves at unit level. There is no need of risk escalation, except at departmental level. b) Prevailing top-down mode, where a corporate risk register is directly created from a detailed operational risk register.
- **Bottom-up approach**: the decision-making process is done at management level. Operational risks are identified by any staff member while performing his or her daily work (e.g., in order to encourage the staff to be more active in defining non-conformities, an opportunity to register them online has been provided).
- **Mixed approach:** the board entity states the criteria (top-down) by which the heads of unit identify and manage risks (bottom-up). Risks may be viewed and assessed throughout the organization at any level (e.g., group, program, office, project, etc.). In order to set the framework, the hierarchy of risks on which attention is focused corresponds to the enterprise, operational and project levels.

Such approaches are not mutually exclusive, and a combination of approaches to the management of processes is desirable to achieve effective integration of risk management at any level within the organization.

These risk management approaches are also a way of cutting across the organization hierarchy and overcome organizational barriers.

The figure below outlines the risk management process according to the top-down perspective; it also highlights the information flows related to decision-making processes, according to the different roles involved.

Figure 2: risk management according to the mixed (top-down and bottom–up) approach



Source: Adapted from Australian Bureau of Statistics, risk management framework

In order to identify risks, the adoption of a suitable tool or method is needed. Two of the most commonly used methods are as follows:

- Commissioning a risk review: A designated team (either in-house or from outside) considers all the operations and activities related to the organization's objectives, and identifies the associated risks. Such a team should conduct interviews with key staff at all organizational levels, in order to build a risk profile for the whole range of activities. (However, it is important for this approach not to undermine line management's awareness of their own responsibilities in managing the risks that are relevant to their objectives.);
- Risk self-assessment: Each level and part of the organization is invited to review its

activities, and to contribute its diagnosis for the risks it faces. This may be done through paper documentation (with a framework for such a diagnosis set out through questionnaires), but is often more effectively conducted through a workshop approach, with facilitators helping groups of staff to work out the risks affecting their objectives. A particular strength of this approach is that ownership of risk is better established when the owners themselves identify the risks.

QUESTION MARK BOX

Q. With reference to the approach adopted, please detail the methodology being used while specifying roles, accountabilities and connections to the different process phases:

R. The process starts by engaging all Directors to respond to a risk questionnaire, to identify the top three/five risks from a divisional program perspective. For this purpose program-level risk registers were reviewed and approved by their respective Field Planning Boards, to ensure consistency in the understanding and relative importance of the risks identified at the divisional or program level. The results of this exercise are presented to the top-management board, who then provides its-own perspective on the corporate risks facing the organization.

Source: Statistics Canada, In-depth survey on risk management practices

QUESTION MARK BOX

Q. The selected organizational stakeholders have been involved in:

R. All stakeholders should identify risks: every staff member can inform process managers about draw-backs and risks identified in their process (Statistics Lithuania).

R. Risk identification and analysis should be dispersed around the organization and carried out by the departments, units, territorial statistical departments, teams and projects (Statistics Finland)

Source: Survey on risk management practices

1.4 Adopting an integrated risk approach connected to statistical quality management

TAGS: Approach; Statistical risk; Quality framework.

Risk management is essential to achieve the organization's strategic outcome, and such fulfilment can only be reached by ensuring that risk is included as a routine in all significant decision-making. This means that risk management should be part of the organization's culture, embedded in every organizational process, including production and supporting processes.

This requires an agreed approach, integrated with corporate strategy, that outlines exposures, issues and potential problem areas: integrated risk management should result in a system that is a part of the regular organizational performance review, where the

organization not only looks at performance and events, but systematically identifies important gaps, variations and exposures, in order to get ahead of (mitigate) their possible impact.

From a practical point of view:

a. Risk management should not be seen as a separate system, existing independently from the way in which the organization manages itself, makes decisions, allocates resources and holds people accountable.

b. Risk management cannot take place at some levels if that means excluding other ones.

c. Risk management cannot take place in only a few parts of the organization.

According to the holistic approach, risks should be viewed and assessed at any level in the organization. They should be a major consideration in approving proposals for investment, and integrated into tools for project management and performance monitoring. Accordingly, they should be integrated into key accountability documents, and internal strategic and project planning.

The most advanced statistical organizations have developed integrated models, based on an enterprise-wide perspective of risk, adopting standardized terms and concepts to promote effective implementation across the organization.

In these systems, all aspects of internal control are developed through a risk-based approach, built on the following criteria:

a. Policy positions reflect the risk appetite of senior management, and are developed to guide the behaviour of empowered staff in managing the risks that they face in performing their assignments.

b. Governance arrangements ensure transparency and accountability in decision making, by promoting strong leadership, sound management, and effective planning and review.

c. Planning and reporting provide great opportunities to document goals and related risks.

d. Assurance activities are a part of Internal audit, aimed at verifying that risk management within an organization is run consistently with international standards and established practice[5]whilst giving due consideration to the importance assigned to the organization's objectives.

e. Organizations should align risks to internal controls to ensure that, where possible,

[5] Internal audit should be carried out by an independent organizational unit, playing an advisory role and providing independent assurance and assistance to the Chief Statistician (see Section 2, Ch. 5)

each risk has controls, and that each control addresses these risks.

Such NSOs have adopted an integrated risk management framework by identifying – in addition to general risk management – a specialized risk management which addresses persistent risks (for example, fraud, work health and safety, Information and Communication Technologies (ICT) security and disclosure risk)[6]. They also put a strong focus on managing statistical risk, defined as the possibility that one or more of the production process components fail to meet the quality standard established, so resulting in a lower statistical output quality or integrity. Given that statistical risks are unavoidably managed at all levels (strategic, operational and project ones) within a NSO, it is worth noting that even when they are managed separately, they should eventually be integrated into an organizational risk framework.

Considering the strong connection between quality and risk[7], risks can be treated by applying quality management, especially at operational level.

Indeed, risk management and quality management are similar, in that:

- Quality management usually defines requirements, and assesses whether and when they are met (through review, audit, etc.). If requirements are not met, correction actions are implemented;
- Risk management identifies threats (risk sources) that can affect objectives. If risk level is too high, mitigating measures are implemented.

Even though a lot of general quality frameworks exist in literature, applications of continuous quality improvement approaches among NSOs are still limited.

In implementing their framework for statistical business process quality improvement, NSOs should pay particular attention to:

- Extracting key elements and possible relations for a general quality framework of statistical processes from these existing models;
- Adopting a common vocabulary for quality and risk management.

A first step in implementing a quality framework, independent of the standard adopted, is to design process flow map(s), in order to identify the points where product and process quality can be measured.

---

[6] One Institution that manages all these persistent risks is the Australian Bureau of Statistics (ABS), which has also developed a quality improvement framework of the statistical chain based on risk management (see Annex).

[7] A) Quality is defined as the extent to which characteristics of an object meet the requirements (ISO 9001:2015). Risk is defined as the effect of uncertainty on objectives (ISO 31000). Objectives can be regarded as high level requirements. B) Traditionally, quality is focused on product quality and customer satisfaction (ISO 9001). However, the definition of quality can be applied to other objects such as processes, input as well as the institution as a whole.

Process mapping can help to understand how a system works, and identifies how a system interacts with other systems and processes.

Another key step is to identify the statistics quality demands from users with respect to the process under consideration[8]. Quality demands should encompass both quality criteria, and demands related to risks. A process is in control when quality criteria are met and risks are acceptable.

NSOs could use the Generic Statistical Business Process Model (GSBPM) as a guide to map the activities of statistical processes. This ensures that all steps of a statistical process are included for monitoring purposes: For example the "Collect" phase of the GSBPM includes any activities related to obtaining data. Considering the recent adoption of the Generic Activity Model for Statistical Organizations (GAMSO), which extends and complements GSBPM by adding other activities which are needed to support statistical production, it would be useful to introduce this standard in order to support implementation of an entire risk management system.
In particular, according to the GAMSO model:

- The risk management governance system and the corporate risk management (i.e. the overall risks that can affect the NSO's strategic objectives), could be placed within the "Strategy and Leadership" activity area, under "Govern and Lead";
- The statistical risk management, related to the identification and monitoring phases of the risk management process, could be placed within the capability management activity area, under "Plan/Monitor capabilities". These kind of risks, which could impact on data quality, are often connected with the correct application of statistical methodologies and production standards;
- Referring to the identification and treatment of organizational risks, the operational risk management connected to supporting activities (i.e. Finance, Human Resources, ICT), can be placed in each sub-area of "Corporate support". In this activity area, there are also specific types of risks (i.e. fraud risks);
- The management of operational statistical risks at the business level, is a routine activity under the responsibility of the risk owners, with regard to the identification and treatment phase, in order to ensure statistical quality and successful delivery.

[8] BLUE-ETS Project : SP1-Cooperation-Collaborative Project /Small or medium-scale focused research project/FP7-SSH-2009-A/Grant Agreement Number 244767/ Deliverable 7.3

2. Risk management resources

TAGS: HR allocation; Internal stakeholders; Organizational changes; Organizational climate; Organizational culture; Risk management training; Skills and competencies.

2.1 Risk organizational culture

Risk management initiatives can promote employees' sense of belonging to a group, as well as their own significance within the organization. (People can cooperate to set up a risk management system, an asset management, to define the cross-organizational measures, and so on.) Moreover, risk management provides a systematic standard mechanism of internal control, that obliges all staff to come together from different areas to discuss, and identify issues and solve problems. These activities also contribute to the quality of the working culture, and allow staff to feel valued and engaged in the process of achieving a broader organizational objective.

Human resources are recognized as one of the key elements for organizations' successfulness[9] and some uncertainties which give rise to risks can actually come from the organization's internal environment.[10] For example, the way in which top management reacts to the results of monitoring may affect the behaviour of employees; the organization should be quite clear about the uncertainty arising from reliance on a single individual to make a large modification to risk, and should properly reward efforts by individuals. When designing the framework, and implementing the risk management process, specific actions are needed in order to integrate such human and cultural factors.

Change, and cultural change in particular, is a weakness in risk management: the process is not the problem, but rather people's perception of it. Two important lessons learned from implementing risk management are: embedding clear risk-based thinking at the highest level of the organization, while ensuring that it cascades down to lower management and employees; presenting the risk based thinking not as something totally new (to reduce resistance to it) and showing it as an important feature of any change process.

Job profiles (outlining role, performance expectations and development objectives), should be identified for staff responsible for risk management matters, and specific descriptions on

[9] Cf. Porter M.E., 1990.

[10] ISO/TR 31004:2013(E) reports common types of error related to human and cultural characteristics: a) failure to detect and respond to early warnings; b) indifference to the views of others or to a lack of knowledge; c) bias due to simplified information processing strategies to address complex issues; d) failure to recognize complexity.

particular issues should be included in the job profiles of the general risk manager and risk officers.

An organization should establish **preventive human resource controls** to reduce the likelihood and/or impact of adverse and critical events like noncompliance and misconduct[11]. Consequently, the organization should enhance and/or revise the prioritized risk matrix and, as needed, the risk optimization plan to reflect implemented human resource incentives, according to current residual risk analysis and performance against planned residual risk analysis.

QUESTION MARK BOX

Q. Have job profiles been identified for the staff assigned to run risk management matters?

R1. "Specific descriptions on risk management issues are included in the job descriptions of risk officers and heads of units"

Source: Romania, *In-depth survey on risk management practices*

R2. "Yes, done. There is a job description for the general risk manager. The risk manager of Statistics Austria holds a certificate of senior risk manager with regard to ÖNORM EN ISO 31000 and ONR 49003 (Austrian Economic Chamber, WIFI-Zertifizierungsstelle)"

Austria, *In-depth survey on risk management practices*

R3. "All staff have a Development and Performance Agreement (DPA) which outlines their role, performance expectations and development objectives. Roles in relation to risk will be articulated in broad planning and in the individual DPAs but it may not be reflected in a title. In addition, roles in relation to managing specific risks are identified in the risk management documentation"

Australia, In-depth survey on risk management practices

2.2 Training

To effectively implement a risk management system, an organization should allocate **appropriate resources, suitable human capital** as well as ensure that those who are accountable can fulfil their role by providing them with the **training and skills** needed. All staff should be aware of the relevance of risk to achieve the objectives assigned and training to support staff in risk management should be available. Awareness and ongoing support enables individuals to know what is expected and reduces the likelihood of errors.

An organization should identify the presence and effectiveness of current actions and controls in order to deal with threats and opportunities. That includes use of education and

[11] At this end, as an example of potential sub practices, an organization can also: define which duties should be segregated to prevent critical events; develop awards and other incentives for contributions by individuals or units that result in reduced residual risk or compliance failures, enforcement actions or other positive challenges to the organization.

awareness programs. The organizations should also conduct a structured needs assessment identifying risk and training needs (e.g. general control system, specific training on risk management systems, internal control standards, dedicated tools, statistical quality modules, etc.) as well as establish appropriate training and support for responsible personnel. Finally, they determine which kind of awareness, education and support practices should be put in place **for each policy and target audience**.

It is advisable to start training with a program devoted to managers and employees assigned to run risk management matters at different levels; it would be best if kick-off training activity focuses first on higher-risk areas. It is also important to carry out training initiatives regularly, in accordance with risk management system development, as well as concurrently with significant organizational changes.

RM training needs to be integrated into existing job training, both if risk management is considered a tool for improvement and for the sake of economic efficiency. Using a suitable level of technology and develop e-learning tools to reach a broader target audience are advisable to disseminate education and awareness. The organizations should also plan *ad hoc* sessions dealing with topics and issues specifically related both to quality and risk management, and in connection with broad organizational change processes requiring careful and effective management of the transitional phase, they should envisage specific training initiatives and/or *ad hoc* events aimed to describe how risk management does represent a change strategic lever.

QUESTION MARK BOX

Q. Please point out the frequency of the specific training initiatives delivered from the start of the risk management system, regardless of their kind:

R. "Yearly training on risk management and Internal Control System (ICS) in the framework of workshops (RM, ICS) with an external expert. A presentation of the risk management system is provided to all new staff members within Statistics Austria's general training programme (half-yearly)".

Source: Austria, *In-depth survey on risk management practices*

2.3 Delivering roles and responsibilities

TAGS: Roles; Responsibilities; Accountabilities

Risk management should work at any organizational level, as well as through participation by the entire staff, according to respective roles and functions.

The governing board is responsible for ensuring the setup of an effective risk management system throughout the organization;

The risk committee/board entity is an oversight entity ruling the risk management system together with other strategic matters. The committee/board sets risk appetite in cooperation with senior management, and communicates it throughout the organization. The committee/board is responsible for: monitoring compliance with the organization's risk policy; monitoring the adequacy of controls; monitoring changes to the organization's risk profile, considered as a part of the organization's strategy and planning processes; assisting the senior management in selecting the key risks; periodically reviewing the risk management reporting system as well as the adequacy of risk management resources; escalating and reporting material risk issues to the chief statistician for consideration.

The risk manager works under the guidance of the committee/board, and is skilled (or even certified) in risk management, and supported by sufficient staff for the size of the organization (see below risk management unit). The risk manager is responsible for: cooperating with top management in identifying high risk areas related to strategic or business processes; cooperating with top management in defining treatment actions related to key risks and supervising the risk management process. Its role should also include: promoting a consistent use of risk management and ownership of risk at all levels within the organization; building a risk-aware culture throughout the organization, including proper education and training; developing, implementing and reviewing risk management; coordinating the other advisory functions on specific aspects of risk management; coordinating responses when risks impact more than one area; managing quality within risk management; reporting, escalating and communicating risk management issues to key stakeholders.

Top management is responsible for: ensuring that there is a fit-for-purpose and up-to-date risk management framework, that processes are in place and that risk management is adequately resourced and financed; providing strategic direction on the appropriate consideration of risk in decisions, setting risk appetite and associated authority; approving the risk management policy, and disseminating culture on managing risk; ensuring that key risks facing the organization are properly assessed and managed; providing direction and receiving feedback on the effectiveness of risk management and compliance with the risk management policy.

The Head of department/divisions/units must actively manage risks that are part of daily work through complying with the enterprise risk management framework. In particular, such offices: establish risk management objectives and formulate key risk indicators; clarify the risk management strategy and risk appetite to their staff; implement the risk management processes; manage the risks that fall within their areas of responsibility; cooperate in identifying key risks; monitor risk management action programs; regularly report to senior management any news or changes to existing risks, or failures of existing control measures.

All staff must take risks into account when making decisions and are responsible for an effective management of risks, including identification of them. All staff are responsible for understanding and implementing risk management policies and processes.

Internal audit (see details in Section 2, Ch. 5) is responsible for reporting to the board on the adequacy of risk management processes within the organization, giving assurance on: their design and how they are working; the effectiveness of controls and response actions to key risks; reliability and suitability of risk assessment. The achievement of the internal audit mandate is performed by an independent office that directly reports to the chief statistician.

The risk management unit is coordinated by the risk manager and is responsible for: collecting the risk identification form that is filled in by those structures (directorates, divisions, units) under the responsibility of the related risk owner; analysing these forms and proposing preliminary treatment actions, escalating risk if it exceeds the unit's level of authority; validating the closing solution; setting tasks, risk-indicators, targets and deadlines for proposed actions; preparing documentation for escalated risks and submitting it to appropriate management level (in particular for cross-cutting actions); monitoring the implementation of control actions, to evaluate the results and proposing corrective actions; filling-in the risk register; filing risk documents; preparing risk documentation and submitting it to the risk manager; preparing risk management meetings.

Descriptions of tasks, deadlines and responsibilities for all the risk management process actors must be included in a procedure to be made known throughout the whole organization.

3. Risk management process (see Section 2)

The risk management process is an element of the framework, and is derived from the risk management policy, which it operationalises.
The risk management process is a systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context of, assessing, monitoring and reviewing risks.
It comprises the following activities:

1) Communication and consultation;
2) Contextual analysis;
3) Risk Assessment:
    a. Identification;
    b. Analysis and measurement;
    c. Weighting;

4) Risk treatment;
5) Monitoring and review.

The process should also concern the risk based audit and information system support in all phases.

Section 2 in this paper contains an analysis of each process phase.

4. Monitoring and reporting

4.1 Monitoring and review of the framework

TAGS: System deviations; Risk management plan; Context Changes; Feedback.

In order to ensure that the risk management system is effective and continues to support organizational performance, an organization should:

1. *Periodically measure progress against and deviation from the risk management policy and plan*: the framework and processes should be fit-for purpose, and aligned to the objectives/priorities of the organization, and relevant stakeholders should receive adequate reporting that enables them to fulfil their roles and responsibilities within the governance structure;
2. *Periodically review whether the risk management framework, policy and plan are still appropriate, given the organization's external and internal context:* the organization should ensure that changes to the context, or changes to other factors affecting the suitability or cost of risk management, are identified and addressed;
3. *Periodically review the risk management process:* the risk management resources should be sufficient, and people across the organization should have adequate risk management skills, knowledge and competence, in line with the risk role they are required to perform on a daily basis;
4. *Periodically review the risk management maturity level* : With a view to achieving continuous improvement, an organization should self-assess the level of its risk management development, to point out strengths and weaknesses and design and/or review a lasting path of growth for the risk management system itself;
5. *Periodically report on the results of monitoring to the board*: based on the results

from monitoring and review, decisions should be made to improve the organization's management of risk and its culture, ensuring that the organization is able to learn from risk events.

4.2 Establishing reporting mechanisms

TAGS: Reporting system; Executive and Operative reporting; Stakeholders' report; Accountability.

An organization should ensure that information about risks derived from the risk management process is adequately reported, and used as a basis for decision making at all relevant levels. For this, clear reporting line mechanisms and strong inter-department knowledge sharing should be established in order to encourage accountability of risk, and to ensure reports are delivered in an accurate, consistent and timely manner. Moreover, the risk management policy (see Ch. 1) should clearly state the way risk management performance will be reported.

Inadequate risk reporting[12] can lead to a failure to fully integrate identified risks into strategic and operational decisions. The organization should report on progress against the risk management plan by proving how well the risk management policy is being followed, to ensure that risk management is effective and continues to support organizational performance. More specifically:

1. The results from risk monitoring and review should be recorded and reported internally and externally, if appropriate;
2. Development in implementation of risk treatment plans should be incorporated into the organization's overall performance management, measurement and internal and external reporting activities, as a performance measure;
3. Enhanced risk management includes continual communications with external and internal stakeholders (see Section 2, Ch. 1), including comprehensive and frequent reporting of risk management performance, as a part of good governance.

The quality and success of risk reporting depends on the following factors:

- Target audience;
- Input and processes;

[12] ISO Guide 73:2009 defines risk reporting as a form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management.

- Frequency;
- Content;
- Format;
- Dissemination channels.

Determining the **target audience** is important because it affects other risk reporting decisions. Whenever a disclosure is demanded by a regulatory requirement, the organization must comply and provide appropriate disclosure. On the other hand, voluntary disclosures should be subject to cost-benefit analysis of audiences' needs and the kind of disclosure (type and detail of risk). Reporting organizational risks should operate on multiple levels to address the needs of diverse audiences, each with their own specific needs, requirements, expectations, agendas and levels of expertise. In this regard, there are two areas of risk reporting:

a) Reporting to **internal audiences**.

b) Reporting to **external audiences**.

The reporting of risks is essential for internal decision makers to integrate risk evaluation into their operational and investment strategy, to review performance, and to review compensation/reward decisions. External risk reporting has rapidly developed in recent years: corporate governance reports also focus attention on internal control, and a review of risks is generally included in the annual reports. Both internal and external audiences can be further divided into two subgroups: on the one hand, some audiences (i.e., boards of directors and regulators, among external audiences) must be informed about the organizational risks and risk management processes because of regulation or recommendations. Voluntary disclosure to other internal audiences (i.e., employees) and external stakeholders (i.e., media, citizens' associations) is recommended because of anticipated benefits to an improved decision-making.

'**Inputs**' and '**processes**' are also critical. The most important **inputs** are represented by:

I. The various risks an organization is facing;

II. The stakeholder risk reporting requirements and expectations;

III. The organization's existing risk management governance, that provides the context for establishing risk reporting processes;

IV. The organizational resources (such as individuals with the necessary skills and experience, financial resources, and access to required information).

Decision must be taken on which risks to report, in what detail, and with what **reporting frequency**.

a) Internal reporting

The organization should establish internal reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that: key components of the risk management framework, its effectiveness and the outcomes and any subsequent modifications, are properly disseminated; relevant information derived from the application of risk management is available at appropriate levels and times; there are processes for consultation with internal stakeholders (see Section 2, Ch. 1). These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information. Internal risk reports can either be real-time or periodic.

The main purpose of **periodic internal risk reports** is to provide aggregate information about various relevant organizational risks, with trend indicators and periodic comparisons highlighting changes in risks. Periodic internal risk reporting contributes to strategic oversight and decision-making, as well as improved operational business decisions. Risk information may be organized around specific key risk categories rather than around phases of the risk management process. Residual risk reporting involves comparing gross risk (the assessment of risk before controls or risk responses are applied) and net risk (the assessment of risk, taking into account any controls or risk responses applied) to enable a review of risk response effectiveness and alternative management options. Risk reporting to the board and committees should be made at least quarterly.

Internal audiences will not only be interested in disclosure of specific risks, but also in the risk management process. A well established and properly managed process will assure internal audiences about the reliability of risk reports: organizations must therefore include information on the quality of their risk management process, particularly in their periodic risk reports.

Comprehensive and frequent internal reporting on significant risks and risk management performance and process substantially contributes to effective governance. In this respect, different levels within an organization who need different information from the risk management process require different report types:

- ***Executive reporting***. The board of directors has the highest oversight responsibility for developing and implementing the organization's mission, values, and strategy, and must carefully review corporate processes of risk identification, monitoring, and management. The board also sets risk philosophy, risk appetite, and risk tolerances. Specific reviews of financial objectives, plans and other significant material transactions also typically fall within a board's responsibility. These responsibilities require broad and transparent reporting on the various organizational risks (strategic,

operational, reporting and compliance risks). Appropriate communication **to the board** includes reporting on:

- Progress against organizational objectives and related risks;
- Effectiveness of the ongoing monitoring processes on risk and control matters, including reporting any significant failings or weaknesses.

Risks can crystallize quickly, and the board should ensure that there are clear processes for bringing significant issues to its attention more rapidly when required, and agree triggers for achieving this. The board should also specify the nature, source, format and frequency of the information it requires, and monitor the information it receives, ensuring that information quality is sufficient to allow effective decision-making.

- ***Operational reporting*.** The risk management system should include procedures for immediately reporting to **appropriate levels of management** any significant control **failings** or weaknesses that are identified, together with details of corrective actions being undertaken. Individuals should systematically and promptly report to low and middle level management any perceived new risks or failures of existing control measures. Middle level management should systematically and promptly report to senior management any perceived new risks or failures of existing control measures. Without proper internal reporting on organizational risks, managers cannot make optimal tactical decisions. Senior management needs relevant and reliable risk reports on a real-time and periodic basis for effective control: an example is represented by the risk matrix, a table in which rows show the risks and columns show their likelihood of occurrence and their impact.
- ***Review/audit report***. Not every risk has an internal control, but every internal control should address a risk. Internal audit reports are a key source of information on the organization's performance and control environment, to align internal controls to risks. The output of a review or audit will be a report summarizing its findings, and providing conclusions of the assessment against pre-determined criteria. This report may provide recommendations for system improvements, based on what the reviewers have observed. An annual report on the overall state of the organization's internal controls should be also provided (see Section 2, Ch. 5).

QUESTION MARK BOX

Q. In your Organization, risk management reporting is about:

R. "Management goals, results of risk workshops, identification and measurement high priority risks, monitoring of risk treatment actions. Monitoring of the implementation of strategic goals is also part of the risk management reporting. The risk management reports are provided to the management, risk owners, staff involved and to the Economic Council".

Source: Austria, *In-depth survey on risk management practices*

b) External reporting

Organizations are under increasing pressure for greater transparency, mandated or voluntary, and a **better alignment of externally reported information with that which is reported internally**. Stakeholders expect intensified corporate dissemination regarding risk, and awareness of the critical role of proper risk management. In view of this, an organization should provide accurate, timely and high quality reports to meet the external stakeholders' needs. Specifically, it should periodically conduct a review of the effectiveness of the risk management system and report to stakeholders on that, and a robust assessment of the principal risks, describing them and explaining how they are being managed or mitigated.

Organizations may consider preparing different, customized risk reports for different external stakeholders. Whilst internal risk reports aim exclusively at internal audiences, external risk reporting, including corporate annual reports, may more broadly include both external users and interested internal groups.

QUESTION MARK BOX

Q. If a specific risk management report with external stakeholders is envisaged, please describe its content:

R. "General description of the risk management system (in relation with initiatives within SSE and UNECE); Objectives related to risk management processes; Main risks identified, treatment actions; Monitoring results, outcomes; Escalated risks, proposed course of action; Improvement of the risk management system, next steps".

Source: Romania, *In-depth survey on risk management practices*

Q. Please specify the frequency of the risk management report that is addressed to the external stakeholders:

R1. "On demand".

Source: Canada, *In-depth survey on risk management practices*

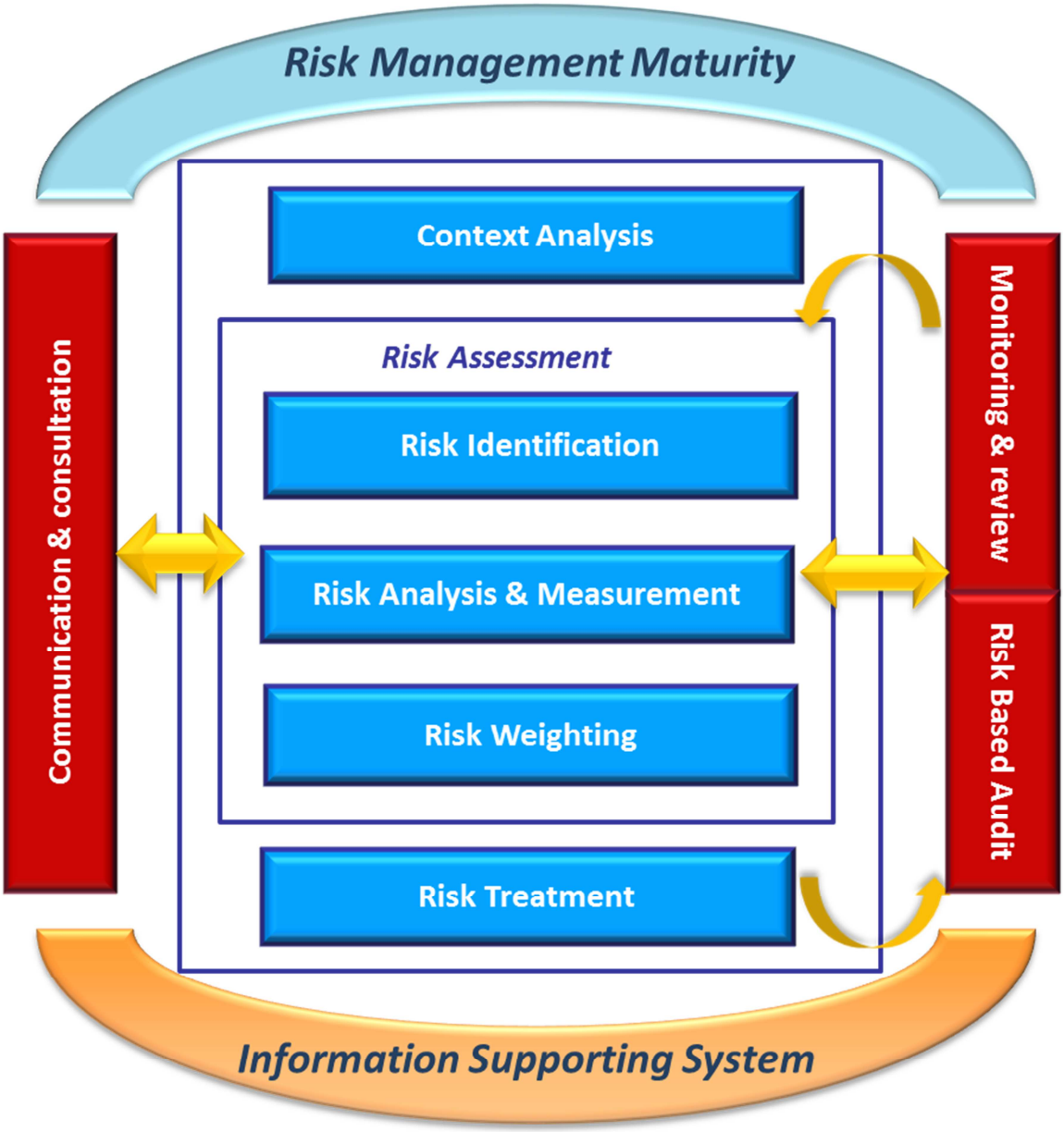
R2. "Yearly".

Source: Romania, Australia, *In-depth survey on risk management practices*

R3. "Quarterly, Yearly".

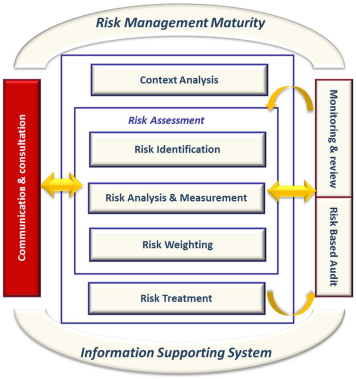
Source: Lithuania, *In-depth survey on risk management practices*

SECTION 2: Risk management process



This page has been left intentionally blank

1. Communication and consultation[13]



TAGS: Stakeholders' involvement; Internal communication; External communication; Information flow; Communication tools.

An organization should ensure that everybody within its staff, according to their role, knows the organization's risk strategy, risk priorities and related accountabilities. Board responsibilities, among other things, include ensuring sound internal information and communication processes, and taking responsibility for external dissemination on risk management and internal control. 'Communication and consultation' is not a distinct stage in the management of risk, but runs through the whole process. Communication and consultation is important because stakeholders also make their own judgments about risk, based on their own perceptions, which should be identified, recorded[14] and integrated into the decision making process.

Consultation with stakeholders needs careful planning, because it can build or destroy trust. To strengthen trust in the results of the process and obtain endorsement for a treatment plan, stakeholders should be involved in all aspects of risk management, including design of the communication and consultation process (see the following sections: Par. 1.1, Par. 1.2).

A plan to disseminate and to account for risk management should involve:

- Engaging internal and appropriate external stakeholders to ensure truthful, relevant, accurate and effective exchange of information, taking into account confidentiality and personal integrity aspects;
- External reporting to comply with legal, regulatory, and governance requirements (see SECTION 1, Ch. 4);
- Providing feedback on communication, consultation and reporting mechanisms.

[13] ISO Guide 73:2009 defines 'communication and consultation' as continual and iterative processes regarding the management of risk, that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders. Consultation is considered a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction.

[14] Records of communication and consultation will depend on factors such as the scale and the sensitivity of the activity.

QUESTION MARK BOX
Q. What are the most important lessons learned from implementing risk management in your organization that other organizations should take into account when developing their own risk management processes?
R. "When developing their own risk management processes, National Statistics Institutes should take into account that it is essential to ensure listening and using feedback"
Source: UK, *Survey on risk management practices*
Q. What are the strengths of the risk management system in your organization?
R. "All employees and necessary stakeholders are consulted during the risk management process"

Source: South-Africa, *Survey on risk management practices*

1.1 Internal communication

Two-way communication with the internal audiences (i.e. board of directors; audit/internal control steering committees, if any; all management levels; employees; integrated supply chain partners/other partners, according to an open organization vision) should be considered as a way to improve the risk management process. Facilitating risk management policy implementation and general engagement in the different process phases is crucial to the entire system effectiveness. Open communication helps decision making processes to use risk management information. Moreover, it helps in the identification of the *corporate risks*[15], and elicits the cross-organizational actions to be implemented in cooperation with the different divisions.

The organization should establish internal communication flows in order to support accountability and ownership of risk, along with widespread involvement. These mechanisms ensure that key components of the risk management framework, as well as any subsequent modifications, are properly communicated and submitted for consultation. Internal communication and consultation mechanisms include the methods and tools through which an organization ensures that everybody within the organization understands the following issues, according to his/her role:

- What the risk strategy consists of;
- Which the risk priorities are;
- How the accountabilities are assigned, and how the related responsibilities fit into the risk framework (who does what).

[15] risks/criticalities gathered into categories according to their strategic significance, and monitored and treated as a priority.

Identification of new risks (or changes in those risks already assessed) depends on maintaining a good communication network through relevant contacts and provision of information. If this is not achieved, risk priorities may not be consistently addressed. A consultative team approach may therefore be useful to help define the context for ensuring that risks are identified effectively, to bring different areas of expertise together in analysing risks, to **ensure different views are appropriately considered** in evaluating risks, and to make appropriate change management during risk treatment.

Risk management goals should be discussed within each organizational unit or project[16] and clearly communicated (for example through the 'risk appetite' statement). All staff, both management and non-management employees (and necessary internal stakeholders), should be consulted during the risk management process. Risk identification and response should result from a cooperative effort involving key elements from every project or process, as well as feedback from management on the integrated risk management process[17]. Moreover, in concrete statistical areas, cross-institutional commissions and working groups can play an important role.

To summarize, the internal communication:

- Assists in embedding the desired behaviours throughout the organization;
- Engages staff in risk management activities;
- Enhances risk management process transparency, and encourages accountability and ownership of risks;
- Facilitates cooperation among the offices/units in defining cross-cutting initiatives, and a common understanding of concepts, rules for action and integration of risk management in statistical processes, as a basis to prioritize control actions for continuous improvement.

Consequently, a **risk management plan**, as an internal communication plan, should include:

- Establishing a team responsible for communicating about risk management;
- Raising awareness about managing risks and the risk management process throughout the organization.

Plans/policy papers, methodological documents, and information resulting from the risk management system, should be disseminated and made available to all employees. Specific

[16] As an example, a risk matrix can be elaborated, as a teamwork task - under the direction of those responsible for any major statistical and/or organizational project - and the results should be communicated to every participant in the project, in order that they may be aware of their respective duties.

[17] Usually on a yearly basis.

communication **channels**, can include: internal events (e.g. workshops, seminars)[18], broadcast e-mails, broadcast voice mails, databases supporting specific risk issues, letters from the board, e-mail discussion groups, intranet sites on enterprise risk management, web info sessions, conference calls, posters or signs reinforcing key aspects of enterprise risk management, face-to-face discussion, newsletters from the chief risk officer, field debriefing sessions, knowledge sharing systems (e.g. wikis).

QUESTION MARK BOX

Q. Risk management goals are clearly communicated within your organization.

R. "Strongly Agree. The procedures and other documents related to the risk management process are disseminated within the body in charge of monitoring, coordination and methodological guidance of the internal/managerial control system development of the NIS. It should be composed of top management from all statistical domains".

Source: Romania, *In-depth survey on risk management practices*

1.2 External communication

An organization should periodically inform and consult its external stakeholders:

a. About how risks are managed;

b. To deal with stakeholders' expectations about what the organization can actually deliver;

c. To assure them that the organization will deliver in the way that they expect.

Effective external communication and consultation ensures that stakeholders understand the basis on which decisions are made.

The 'Risk profile' should be developed through a comprehensive process, including review of risk information and reflecting recommendations from different sources. It is important that organizations consider each of their significant relationships with partners, contractors and third parties, and ensure that appropriate communication and understanding about respective risk priorities are achieved. Communication to external stakeholders about risk issues is crucial: misunderstandings on respective risk priorities can cause serious problems.

[18] Especially during the start-up phase, meetings with all the organizational divisions involved should be organized to discuss various topical issues in more detail, and providing every staff member with the opportunity to express their opinion and to participate in the decision-making process. Presentations from senior leaders should show support and set expectations for staff in relation to risk, so positively grounding a risk culture.

A regular and well-made risk management stakeholder relationship plan should take into account and determine its critical components: dissemination strategy and channels. With reference to the first element, the corporate site is particularly useful for external real-time risk communication. With respect to external periodic risk communication, parts of annual reports or quarterly reports (electronic and/or hard-copy version), are generally viewed as the main channels. Possible communication tools to share information with external stakeholders and to promote dialogue are as follows:

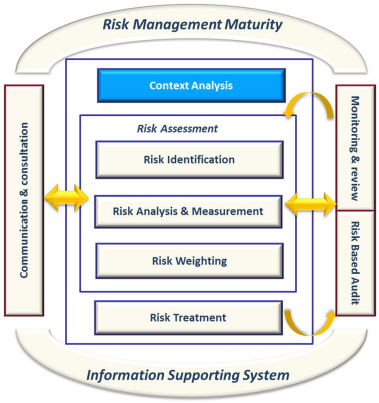
1. Corporate site;
2. Publications and papers;
3. Annual meetings;
4. Other external events (e.g. conferences, scientific meetings, workshops, seminars, days of study);
5. Corporate newsletters;
6. Messages integrated into ongoing corporate communications.

Whatever method is practiced, the communication goal should be to provide external audiences with a sound basis to make comprehensive assessments of reported data (see Section 1, Ch. 8).

Above all, a model of risk communication should integrate, instead of fragment, the risk-related information that an organization uses for external disclosure. The challenge is to inform the average member of the external audiences, while being fair and balanced in covering all critical perspectives.

QUESTION MARK BOX
Q. If risks are identified with internal and/or external stakeholders please indicate what kind of consultation is used.
R. "Users of statistics, respondents and other national producers of official statistics should have possibility to make suggestions, comments, complaints. A single contact point is established"
Source: Lithuania, *Survey on risk management practices*

2. Context analysis



TAGS: Context; analysis; process; mapping.

2.1 Establishing the context

The different maturity level of NSOs should be taken into account when designing risk management. The state of projects, programs and the portfolio maturity level of the NSO should be assessed before the beginning of the risk management process. In particular, it is important to identify, classify (general, specific) and assess risks related to implementation of the organization's strategy (so-called "risk of risk management")[19].

To ensure proper accuracy and quality, a detailed consideration should be undertaken of the context in which the risk management process will take place.

Establishing the external context ensures that stakeholders and their objectives are considered when developing risk management criteria, and that externally generated threats and opportunities are properly taken into account.

Evaluating the organization's external context may include, but is not limited to:

- The legal, regulatory, environment (whether international, national, regional or local);
- The financial, technological, and economic environment;
- Competitive environment analysis;
- Key drivers and trends having impact an on the organization's objectives;
- Relationships with, as well as perceptions and values from, external stakeholders[20].

[19] For details on risk Maturity Management see Ch. 8. For a focus on risk Maturity Management Practices see the Appendix.

[20] Persons or organizations that can either affect or be affected by or perceive themselves to be affected by any decision or activity.

As risk management takes place in the context of the organization's goals and objectives, it's necessary to understand the internal context.

Organizational analysis and process mapping are two tools which can support this work. Organizational analysis takes into consideration:

- Governance, organizational structure;
- Policies, objectives, and the strategies set to achieve them;
- Resources and knowledge (e.g., capital, time, people, processes, systems and technologies);
- Information systems;
- Relationships with, as well as perceptions and values from, internal stakeholders and the organization's culture;
- Standards, guidelines and models adopted by the organization.

Through process mapping, all processes are broken down, analysed and represented while identifying inputs, information flows, roles and accountabilities and outputs for each of them.

2.2 Process[21] mapping

Risk management system implementation requires a deep and documented process analysis, concerning the whole organization: it must increasingly involve all activities while distinguishing among the core and cross-cutting ones, down to detailed operational activities. Process mapping should allow an organization to carry out 'risk identification' (see Ch. 3), describing objectives, staff, activities, responsibilities, organizational units, outputs, deadlines, sequencing and linkages/interactions among the sub-processes and related documented procedures.

Consequently, 'risk analysis' (see Ch. 3), is effective when including identification of all key processes containing potential exposure to some consequence. It should involve process analysis, directing special attention to key cross-organizational dependencies and significant

[21] ISO 9000:2000 defines the 'process' as a set of interrelated or interacting activities which transforms inputs (financial, people, technology, facilities, information) into outputs. Inputs to a process are generally outputs from other processes. Processes in an organization are planned and carried out under controlled conditions in order to add value. ISO 8042:1994 defines the 'process' as a set of inter-related resources and activities which transforms inputs into outputs. Resources may include personnel, facilities, equipment, technology and methodology.

control nodes, for example: where data originate, where they are stored, how they are converted to useful information and who uses such information.

The process mapping activity entails a number of **steps**:

- Identifying all routine activities within the scope of the specific process analysed;
- Grouping the activities into key sub-processes;
- Determining the sequence of events, and links between the sub-processes.

To ensure process maps accurately reflect what actually happens, organizations may combine different **methods** (see appendix), so an organization should choose the **kind of 'Process Modelling and Mapping'** suitable for its specific goals. The map can be a simple macro-flowchart, showing only enough information to understand the general process flow, or it might be detailed enough to show every single action and decision point.

What follows is a description of different mappings.

- Macro-level process map. This is a very deep level as well as rather rare mapping that outlines the operational routes of an organization.
- Top-down or high-level process map. It shows end-to-end processes across the above operational areas. It is quick and easy to draw, but may not provide the necessary details to build understanding or realize improvements. It is good to show the major clusters of activity in a process.
- Cross-functional process map. It shows roles, inputs, outputs and steps required to complete a specific process within an operational area. Cross-functional process mapping provides enough information for improvement efforts, and uses flowcharts to show the relationship between a business process and the functional units (such as departments) responsible for such a process. These charts emphasize where people or groups fit into the process sequence, and how they relate to one another throughout the process. Cross-functional charts are excellent tools to show how a process flows across organizational boundaries.
- Detailed Process Flowchart. It details systems, instructions and procedures required to complete steps in processes at level three (Cross-functional process map), and shows inputs, outputs, related steps and decision points. Because of the level of detail, such a mapping can be resource-intensive to create, but can offer the greatest improvement potential since it shows decisions and subsequent actions, so providing excellent training and reference materials. Flowcharts may be maps or graphical representations.

The process owner should be in charge of process mapping, while process analysis should be made by other roles (either within or without the organization), in order not to be

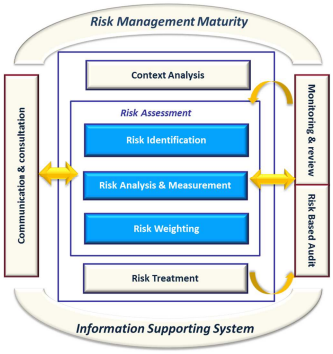
influenced by one's own working method.

Lastly, references to the maps, procedural information, and the maps themselves need to be stored in a consistent structure called a **process library**. Responsibility for the process library needs to be clear, just like any process itself needs an owner.

QUESTION MARK BOX

Q1. In your organization, are identified risks a result of a previous process mapping?
R. "A proxy, i.e. a list of the activities that appear in the planning and control information system, has been utilized".
Source: Italy, *Survey on risk management practices*
Q2. Process mapping in your Organization has involved:
R1. "For all business areas (pure statistical or support), integrating the IT specific (sub)processes, a list of generic activities was defined (starting with early 2000s), linking objectives, processes, organizational units, accountabilities, deadlines and outputs. In principle, for each process with underlying activities, an operational (for vertical processes) and a system (for transversal processes) procedure should be described and documented, according to a standard template".
Source: Romania, *In-depth survey on risk management practices*
R2. "The business process model of Statistics Austria was implemented in 2000 and covers 32 statistical core processes and approx. 35 cross-cutting processes. For all these processes detailed descriptions of operational activities are provided and regularly used".
Source: Austria, *In-depth survey on risk management practices*
Q3. The risk management training program involves:
R. "A set of statistical quality training modules has just been developed that supports process mapping and the application of the various statistical controls into business areas"
Source: Australia, *In-depth survey on risk management practices*

3. Risk assessment



TAGS: risk identification; risk analysis; risk weighting; Techniques; Roles and accountabilities

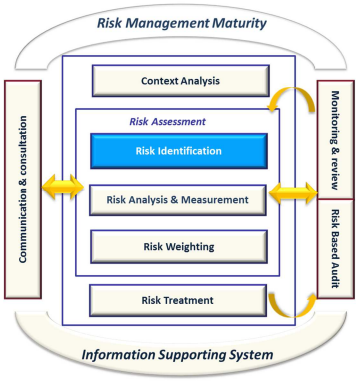
Organizational context analysis affects the methodology used to assess risks, since it affects the choice of assessment criteria. The first activity within the risk assessment process is to develop a common set of assessment criteria, to be deployed across business units, corporate functions, and large capital projects. Risks and opportunities are typically assessed according to both their impact and likelihood.

Some risks are dynamic, and require ongoing assessment, other ones are more static but their periodical reassessment counts toward an ongoing monitoring process that triggers an alert should circumstances change.

Risk assessment includes three steps:

1. Identification;
2. Analysis and measurement;
3. Weighting (risk prioritization)

3.1 Risk identification



TAGS: Risk Definition; Risk Criteria; Risk Identification; Different approaches; Risk Hierarchy; Techniques; Stakeholder's involvement; Roles and accountabilities.

Risk generally is the uncertainty inherently related to consequences – either positive i.e. opportunity, or negative i.e. threat – of actions and events. It is measured through a combination of likelihood and impact, including perceived relevance. "Inherent risk" is the exposure arising from a specific risk before any action has been taken to manage it, while "residual risk" is the exposure arising from a specific risk after any action has been taken to manage it, and in case such an action has proved effective.

An organization defines the criteria to be used to evaluate risk significance. Such criteria should reflect both the stakeholders' risk perception (based on a set of values/concerns), and the organization's values, objectives and resources. Some criteria can be imposed by, or derived from, legal and regulatory requirements. Risk criteria should be consistent with the organization's risk management policy, defined in the risk management framework.

Defining risk criteria involves deciding on:

1. The nature and kind of consequences to be included, and how they will be measured;
2. The way probabilities are to be expressed;
3. How a level of risk is going to be determined;
4. The criteria for determining when a risk needs treatment;
5. The criteria for deciding when a risk is acceptable and/or tolerable;
6. Whether and how combinations of risks will be taken into account.

Risk identification requires analysing several issues:

- *Source/root cause event*: any activity having a potential to increase a specific risk, whether or not such an activity is under the control of the organization;
- *Areas of impact*: dealing with categorization/prioritization of consequences;

- *Enablers*: the organizational features helping a risk-event to occur;
- *Events*: occurrence of a particular set of circumstances; and
- *Their potential consequences*: potential outcome of an event. A wide range of risk consequences should be considered, including cascade and cumulative effects.

The above issues can create, enhance, prevent, degrade, accelerate or delay the ability of either the whole organization, or part of it, to achieve its own objectives.

I. Risk hierarchy and risk categorization

The risk management framework includes a hierarchy of risks, comprising a variety of risk levels together with priorities in risk treatment strategies.

- **Enterprise or so-called "corporate" risks** are strategic (i.e. can significantly impact on the organization). To manage them is fundamental to the long term viability of the organization and this must be done under the supervision of the risk committee;
- **Portfolio management risks** are inherently related to the portfolio of projects as a whole, and are managed by senior management. Some examples of portfolio risk are: affordability of the portfolio; lack of capability/capacity to implement the portfolio; lack of timely availability of skills and human resources;
- **Project risks** can impact on the projects' objectives and outcomes, and are managed by the project risk manager; where appropriate, they will be addressed as part of the project management framework. Some examples of project risk are: project scope poorly defined, resources not available when required, quality requirements not clearly specified.
- **Operational risks** can impact on a program's objectives and/or outcomes (i.e. unsuitable skills mix, resources reduced due to budget cuts, outputs not delivered on time, poor quality outputs) and are managed by the program directors.

While each risk captured may be important for management at the function and business unit levels, the corporate risk list requires prioritization to focus the attention of the board and senior management on key risks.

The management of risk at corporate, enterprise and operational levels needs to be integrated, so that the levels of activity support each other. In this way the organization's risk management strategy will be led from the top, and be embedded in the normal working routines and activities.

Risk specialists on specific risks, directly referring to the related senior managers, are

needed. Specific risk areas include, for example:

- Health and safety risks;
- Fraud risks (i.e., manipulation of any procedures for dishonest purposes; failure to comply with procedures and/or internal regulations; alteration of checks on execution of works or on delivery of supplies; etc.);
- ICT risks (i.e., security systems risks; business continuity; etc.)

An organization should therefore set and document its risk categories and risk consequence categories according to its size, purpose, nature, complexity and context. The risk categories, including those from stakeholders, should be communicated throughout the organization in order to share a common understanding.

Grouping similar kinds of risks into risk categories helps to:

1. Allow consistent assessment;
2. Profile and report the consequences of actual and potential events;
3. Facilitate comparison across the organization;
4. Aggregate and map similar kinds of risk across the organization;
5. Allocate risk management responsibilities;
6. Build internal skills, knowledge and expertise throughout the organization.

The table below shows risk categories and classes for a NSO, according to the allocation suggested by Co.S.O. enterprise risk management standard.

Strategic	Statistical production, Statistical data dissemination, Management systems and processes, Organization
Operational	HR, Finance, ICT, Procurement
Compliance	Compliance to law, standards
Reporting	Communication flows

II. Risk identification techniques

Risk identification may require a multidisciplinary approach, since risks may cover a wide range of causes and consequences.

Risk identification methods can include:

a) Evidence based methods, for example checklists and historical data reviews;
b) Systematic team approaches (a team of experts systematically identifies risks by means of a structured set of prompts or questions (i.e. structured or semi-structured interviews, Brainstorming[22], Delphi method[23]));
c) Inductive reasoning techniques (i.e. preliminary hazard analysis, HAZOP, HACCP);
d) Scenario analysis (i.e. root-cause analysis, scenario analysis as such, cause-consequence analysis);
e) Statistical methods (i.e. Monte-Carlo analysis, Bayesian analysis).

In implementing these techniques the maturity of a risk management system should always be taken into account. During the experimental phase of the risk management model, the experience analysis should always be combined with either structured or semi-structured interview, or a prompt/check list, in order to guide risk owners through the risk analysis.

The experience analysis needs to be based on actual information, through the examination of data from various systems (e.g. electronic document management systems, non-conformities and IT incidents registration system, time use recording system, as well as a specific system to record quality features of statistical surveys). Once the risk management culture is more established throughout the organization, brainstorming and the Delphi technique can replace the interview, the cause/consequence analysis, the check-list or any other simpler kind of scenario analysis.

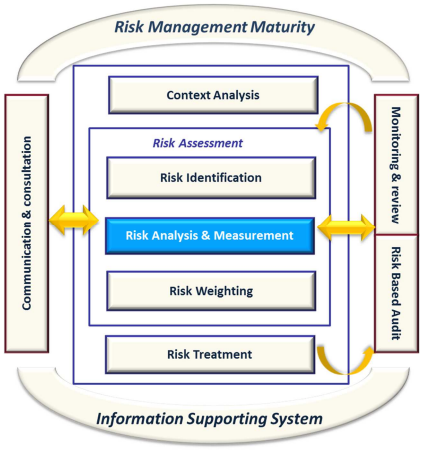
Factors influencing selection of techniques are:

1. Problem complexity and the methods needed to analyse them;
2. The nature and degree of risk assessment uncertainty, that is based on the amount of information available and requirements to satisfy objectives;
3. The extent of resources needed in terms of time and level of expertise, data needs or cost;
4. Whether the method can provide a quantitative output.

[22] Brainstorming is a means of collecting a broad set of ideas and evaluation, ranking them by a team. It may be stimulated by prompts or by one-on-one and one-on-many interview techniques

[23] A means for combining expert opinions to support the source and influence identification, probability and consequence estimation and risk evaluation. It is a cooperative technique for building consensus among experts (ISO ISO31010 – risk Assessment Techniques)

3.2 Risk analysis and measurement



Risk analysis involves consideration of risk causes and sources, their positive and negative consequences and the likelihood of such consequences occurring.

It normally includes estimation of the range of potential consequences that might arise from an event, situation or circumstance, and their associated probabilities, in order to measure the level of risk. However, in some instances (such as where the consequences are likely to be insignificant, or probability is expected to be extremely low), a single parameter estimate can be enough to make a decision.

In any case, some framework for assessing risks should be developed. The assessment should draw as much as possible on unbiased independent evidence, should consider the perspectives of the whole range of those stakeholders affected by the risk, and avoid confusing a fair risk assessment with any judgment about the acceptability of particular risks.

There are three important principles in assessing risk:

1. Ensuring that there is a clearly structured process, through which both likelihood and impact are considered;
2. Recording risk assessment in such a way to facilitates monitoring and identification of risk priorities;
3. Distinguishing between “inherent” and “residual” risk[24]. The level of risk will depend on the adequacy and effectiveness of existing controls.

Methods used in analysing risks can be:

- Qualitative: such methods define consequence, probability and level of risk, according to descriptive scales, may combine consequence and probability, and evaluate the resulting level of risk against qualitative criteria.
- Semi-quantitative: such methods use numerical rating scales for consequence and probability, and combine them to produce a level of risk using a formula. Scales may

---

Inherent risk: the risk to an entity in the absence of any actions management might take to alter the risk's likelihood or impact.

Residual risk: the portion of total risk remaining after risk treatment has been applied. Residual risk comprises acceptable risk and unidentified risk.

be linear or logarithmic, or have some other relationship; the formulae used can also vary.

- Quantitative: this kind of analysis estimates practical values for consequences and their probabilities, and produces numerical values for impact, likelihood and level of risk, using data from a variety of sources. Full quantitative analysis may not always be possible or desirable due to poor information about the object being analysed, lack of data, influence of human factors, etc.

Both qualitative and quantitative techniques have advantages and disadvantages.

Qualitative analysis is relatively quick and easy, provides a lot of information about non-financial impacts and is easily understood by a large number of employees.

On the other hand, it doesn't make much difference among levels of risk, cannot numerically aggregate or address risk interactions or correlations, and provides limited opportunity to perform cost-benefit analysis.

Quantitative analysis allows many qualitative methods weaknesses to be overcome, although it can be time-consuming and costly especially at first, during model development.

Cause-effect analysis is a semi-qualitative, structured method allowing a potential event to be traced back to its original causes. It organizes possible contributory factors into broad categories, so that all relevant hypotheses can be considered. It does not, however, by itself point to the actual causes, since these can only be determined by real evidence and empirical testing of hypotheses. Cause-and-effect analysis provides a structured pictorial display (diagram) of a list of causes for a specific effect (positive or negative depending on the context). It is used to build consensus on all possible scenarios, and the most likely causes identified by a team of experts; such causes can then be tested empirically or by evaluation of available data.

A cause-and-effect diagram can be made when there is need to:

- Identify the possible root-causes for a specific effect, problem or condition;
- Sort out and correlate some of the interactions among factors affecting a particular process;
- Analyse existing problems so that improvement action can be taken.

The input to a cause-and-effect analysis may come from expertise and experience from participants, or a previously developed model that has been used in the past.

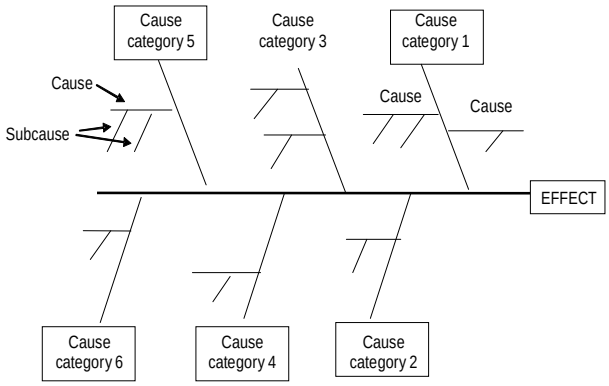
The cause-and-effect analysis should be carried out by a team of experts who are aware of the problem requiring resolution.

The basic steps in performing a cause-and-effect analysis are as follows:

1. Establishing the effect to be analysed, and placing it in a box;
2. Determining the main categories of causes (chosen to fit the particular context), and representing them by boxes in the Fishbone diagram;
3. Filling in the possible causes for each major category with branches and sub-branches to describe the relationship among them;
4. To keep asking "why?" or "what caused that?" to connect the causes;
5. Reviewing all branches to verify consistency and completeness, and to ensure that the causes apply to the main effect;
6. Identifying the most likely causes, based on the opinion of the team and available evidence.

The results are normally displayed as either a Fishbone (or Ishikawa) diagram or tree diagram. The Fishbone diagram is structured by separating causes into major categories (represented by the lines off the fish backbone), with branches and sub-branches that describe more specific causes under the above-mentioned categories.

Figure 3: Example of Ishikawa or Fishbone diagram



Source: IEC/FDIS 31010:2009, Risk management – Risk assessment techniques

As mentioned above, the level of risk is a function of factors, in particular likelihood and impact.

<u>Impact</u> refers to the extent that a risk event may affect an organization. Impact assessment criteria may include financial, reputational, regulatory, health, safety, security, environmental, employee, customer and operational consequences. Organizations typically define impact using a combination of such consequences, given that certain risks may impact the enterprise financially, while other risks may have a greater impact to reputation or health and safety.

<u>Likelihood</u> represents the weak/strong possibility that a given event will actually occur.

Likelihood can be expressed through either qualitative, percent or frequency terms. Sometimes organizations describe likelihood in more personal and qualitative terms such as "event expected to occur several times (or not expected to occur) over the course of a career".

The Appendix shows examples of risk indexes for impact and likelihood.

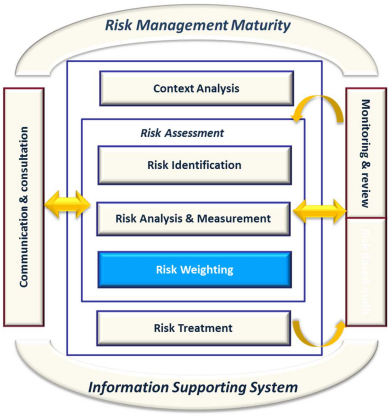
When using either qualitative or semi-qualitative methods – for example risk indexes – aimed at evaluating risk level whatever the event (statistical, organizational or specific ones), applying the same number of parameters for impact as well as likelihood is crucial. In order to balance subjectivity in evaluation, more than one evaluator for single risk is needed and evaluation should be supported through objective data as much as possible.

As for the roles and accountabilities, risk factors assessment is under the responsibility of the process owners. Risk measurement is a task for working groups supported by the risk management office, and participated in by the staff working on the processes in question, who submit their results for authorization/review at senior levels. Experts (e.g., IT, data protection/statistical confidentiality, etc.) are responsible for the measurement of specific risks. The results of assessment are always also reviewed and validated by the risk manager.

QUESTION MARK BOX

Q. With reference to the risk measurement phase, does your Organization use different techniques concerning risk classification (IT, financial, compliance, etc.)?
R. The risk assessment (in statistical areas) includes consideration of the range of issues in a statistical processing cycle that can affect data quality as well as managing stakeholder relationships.
Source: Australia Bureau of Statistics, In-depth survey on risk management practices

3.3 Risk weighting



Risk weighting involves comparing estimated levels of risk to assessment criteria, in order to identify the most significant risks, or to exclude minor risks from further analysis. The purpose is to ensure that use of resources will be focused on the most important risks. Care should be taken not to screen out low risks which occur frequently and can therefore have a significant increasing effect.

The preliminary analysis determines one or more of the following courses of action:

- Setting aside insignificant risks (so called acceptable risks) which would not justify treatment;
- Deciding to treat unacceptable risks;
- Setting priorities for risk response.

Risk weighting provides inputs to decisions on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods. Subsequently, the purpose of risk weighting is to assist in making decisions (based on the outcomes of risk analysis) about which risks need treatment and which priority must be assigned for their treatment. Risks are related to objectives, so can easily be prioritized for risk response in relation to such objectives. Unacceptable risks are ranked and prioritized in relation to other risks. Therefore, the decision about whether and how to treat the risk may depend on costs and benefits from taking the risk, and costs and benefits from implementing improved controls.

A common approach to prioritizing risks is to divide them into three bands:

- An upper band, where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its costs;
- A middle band, where costs and benefits are taken into account and opportunities balanced against potential consequences;
- A lower band, where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.

Some organizations represent this portfolio as a hierarchy, some as a collection of risks plotted on a heat map (also risk map or risk matrix).

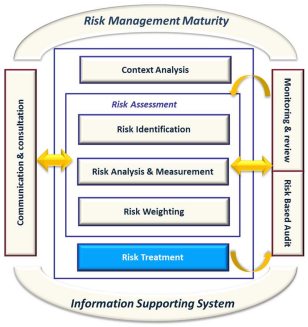
First, the risks are ranked according to one, two, or more criteria, such as impact rating multiplied by likelihood rating.

Second, the ranked risk order is reviewed in light of additional considerations, such as impact alone, or the size of the gap between current and desired risk level (risk tolerance threshold).

If the initial ranking is done by multiplying financial loss by likelihood, then the final prioritization should also take into consideration other qualitative factors (for example loss of reputation).

The most common way to prioritize risks is by assigning a risk level for each area of the graph such as very high, high, medium, or low, where the higher the combined impact and likelihood ratings, the higher the overall risk level. The boundaries among levels vary from entity to entity, depending on risk appetite. For example, an organization with a greater risk appetite will have boundaries among risk levels shifted toward the upper right, and an organization with greater risk aversion will have boundaries among risk levels shifted toward the bottom left. Also, some organizations adopt asymmetric boundaries placing a somewhat greater emphasis on impact than on likelihood. For example, a risk having a "moderate" impact rating and a "frequent" likelihood rating has a "high" risk level assigned, whereas a risk having an "extreme" impact rating and a "possible" likelihood rating has a "very high" risk level assigned.

4. Risk treatment



TAGS: Priority for treatment; Response actions; Risk mitigation; Risk reduction.

The purpose of addressing (treating) risks is to turn uncertainty to the organization's benefit, by constraining threats and taking advantage of opportunities.

After assigning priority to risks, risk treatment should be identified both for corporate and operational risks, as well as linked to business planning processes. The challenge is to determine a portfolio of suitable responses that form a consistent and integrated strategy, so that the remaining risk falls within the acceptable level of exposure. It is worth noting that there is no right response to risk. The response chosen depends on issues such as the

organization's 'risk appetite'[25] (see Section 1, Ch. 1), the impact and likelihood of risk, and costs and benefits of the mitigation plans.

Risk treatment should comply with legal requirements, as well as government and organizational policies. Therefore, decisions concerning whether risk treatment is required may be based on operational, technical, financial, legal, social, environmental or other **criteria**. Such criteria should reflect the organization's context, and depend on its internal policies, goals and objectives, as well as its stakeholders' needs. In this respect, a team approach is useful to help define the context properly and for well-targeted change management during risk treatment.

4.1 Risk treatment actions

There are different **response action categories** which correspond to **key general approaches for risk treatment**. These response action categories are:

1. **TOLERATE**. The exposure may be tolerable without any further action being taken or even if not tolerable, the ability to do anything may be limited (or the cost of taking any action may be disproportionate to the potential benefit). In these cases the response may be to tolerate the existing level of risk. This option, of course, may be supplemented by contingency planning for handling the impact that will arise if the risk results in actual events.

   The actions related to this kind of approach are:

   - Risk acceptance: no action is taken to affect likelihood or impact.
   - Retaining: after risks have been changed or shared, there will be residual risks that are retained. The risk can be retained by informed decision: acceptance of the burden of loss, or benefit of gain, from a particular risk, including the acceptance of risks that have not been identified. Risks can also be retained by default, e.g. when there is a failure to identify or appropriately share or otherwise treat risks. Moreover, after opportunities have been changed or shared, there may be residual opportunities that are retained without any specific immediate action being required (retaining the residual opportunity).

[25] Before responses are developed for each risk identified, it is necessary to determine the organization's attitude to risk or 'risk appetite', influenced by the size and type of organization, its culture and its capacity to withstand the impacts of adverse occurrences.

2. **TREAT.** Usually, the majority of risks are addressed this way. The purpose of treatment is that whilst continuing with the activity that gives rise to the risk, specific action is taken in order to constrain such a risk to an acceptable level.

   Actions related to this kind of approach are as follows:

   - Removing: removing the risk source.
   - Risk reduction, actions are taken for:
     - Changing likelihood (mitigating actions): action taken to reduce the likelihood of negative outcomes and/or to increase opportunity, in order to enhance good outcomes.
     - Changing the consequences (contingency actions): actions taken to reduce the extent of losses and/or to increase the extent of gains with reference to related opportunities. These include setting up pre-event measures and post-event responses such as continuity plans.

   From the risk management perspective, the first kind of action (changing likelihood) should be preferred as it prevents the risk rather than waiting for the consequences.

3. **TRANSFER**. For some risks the best response may be to transfer them[26]. The transfer of risks may be considered to either reduce the exposure of the organization or because of another organization (which may be another public organization) judged more capable of effectively managing such risks. It is worth noting that some risks are not (fully) transferable: in particular, reputational risk can hardly be transferred. Relationship with the third party to which the risk is transferred needs to be carefully managed to ensure a successful transfer.

   Actions related to this kind of approach are as follows:

   - Transferring[27] the risk or a portion of it[28].
   - Sharing[29]: another party or parties bearing or sharing some part of the risk outcomes, usually by providing additional capabilities or resources that increase the likelihood of opportunities, or the extent of gains from them. Sharing positive

[26] This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets.

[27] ISO 73:2009 Standard considers the 'risk transferring' as a form of risk sharing.

[28] For example through insurance or outsourcing.

[29] The ISO 73:2009 highlights how risk sharing involves the agreed distribution of risk with other parties, noting that legal or regulatory requirements can limit, prohibit or mandate risk sharing itself. Moreover, the extent to which risk is distributed can depend on the reliability and clarity of the sharing arrangements.

outcomes can involve sharing some of the costs involved in acquiring them. Sharing arrangements can often introduce new risks, in that the other party or parties may not effectively deliver the required capabilities or resources.

4. **TERMINATE**. Some risks will only be treatable, or reducible to acceptable levels, by terminating the activity. It is worth noting that such an option can be severely limited in the public sector when compared to the private one. It can be particularly important in project management.
   - Avoiding: action is taken to stop the activities giving rise to risk or avoiding the risk by not starting such activities (where this option can be practiced). Risk avoidance cannot occur properly if individuals or organizations are unnecessarily risk-averse. Inappropriate risk avoidance may either increase the significance of other risks or lead to the loss of opportunities.
5. **TAKE THE OPPORTUNITY.** This option is not an alternative to those above; rather it is an option that should be considered whenever tolerating, transferring or treating a risk. This can occur in two ways: the first is when an opportunity arises to exploit positive impact whether or not action is taken to mitigate threats at the same time. The second is when circumstances arise which, whilst not generating threats, offer positive opportunities.
   - Taking/increasing: taking or increasing risk in order to pursue an opportunity.

Risk treatment options are not necessarily mutually exclusive, or appropriate in all circumstances. Often a risk response may combine two or more of these strategies to achieve the desired results. An organization can normally benefit from adopting a combination of treatment options. Implementation of the risk responses selected involves developing a risk plan, outlining the management processes that will be used to manage risk or opportunity to a level set up by the organization's 'risk appetite' and culture.

Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, treatments provide or modify controls: any action taken to address a risk forms part of what is known as "internal control".

4.2 Risk treatment process

Risk treatment involves a **cyclical process** of:

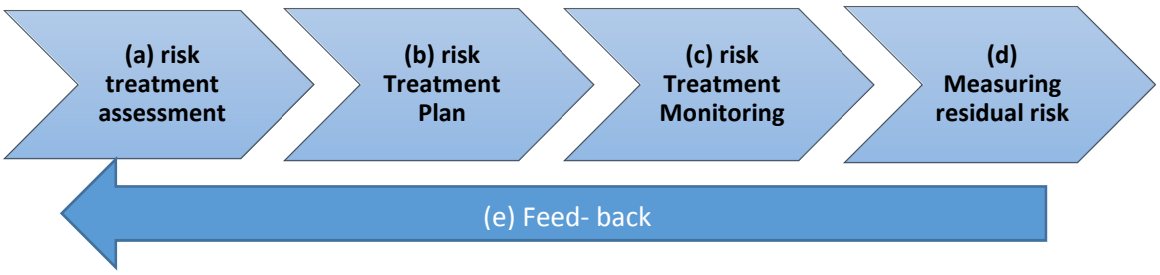
a) Assessing a risk treatment: identify and evaluate risk treatment options;

b) Planning risk treatment: prepare a risk treatment schedule and action plan;

c) Monitoring effectiveness for that treatment (see Ch. 5);

d) Measuring residual risk: deciding whether residual risk levels are tolerable;

e) Feed-back actions: if residual risk is not tolerable, generating a new risk treatment (back to step no. a) and repeating the process.



a) Risk treatment assessment: an organization should select the best option at its disposal. That involves balancing the costs of implementing each option against the benefits derived from it, with regard to legal, regulatory, and other requirements such as social responsibility. In general, the cost of managing risks needs to be balanced with the benefits obtained. When making such cost versus benefit judgments, the context should be taken into account. It is important to consider all direct and indirect costs and benefits, whether tangible or intangible, and measure them in financial or other terms.

b) Risk Treatment Plan: Treatment should involve, at the operational level, preparing and implementing a related plan. It shows how the treatment options selected will be implemented and should be integrated with the management and budgetary processes. Specifically, the information provided in a treatment plan should include:

a. The reasons for selecting the treatment options, including expected benefits;
b. Who is accountable for approving the plan and who is responsible for implementing it;
c. The actions proposed;
d. Resource requirements, including contingencies;
e. Performance measures and constraints;
f. Reporting and monitoring requirements;
g. Timing and schedule.

Lastly, responsibilities related to the treatment phase should be clearly assigned, specifying who is accountable for the management of particular risks (or categories of risk), for implementing treatment strategies, and for the maintenance of risk

controls. For this, the board should ensure that management considers and implements appropriate risk responses: responsibility for treatment is usually assigned to the management level (directors-general, heads of divisions; project managers) and assigned to staff, where appropriate. Management should also identify and note in the 'risk register' those actions selected as treatment, and should show to the board how such risk responses improve the performance of the organization. Risk owners, according to their respective roles in the project or process, are indicated to set risk treatment plans, even though at this stage responsibilities vary according to the kind of risks (either corporate or operational). For example, senior managers are responsible for corporate risks, their mitigation strategies and action plans. The operational risk responsibility relies on the divisional levels which the program is assigned to.

c) **Risk treatment monitoring**: in designing response actions, it is important that the **controls** put in place are proportional to the risks. Risk analysis assists such a process by identifying those risks requiring attention by the management. Risk control actions will be prioritized in terms of their potential to benefit the organization. Effectiveness of internal control is determined by how much the risk will be either eliminated or reduced by the control measures proposed. The latter need to be measured in terms of potential economic effect if no action is taken, versus the cost of the action(s) proposed, and invariably require more detailed information and assumptions than are promptly available. Every response action has a related cost, and it is important that the treatment offers value for money in relation to the risk controlled by it. In this regard, options in addressing risk ("TREAT") can be further analysed into four different types of **related/associated controls**:

- PREVENTATIVE CONTROLS. These are designed to limit undesirable outcomes. The more an undesirable outcome should be avoided, the more appropriate preventative controls should be implemented[30]. Most of controls implemented in organizations tend to belong to this category.
- CORRECTIVE CONTROLS. These are designed to correct undesirable outcomes that have occurred, and provide a way to achieve some recovery against loss or damage[31]. Contingency planning is an important element of corrective control.

[30] Examples of preventative controls include restriction of action to authorized persons only, for example, permitting only those suitably trained and authorized to handle media enquiries prevents releasing of inappropriate comments to the press.

[31] For example, drawing up contract clauses to allow recovery of overpayment. Insurance can also be regarded as a form of corrective control as it facilitates financial recovery against the actualization of a risk.

- DIRECTIVE CONTROLS. These are designed to ensure that a particular outcome is achieved, and are particularly important when avoiding an undesirable event – typically related to Health and Safety or to security – is crucial[32].
- DETECTIVE CONTROLS. These are designed to identify occasions of occurrence of undesirable outcomes. Their effect is, by definition, "after the event" so they are only appropriate when the resulting loss or damage can be accepted[33].

d) Residual risk measurement: If a residual risk persists even after treatment, a decision should be taken about whether to retain this risk or to repeat the risk treatment process. For residual risks that are deemed to be high, information should be collected about the cost of implementing further mitigation strategies.

EXAMPLE OF RISK TREATMENT PLANNING

RISK TREATMENT - SCHEDULE	
PROPOSING DEPARTMENT	_____
VALIDATING DEPARTMENT	_____
RESPONSIBILITY	_____
KIND OF TREATMENT	_____
RISK DESCRIPTION	.....
PROCESS	.....
PHASE	.....
CAUSE	.....
ENABLING FACTORS	.....
TIMETABLE	.....

[32] For example, requiring that staff are trained to get certain skills before being allowed to work unsupervised.

[33] Examples of detective controls include "Post Implementation Reviews" which detect lessons to be learnt from projects, for application in future work, and monitoring activities which detect changes to be responded to.

RISK TREATMENT - MONITORING		
OBJECTIVES	…….	
OUTPUT INDICATORS	…….	
CONTROL PROCEDURE	…….	
RISK TREATMENT – ACTION PLAN		
PHASE	UNIT	TIME
1. …….	…….	…….
2. …….	…….	…….
3. …….	…….	…….

QUESTION MARK BOX

Q1. Following risk identification and assessment in your organization, is any treatment of the risks put in place?

R1. "Yes. risk treatment of most significant risks is assigned to managers, and followed up (annually or bi-annually by the board of directors). The less significant risks are treated as a part of normal operations. The risk treatment of moderate or higher risks is taken to the department's management team for approval. The treatment is assigned to a person responsible for implementing the treatment as a part of normal operations or if that is not possible a separate implementation plan is to be prepared".

Source: Finland, *Survey on risk management practices*

R2. "Yes. Risk is weighted and asset owners have to set up a plan to reduce risks that are measured above a certain level"

Source: Iceland, *Survey on risk management practices*

R3. "Yes. Treatments are identified as part of the risk identification process - a template is completed by Heads of Division twice a year, and individual directorate risk registers and a corporate risk register are created. Ownership of the risk is assigned and the process is reviewed twice a year by the senior management committee with the individual Head of Division. The project management system also facilitates risk identification and management, and the project team review the project regularly. Risk management treatments can involve human resource solutions".

Source: Ireland, *Survey on risk management practices*

R4. "Yes. Treatment of the risks is the main result of risk analysis. The results are known as control activities. In some cases control activities have been established as a result of previous experiences, well before any formal risk analysis. However only a full analysis can give a reasonable security that everything that counts has been considered and that the institution are prepared to face the consequences.

Source: México, *Survey on risk management practices*

R5. "Yes, in accordance with the system procedure on the risk management approved by the NIS President (Decision no. 1038/2011). The audit reports on risk management are taken into consideration to propose treatment actions".

Source: Romania, *Survey on risk management practices*

Q2. Please indicate which kinds of risks are being managed through the risk management process, while specifying connections and differences in treatment:

R1. "Approach in treatment depends on greater or lower influences of CBS in reducing risk to an acceptable level. Regarding the risk treatments, most of identified and assessed risks have been classified into two categories: risk reduction and risk avoidance or in combination".

Source: Croatia, *In-depth survey on risk management practices*

Q3. Please describe the methodology used in identifying and monitoring the risk treatment, while specifying the oOrganization roles involved:

R1. "The methodology used by INEGI is based mainly on the international standard ISO 31000 about risk management, ISO/IEC 27000 about information security, some elements of COSO ERM (enterprise risk management), and also from the standard of the European Federation of risks (FERMA). The first version of the methodology was released in 2010, and the present version has been the result of the institutional experience of its use".

Source: México, *In-depth survey on risk management practices*

Q4. With reference to RM, Internal Controls and Internal Audit System within your Organization, please describe the connection/integration between these ones in detail, while specifying: how risk treatment actions are monitored functions, roles and accountabilities involved in the monitoring of the risk treatment actions…"

R1. "As for the risks, each head of an administrative unit is responsible to identify, analyse, evaluate and determine the actions of treatment.

Source: México*, In-depth survey on risk management practices*

Q5. Please describe who sets priorities for risk treatment actions and how:

R1. "On a corporate level, the board of directors sets the priorities. On a process level, the process owner sets the priorities".

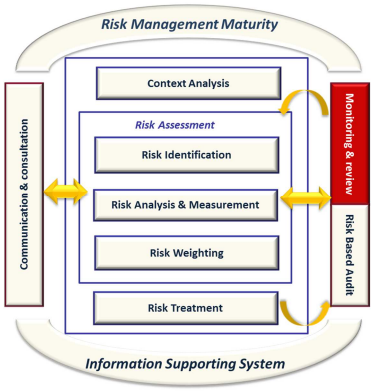
Source: Netherlands, *In-depth survey on risk management practices*

Q6. Following risk identification and assessment in your organization, is any treatment of the risks put in place?

R1. "Yes. Directors/division chiefs (risk owners) propose response actions validated by the risk manager/fraud and corruption prevention manager. These actions are selected on a priority basis (risk strategic area, risk value, feasibility), and then entrusted to the executives. Managers propose the response actions; the governance select the actions after defining their significance (prioritization); the framework is populated by the internal representative network. The validated and selected response actions are designed, carried out and monitored under the responsibility of the managers (directors/division chiefs); the framework is filled in by the representative network with the monitoring information".

Source: Italy, *Survey on risk management practices*

5. Monitoring and control



TAGS: Monitoring; Review; Roles and accountabilities; Key-risk indicators; Risk-based Audit; Internal audit cycle.

5.1 Monitoring and review

Risk management is dynamic, iterative and responsive to change. As risks and priorities change, risk treatments should be monitored as a part of the risk management process.

The organization's monitoring processes should encompass all the features of risk management in order to:

- Ensure that controls are effective and efficient;
- Detect any changes in existing risks which require revision to risk treatments and priorities;
- Identify emerging risks.

Monitoring and review are two different and complementary activities, since monitoring involves the routine surveillance of actual performance against expected (or required) performance, while review involves periodic (yearly at least) checking of the current situation for changes in the internal/external context.

The overall responsibility for monitoring and review activities relies on the board and top management: the way the top management reacts to the results of monitoring program will affect the actions of employees.

Monitoring should be an integral part of management, and risks and controls should be allocated to owners, who are therefore responsible for monitoring them. A typical approach for monitoring includes:

- Environment scanning by risk owners, to monitor changes in risks or in context;

- Risk treatment plan monitoring by risk owners;
- Control monitoring by control owners and risk officers, through performance indicators and key risk indicators, according to the quantitative thresholds described in the risk appetite statement (see below).

Monitoring and review activities can also be considered in terms of a hierarchy. Responsibilities can vary according to the kind of risks monitored (corporate, operational, project): operational risks are monitored at business unit level, project risks are monitored within the project management system, and corporate risks are monitored by senior managers (i.e., directors-general or heads of department).

5.2 Key risk indicators

Key risk indicators (KRIs) are used for monitoring risk treatment actions.

Key risk indicators are metrics used to provide an early warning on increasing risk exposures in different areas within an organization. In some instances, they may represent key ratios that are tracked by management throughout the organization as indicators of evolving risks, and potential opportunities, that alert on the need for actions to be taken. Others may be more complex, and involve aggregation of several individual risk indicators into a multi-dimensional score about emerging events, that may lead to new risks or opportunities.

KRIs are typically derived from specific events or root causes, internally or externally identified, that can prevent performance goals from being achieved. Linkage of top risks to core strategies helps pinpoint the most relevant information that can serve as an effective leading indicator of an emerging risk.

An effective method for developing KRIs begins by analysing a risk-event that has affected the organization in the past (or at present), and then working backwards to pinpoint intermediate and root cause events that led to the ultimate loss or lost opportunity. The closer the KRI is to the root cause of a risk-event, the more likely that the KRI will provide management time to take positive action to respond to such an event.

Effective KRIs often result from being developed by teams including professional risk management staff, and business unit managers with a deep understanding of the operational processes subject to potential risks. Ideally, these KRIs are developed in cooperation with strategic plans for individual business units, and can then embed acceptable deviations from the plan which fall within the overall risk appetite of the organization.

The development of KRIs that can provide relevant and timely information, to both the board and senior management, is a significant component of effective risk oversight. It is also important to consider the frequency of reporting the KRIs. The appropriate time horizon depends on the main user of a specific KRI. For operational managers, real-time reporting may be necessary. For senior management, where a compilation of KRIs that highlight potential deviations from organization-level targets is the likely goal, a less frequent (e.g., weekly) status report may be enough. At the board level, the reporting is often aggregated to allow a broader analysis. Management can then use such analyses to identify information related to the root cause event, or intermediate event that might serve as a key risk indicator related to either event. When KRIs for root cause events and intermediate events are monitored, management is in the best position to identify early mitigation strategies to begin to reduce or eliminate the impact associated with an emerging risk event.

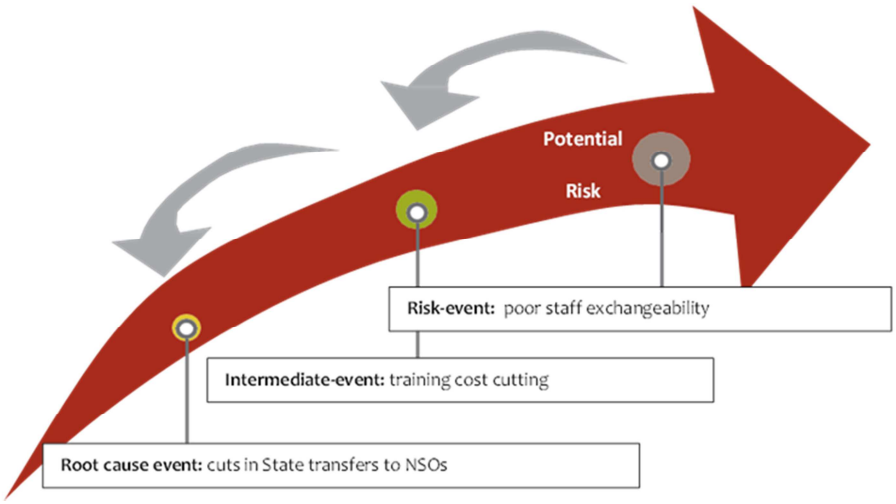
KRIs do not manage or treat risk, and can lead to a false sense of safety if poorly designed. An important feature of any KRI is the quality of the available data used to monitor a specific risk, and attention must be paid to the source of information, either internal to the organization or drawn from an external party. Sources of information to inform decisions about the choice of KRIs may be available; for example, internal data may be available concerning prior risk events which can be informative about potential future exposures. Nevertheless, internal data is often unavailable for many risks — especially if not previously encountered. In addition, risks likely to have a significant impact may often arise from external sources, such as changes in economic conditions, interest rate shifts, or new regulatory requirements/legislation. Therefore, KRIs may be based on external data, given that root cause and intermediate events may arise from outside the organization.

A well-designed KRI should:

1) Be based on established practices or benchmarks;
2) Be consistently developed across the organization;
3) Provide an unambiguous and intuitive view of the highlighted risk;
4) Allow for measurable comparisons across time and business units;
5) Provide opportunities to assess the performance of risk owners on a timely basis;
6) Consume resources efficiently.

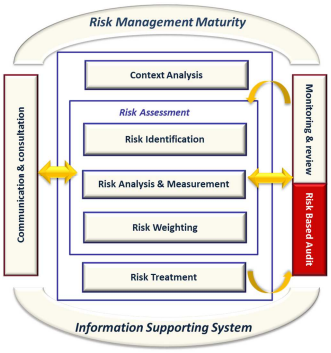
In the picture below, identification of a key-risk indicator related to the objective “Enhancing job rotation” is assisted by developing a cause-effect chain between an event that can negatively impact on a particular objective, and its root cause.

Figure 4: Example of Key Risk Indicator: "Enhancing job rotation"



Formula:

Key Performance Indicator (KPI)	Key Performance Indicator (KPI)
% of staff transfers per year.	*% of training expenses per year*



6. Risk based control and audit

TAGS: RBA; Internal audit cycle

The internal control framework, which includes the risk management framework and the internal audit framework, differentiates among three levels of control:

- Internal control (preventative or subsequent), deployed within the risk management framework, under the responsibility of management (risk owners), aiming to prevent or reduce the consequences related to risk occurrence;

- "Compliance" level, aiming to help and monitor an actual risk management implementation by risk-owners; such a level oversees risk assessment and control processes also ensuring their consistency with organizational goals (risk management unit);
- "Risk based audit", ensuring an effective deployment of audit resources to assess management of those risks related to the actions of an organization, by examining and evaluating the adequacy of the risk management system and internal controls, processes and management. Therefore, internal audit monitors and shows the progress of implementation of audit recommendations and improvements in the audited area.

The Risk Based Audit (RBA) objectives are as follows:

- **Assurance for the risk management strategy**: to ascertain the extent to which all line managers review the risks/controls within the scope of their own responsibility; to evaluate the adequacy of risk management policy and strategy for achieving their objectives;
- **Assurance for management of risks/controls**: to encompass all the key risks as well as enough of the other risks to support confidence in the overall opinion reached; to evaluate the adequacy of the risk management processes designed to constrain residual risk to the risk appetite;
- **Assurance for the adequacy of the review/assurance process**: quality assured to engender confidence in the review process; to identify limitations in the evidence provided, or limitations to the depth/scope of the reviews undertaken; to identify gaps in control and/or over control, and provide opportunities for continuous improvement; to support preparation of internal audit summary report to the risk committee/chief statistician.

The RBA management cycle is carried out through the following six steps:

a) **Object**: procedures, processes and internal service charters, risks selected according to priorities but: risks within risk appetite, risks not requiring audit in the short term, risks otherwise audited, tolerable risks.
b) **Audit Plan**: internal audits to be carried out in the short term are managed according to an annual plan that is endorsed by the board, and shared with the organizational divisions involved. Such a plan shows, with reference to any action: i) the audit lifespan, ii) the team composition, iii) the accountabilities, iv) the audit tasks (according to procedures, contractual requirements, etc.), v) the documents required, vi) the lead times. The annual plan is prepared for a single year on the basis

of the strategic plan, according to risk assessment. Therefore, audit planning takes into account the results of previous audit studies, as well as management assessment of current levels of risk related to specific organizational programs.

c) **Audit run-up**, consisting of some actions that are preliminary to actual audit, such as: a) formal assignment of duties; b) definition of the activity plan; c) identification of documents needed to define the audit range of reference and intervention; d) communication on audit start; e) kick-off meeting with the staff involved.

d) **Audit implementation**, actual audit, consisting of: i) operational meetings; ii) preliminary assessment of criticalities; iii) check of suitability and accordance with the risk management or quality system; iv) drawing up recommendations and possible mitigation actions. Audits can be used to assist risk managers in assessing the effectiveness of controls for each risk. An assessment could be made on whether the controls are adequate to reduce the level of risk (i.e., to reduce the risk from extreme/high to medium or low), or whether additional treatments/controls are required.

e) **Reporting.** Auditing ends with a meeting for sharing the main results obtained. An audit report is drafted that contains: i) its findings, ii) the actions performed, iii) the criticalities found, and suggestions proposed, iv) possible action plan, in cooperation with the unit/division involved. Following the assessment of the control effectiveness for each risk, proposals for additional treatment strategies to reduce the level of risk will emerge, and some of the treatment strategies proposed during this process will be suitable for inclusion in the internal audit plan (feed-back).

f) The **follow-up** is aimed at checking the actual implementation of response actions related to any remarks or recommendations.

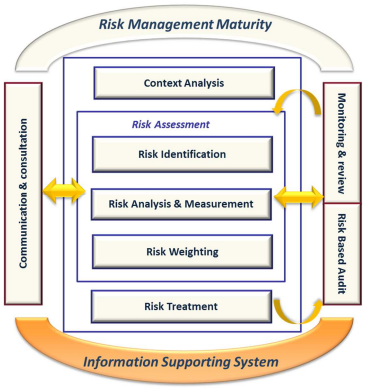
QUESTION MARK BOX

Q. With reference to risk management, internal controls and internal audit system within your organization, please detail the connection/integration between these ones

R. "Strategic Internal Audit Plan is consistent with the objectives contained in the Strategic Plan".
(Source: Croatia Bureau of Statistics, In-depth survey on risk management practices)

R. "Once the key strategic/operational areas have been reviewed, the internal audit program will be prioritized on the agreed assessment and the risk rankings"
(Source: Australian Bureau of Statistics, In-depth survey on risk management practices)

7. Risk management information system



TAGS: Document management; Information management; Integrated and networked information system; Risk management software; Record; Web-based tool

An organization should document how it manages risk. Information about risks, and the output from all applications of the risk management process, should be **recorded** in a consistent and secure way, establishing the policies and procedures required to access, use and transfer information as a part of an information management plan. Risk management information systems should be able to:

- Record details of risks, controls and priorities, and to show any changes in them;
- Record risk treatments and related resource requirements;
- Record details of incidents and loss events, and the lessons learned;
- Track accountability for risks, controls and treatments;
- Track progress and record the completion of risk treatment actions;
- Allow progress checks against the risk management plan;
- Trigger monitoring and assurance activity.

The organization should identify adequate resources in terms of information systems and document management systems, so that capability information is relevant, reliable, timely, secure and available. This requires the maintenance of proper records and processes which generate a flow of timely, relevant and reliable information. Therefore, each stage of the risk management process should be recorded properly. Record management is an important aspect of good corporate governance: it supports activities and decisions, as well as ensuring accountability to present and future stakeholders.

The quality of an information and document management system depends on the following **principles**:

- Information across the organization should be consistent, to allow for efficient and accurate flow;
- Standardizing the definitions of terms and taxonomies ensures that different parts of the organization do not have different understandings of information, or are not operating on conflicting sets of information;

- It is not necessary to have a single record management system across the organization, as long as management designs and operates multiple systems to allow an **efficient consolidation, exchange and integration of information**.
- At the operational level, the organization should first determine the definitions, classifications and procedures needed to identify and manage risk information, as a part of an information management plan. Subsequently, as core sub-practices, it should set up 'risk management records' through the following steps:
    - Defining and maintaining a risk management classification scheme and methodology;
    - Defining an ongoing process for risk management information inventory and classification, including characteristics such as: type, preservation requirement, retention requirement, disposal requirement, availability requirement, operational/strategic value, data owner, source of information (data base/application, email, spreadsheet, etc.), confidentiality requirement, and associated organizational processes and policies.
- The organization should periodically consider changes to the classification structure, and its underlying definitions and classifications, as necessary.

The whole risk management process should be documented through a web-based tool which allows risks and treatments to be delegated and escalated among the organizational levels, and also makes it possible to connect a risk to a specific goal or activity in the operational plan of the agency (or the departments' own action plans). Consequently, the organization should identify resource requirements related to information systems and databases.

The main features of a risk management information system within each phase of the risk management process are: data exchange/interoperability, data integration, traceability, data security.

Risk identification, analysis and measurement should be carried out within a specific tool through four steps:

1. <u>Qualitative assessment</u> (risk identification and risk analysis). The risk management information tool should record the assessment of risk in a way that assists the monitoring and identification of risk priorities. Risk assessment should be documented in a way which records these processing phases. Documenting risk assessment reveals an organization's risk profile which: facilitates identification of risk priorities (in particular to identify the most significant risk issues with which senior management should concern themselves); records the reasons for decisions made about what a tolerable exposure is and is not; facilitates recording of how it is decided to address risk; allows all those concerned with risk management to see the

overall risk profile, and how their areas of particular responsibility fits into it; facilitates review and monitoring of risks.

2. Prioritization;
3. Risk measurement;
4. Monitoring risk treatment actions. Staff members/managers who are responsible for risk treatment actions have to periodically report (e.g., monthly, quarterly, yearly) on the implementation/execution of actions within the tool.

QUESTION MARK BOX

Q1. What are the most important lessons learned from implementing risk management in your organization that other organizations should take into account when developing their own risk management processes?

R1. "Efficient IT-tool is very important"

Source: Austria, *Survey on risk management practices*

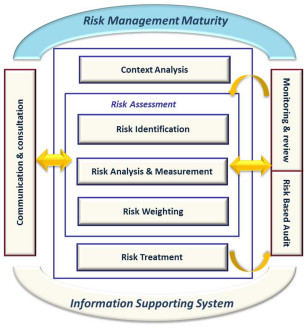
Q2. In your organization, the amount of financial resources spent to run the risk management system is suitable.
R2. "Adequate resources in the information system supporting the risk management process have been invested".

Source: Italy, *Survey on risk management practices*

Q3: In your organization, the risk management process is connected to:
R3. "Organization performance assessment: risk analysis is fully integrated in the planning and follow up process for operations and is reported by each department in a common web based tool". As for standardized techniques for risk identification and assessment: "the important thing is that the result is documented correctly in the web based tool".

Source: Sweden, *In-depth survey on risk management practices*

8. Risk management maturity model



TAGS: Corporate maturity towards risk; Development stage; Evolutionary path; Level / degree of sophistication; Maturity scale; Maturity indicators; Maturity models; Measuring progress; Phased implementation; risk management capability

In order to enable benchmarking between implementation levels of risk management in organizations, researchers, public agencies, professional associations and standards bodies tried to define their own risk management model[34]. This type of tool contains the fundamental elements of effective risk management processes, and depicts the **evolutionary scale** from a basic approach to an embedded and holistic one. It allows NSOs to gauge progress in developing the necessary risk management capabilities, and to assess the effectiveness of risk handling and impact on delivering successful outcomes. It also promotes a common language and understanding. A phased approach allows the NSO: to measure where it currently is; to set goals for where it wants to go; to plot a path to get there, focusing its efforts for improvement on areas of identified weakness. Furthermore, a maturity model can serve as a recognition program[35] within the organization: attainment of a maturity level can be considered as a performance indicator.

Moreover, given that:

– There is no optimum maturity level that would be considered as appropriate for every organization (it depends on its external context, size, internal culture, people, history, complexity of the organizations' activities, etc.)[36]; and

[34] *Risk Maturity Model (RMM)* by Hillson (1997); Government Centre for Information System (1993); Hopkinson's Risk Maturity Model for Business (2000); *Mature Risk Management Diagnostic Tool* by Basil Orsini (2002); *Risk Management Maturity Model (RMMM)* by PMI Risk Significant Interest Group - RiskSIG (2002); *The Business Risk Management Maturity Model (BRM)* by IACCM (The International Association for Contract and Commercial Management) Business Risk Management Working Group (2002); *Capability Maturity Model (CMMI)* Software Engineering Institute (SEI) (2002); *Risk Maturity Model for Enterprise Risk Management* (RIMS) by Risk and Insurance Management Society and Logic Manager (2008); *Performance Level Scale* by HM Treasury (2009); *The National performance model for risk management in the public services* by Alarm, The Public Risk Management Association – UK (2010); *Risk Management Maturity Model* by The Institute of Internal Audit (2010); Operational Risk Management Maturity Model (ORMMM) by McConnell (2012); *Comcover Risk Management Maturity Model* by the Australian Government (2013); RMMM by IIRM (Investors in Risk Management) (2015).

[35] By using a recognition program the organization can incentivize its stakeholders to continually improve resilience and performance.

[36] Wheatley (2007).

– The same entity could present heterogeneous levels of maturity with reference to different organizational areas (any risk management linked processes and activities can be more developed than others);

To facilitate deeper understanding of risk management, a **multidimensional analysis and reading grid** is proposed (Figure 5, see the full version in the Annex). It takes into account inputs from different sources: collection of actual cases of implementation of risk management systems, among statistical organizations (*practices*); selected case-studies, reporting certain significant experiences of NSOs; existing maturity models which are reported in the scientific and technical literature, also belonging to heterogeneous fields.

The grid has been developed by abstracting the principles of capability maturity modelling observed in the practices analysed, and through literature review. Its structure is a matrix where each of the cells is populated with a competency or capability. First, *some core* areas/items representing consistent sets of significant features have been identified. As a second step, specific descriptors have been developed for the purpose of illustrating in greater detail the different topics connected to the core areas. Descriptors allow the items to be allocated among four maturity levels characterised with reference to attributes/performance indicators, consisting of potential/typical features that reflect the extent to which each risk management competency or capability is defined, institutionalised and controlled. The multidimensional grid has been designed as a diagnostic tool instead of a prescriptive model for implementation: its approach builds on the assertion that the quality of an organization's risk management process should improve with time, with additional value being provided at each step toward increased maturity.

The grid also highlights, for each descriptor, three elements or reading-keys used both in the survey design, and in the processing phase. The data collected is analysed according to a theoretical paradigm/protocol named "The Template"[37]. The first element, *risk rationalities (processes)* corresponds to the organizations' efforts to translate uncertainty into a manageable and communicable conceptualization of risks, and the definitions of activities and tasks for dealing with them. It reflects the main purpose around which any organization bases its risk strategy (i.e. the improvement of compliance, performance, company value, etc.). The second element, *uncertainty experts (roles),* refers to the actors - their experience, background and interactions -, organizational units or structures to which the organization assigns the responsibility for risk management. The third element of analysis, *technologies*

[37] The *Template* shared during the *Workshop of the Modernization Committee on Organizational Framework and Evaluation*, held in Geneva on 14 to 17 October 2014, takes into account the most used and well known international standards, such as Enterprise Risk Management Conceptual Framework (ERM): Internal Control-Integrated Control, developed by Committee of Sponsoring Organizations (Co.S.O.), and ISO 31000:2009 (Risk Management – Principles and guidelines).

(support), denotes the complex sets of practices, procedures and tools enacted to accomplish the management and control of risks.

The maturity of an organization's risk management system can be categorized into clusters, that range from having no formal process, to fully integrated into all aspects of the entity. Risk management capability is a broad spectrum, ranging from the occasional informal application of risk techniques to specific projects, through routine formal processes applied widely, to a risk-aware culture with proactive management of uncertainty. In view of this, core areas/items are graded using a four-point scale, designed to take into account that each maturity level is a defined position in an achievement hierarchy, which establishes the attainment of certain risk management capabilities. This hierarchy is based on different stages of progressively mature organizational behaviour. It was judged that having more levels would increase the amount of ambiguity and misunderstanding, without giving sufficient additional refinement to aid usability and clear framing with respect to a specific NSO's context. In determining its target risk maturity level, an organization needs to consider the model as progressive: so where a competency has been achieved in a previous level, it is assumed to also have been achieved in the next level. The boundaries are defined by the ends of a continuum between an immature state to that of a mature organization. The multidimensional grid has been designed to be scalable, flexible and adaptable to accommodate changes in an organization's size, structure or regulatory context. It represents a live map which may be updated and integrated when necessary, to reflect new inputs, standards, governance regimes and so on.

At **LEVEL 1**:

- There are no risk management processes in place. The organization does not feel the need for managing risk, and does not use structured approaches for this purpose: it is not carrying-out pre-planning activity, but is reacting to situations and risk issues after they occur with no proactive thought.
- The organization is not able to distinguish between positive and negative risk.
- Management processes are repetitive, with no attempt to learn from the past and to prepare for future threats.
- There might be a belief that most important risks are known.
- The effects of risky events might be identified, but not linked to goals, and risk events are not associated with their process sources.
- No attempt is made to develop mitigation plans.
- There is no culture of control, but one of resistance to change prevailing. There is emphasis on protecting physical and financial assets.

To move from Level 1 to Level 2, the organization needs to recognize the value of risk management, and to became aware of its potential benefits. To this end, a disruptive event or external factors – such as stakeholders' influence, government pressure, etc. – may trigger a more proactive approach towards risk, and an awareness that some form of structured system needs to be put in place to deal with uncertainty.

At **LEVEL 2**:

- Top management are aware of the need to manage uncertainty and risk, and have made basic resources available to improve.
- A risk strategy has been identified, and a risk management policy has been drawn up.
- Key people are conscious of the need to assess and manage risks, and they understand risk concepts and principles.
- Some stand-alone risk processes have been identified, and the related risk mitigation activities are sometimes identified but not often executed.
- Risk management mainly focuses on past events.
- Corporate culture has little risk management accountability, with process owners not well defined or communicated.
- Risk culture is enforced by policy still interpreted, nevertheless, as compliance.
- A pilot training programme has been implemented, and a core group of people have the skills and knowledge to manage risk.
- Programs for compliance, quality management, process improvement and so on still operate independently, and have no common framework, causing overlapping risk assessment activities and inconsistencies.
- Controls are mainly based on departments and finances.
- Consistent planning and tracking of performance is missing. Qualitative risk assessments are unused or informal.

Summarizing, although the organization is aware, at some level, of the potential benefits of managing risks, there is no effective widespread implementation process, and it is up to an interested individual manager to pursue good practices. There is limited evidence that risk management is being effective in at least the most relevant areas.

At **LEVEL 3**:

- Organizational processes are identified, and risk ownership is clearly defined and well communicated to all staff.
- Authorities, roles and responsibilities are identified, and appropriate resources allocated.

- Agreement exists on a risk framework, and operating guidance is available.
- Senior managers take the lead to ensure that approaches for addressing risk are being developed and implemented in all key and relevant areas.
- Events are associated with their process sources.
- Emphasis is on developing a series of proactive action plans, to deal with events that may impact the organization and its stakeholders, to better respond to identified issues, and to consider measures reducing the likelihood of undesirable events and their consequences.
- More weight is given to pre-emptive planning.
- Qualitative assessment methods are used to determine what deeper needs exist for use of quantitative methods, analysis, tools and models.

This phase provides the opportunity to increase awareness for a large portion of the organization. There is clear evidence that risk management is being effective in all relevant areas. By the end of this stage, a culture of risk management is taking hold within the organization, and includes the management of opportunities.

At **LEVEL 4**:

- The management of risk is everyone's responsibility, and the risk management system is enforced at every level: it is embedded in all organizational processes and strategies, and is a formal part of goal setting and achievement.
- Accountability is embedded into all processes, support functions, lines and locations, as a way to achieve goals.
- A risk-based approach to achieve goals is used at all levels.
- A terminology and classification for collecting risk information is fully implemented.
- Risk and performance information is collected from all areas, to identify dependencies and root cause indicators' frequency; moreover, it is actively used to improve all organizational processes.
- Mitigation measures are determined, and a method to quantify effectiveness is understood.
- Risk mitigation is integrated with assessment (carried out with quantitative analysis, tools and models supporting qualitative methods) to monitor effective use.
- Measures ensure downside and upside outcomes of risks and opportunities are aggressively managed.
- Standardized evaluation criteria of impact, likelihood and controls' effectiveness are used to prioritize risk for follow-up activity.
- Frontline employees' participation and documents risk issues' or opportunities' significance are promoted.

- Process owners regularly review and recommend risk indicators that best measure their areas' risks.
- The results of internal adverse event planning are considered to be a strategic opportunity.
- Career development and compensation include incentives for effective risk management.
- The organization measures the effectiveness of managing uncertainties and seizing risky opportunities.
- Deviations from plans or expectations are measured against goals.
- A clear, concise and effective approach to monitoring progress toward risk management goals is communicated regularly with business areas.

Level 4 is viewed as an iterative continual improvement phase, where risk management system feedback loops permanently encourage learning from experiences in order to achieve excellence. A proficient level is characterized by specific features, such as: organizational resilience and commitment to excellence; risk management as an inseparable part of decision making and day-to-day operations; risk management as an objective in all senior management performance agreements; risk capability continually reinforced and sustained by top management; leaders regarded as exemplars; organization selected as an example of good practice by others; good record of innovation; sound risk management arrangements established to manage risks together with all partners.

Figure 5. *Extract from a Multidimensional analysis and reading grid: Risk management maturity*

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	MULTIDIMENSIONAL ANALYSIS AND READING GRID: RM MATURITY			
			STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
RISK RATIONALITIES: RM FRAMEWORK AND PROCESSES	Risk Framework	*Attitude towards uncertainties (Risk Philosophy)*	No proactive though: the organisation is reacting to situations and risk issues after they occur and it is not able to distinguish between positive and negative risk	Risk is considered a static phenomenon instead of a dynamic one. Risk approch mainly focuses on past events	Opportunistic approach: a common and consistent definition of risk exists and is applied throghout the organisation, but risk approch mainly focuses on avoiding unexpected large loss events	Open and proactive approach to risk that considers both threat and opportunity. Risk based approach to achieve goals is used at all levels
		Mandate	The board does not feel the need for managing risk	Following an external demand (legislative or regulatory, government pressure, stakeholders' influence)	By an administrative or political board	Both by a strong both administrative and political board
		Management leadership and committment	Management is not committed to establishing risk management and has not assumed a leadership role in implementing it	Some risk management initiatives are supported by top management on ad hoc basis across the organisation	Senior managers take the lead to ensure that approaches for addressing risks are being developed and implemented in all key and relevant areas	The leadership for risk management is embedded at all levels of the organization. RM is a formal and regular senior management activity. Senior management also oversees all the risk management framework and is visible involved in risk management practices and initiatives
UNCERTAINTY EXPERTS: PEOPLE, ROLES, STRUCTURES AND INTERACTIONS	Culture	*RM internal culture*	The focus is primarily on responding to crises and is reactive rather than proactive. Prevails a culture resistant to change witjh emphasis on protecting physical and financial assets	People tend to be risk adverse: a caution approach is taken to risk management overall (risk avoidance)	RM is done proactively and a culture of control is being disseminated	Individual and organisational expectations for RM are synchronised. The focus is on opportunities, not just risk avoidance. The organisation fosters a culture of continuous learning and participation and people are encourage to be innovative. Staff is highly committed to the success of the organisation
		Linkage to ethics and value	No ethics policy or guidelines in place. No clear statements of shared values or principles or attention to legal issues	Organisation may have an ethics statement but philosophy reflects legal and political considerations (compliance approach) and any written policies are applied inconsistently	Ethics and values principles/guidelines and legal/political considerations are understood by staff and risk management approach is aligned with them	Ethics and values are consistently reflected in RM organisation practices and actions. Regular surveys on this topic consider risk. An organisational climate of nmutual trust exists at all levels
TECHNOLOGIES: SUPPORT	RM Information system	*ICT tools*	No RM information system has been envisaged	A specific pilot RM information system is being implemented as a part of other information systems	A generic software may be used to support management in tracking key and relevant process areas	Each stage of the risk management process is tracked in a Web based tool thoroughly integrated with other corporate information systems
		Document management	Record management supporting activities and decisions is focused on physical and financial assets. The organisation does not document information about risk	A document management system, mainly focused on past events, may be envisaged: 1. to comply with legal, regulatory and governance requirements; 2. to record information with reference to some stand-alone processes identified and related mitigation actions	Organization identify resources in terms of document systems to support management in recording key and relevant process areas	Information about risks are recorded in a consistent and secure way, establishing the policies and procedures needed to access, use and transfer information, as part of a structured Information Management Plan. Each stage of the risk management process is recorded appropriately

QUESTION MARK BOX

Q. With reference to the risk measurement phase, does your organization use different techniques concerning risk classification (IT, financial, compliance, etc.)?
R1. "Yes. This varies considerably depending on the type of risk and the **risk maturity** of the business area. Typically corporate areas are more **risk mature**, usually by virtue of having a long standing responsibility for supporting the organization to manage a specific type of risk".

Source: Austria, *In-depth survey on risk management practices*

Q. Comments or observations:
R1. "The risk management system is still being developed, and we anticipate moving along the **maturity model** as the system is further developed".

Source: Ireland, *In-depth survey on risk management practices*

Q. Has the level of staff awareness of risks and/or risk management been evaluated during the implementation of the risk management process in your organization?
R1. "Yes, during the starting phase. A survey involving the management was carried out in order to evaluate and measure the risk perception and the **maturity** of the internal (within the single organizational divisions) and external (among divisions within the organization) control systems.

Source: Italy, *Survey on risk management practices*

R2. "Review of **risk maturity** and understanding is part of the design of the risk management framework but has not yet been developed".

Source: New Zealand, *Survey on risk management practices*

Q. In your organization, the risk management process is connected to:
R1. "Both organization and individual performance assessment. Risk management is an objective in all senior management's performance agreements – There are considerations being made to roll this out to the whole organization's employees. The organization has a risk policy and process guide, which sets out the process to which the entire organization adheres daily. The **risk maturity** level is a measure against which we record our progress, as well as management information being presented in the monthly Performance Report to Directors".

Q. In your organization, the information derived from the risk management process has been used to: Understand causes of low performance (organizations and/or individual) and review change processes:
R1. "Somewhat Agree. This is done, but the organization is developing its **risk maturity** and is not quite embedded yet, but the risk management team has a plan to ensure this continues to **mature** over the next 12 months".

Q. In your organization, which development phase is the risk management process currently in?
R1. "Some areas are very **mature**, others have opportunity for improvement, though in general it's a very good standard".

Q. What are the strengths of the risk management system in your organization?
R1. "Introduction of risk targets and reassessment of risk appetite. New risk database and new risk policy have all helped **maturity** and risk literacy".
Source: UK, *Survey on risk management practices*

9. Lessons learned

TAGS: What was most successful, what difficult and what not to do when implementing a Risk management system in NSOs

9.1 Strengths and weaknesses when implementing a risk management system in NSOs

To validate as well as underpin the Guidelines, a closing survey has been designed to get a full picture of the implementation routes for Risk management systems among statistical organizations.

This Survey has been made up of six different questionnaires addressed to as many organizational areas (*Risk management; Statistical quality analysis; Statistical production process management; Organizational process management; Internal control and/or internal auditing; Services supporting statistical production*). The sample selected has consisted of organizations presenting different levels of *Risk maturity*; therefore, the approach has been comprehensive enough to catch the diverse perspectives and so to help bring out elements that are as much as possible representative of the different contexts analysed. A dedicated Survey section made up of no more than 6 (six) questions has been provided for each target-audience area.

Each questionnaire has focused on four main subject areas:

1. RISK MANAGEMENT FRAMEWORK
2. RISK MANAGEMENT PROCESS
3. OVERARCHING PROCESSES
4. ORGANIZATION RISK MATURITY

For each subject area several topics/issues have been identified to help respondents describe their own experiences and give their own opinions and considerations.

Each ITEM has been dealt with open-ended questions targeted on the above-mentioned audiences and highlighting:

- WHAT WAS MOST SUCCESSFUL": Which have been the best effects on the organization coming from introducing Risk management;

- "WHAT WAS MOST DIFFICULT": Which have been the main stumbling blocks in developing Risk management;
- "WHAT NOT TO DO": According to the experience gained by NSOs participating in the Survey, which errors are best not to be repeated in implementing Risk management.

Here follows a selection of the "most successful", "most difficult" and "not to do" relevant topics from the third survey that have shown as the most shared (a more comprehensive and detailed selection can be found in the tables proposed at the end of every section). Such topics have also been selected for their inherent consistency as well as consistency with the Risk management guidelines, through the evidence coming from the Risk management, Quality management and Internal auditing practices among the NSOs.

To this purpose, the results from the Survey have been grouped in 5 clusters, traceable to the 4 subject areas above mentioned:

- Cluster 1: Mandate to manage risks and Risk policy;
- Cluster 2: Risk management procedure and the role of Risk management office;
- Cluster 3: Risk management Integration with other functions;
- Cluster 4: Risk management process;
- Cluster 5: Risk management supporting process

The following paragraphs analyze the answers to each of the survey items, which have been then grouped together in the following 5 affinity clusters to facilitate analysis:

- Cluster 1 - MANDATE & RISK POLICY. Items: *Mandate and commitment to manage risks; Defining a Risk Policy*
- Cluster 2 - RISK MANAGEMENT PROCEDURE AND ORGANIZATIONAL SET-UP. Items: *Risk management procedure; Setting up of a Risk management unit/office*
- Cluster 3 - RISK MANAGEMENT PROCESS. Items: *Risk identification phase; Risk assessment phase; Risk treatment phase*
- Cluster 4 - RISK MANAGEMENT INTEGRATION. Items: *Risk management integration with other organizational functions; Risk management Integration with Quality management; Risk management Integration with Internal Control/Internal Audit;*
- Cluster 5 - RISK MANAGEMENT: SUPPORTING SERVICES. Items: *Training; ICT System Supporting the RM process; Communication & Consultation*.

Paragraphs 9.2 to 9.6 outline the Clusters and related items through analyzing the most representative answers, according to the questionnaire structure (Most successful, Most difficult, Not to do).

The Summary Table at the Annex pages 45-56, shows more details about the answers.

Finally, paragraph 9.6 analyzes the risk management Integration into ongoing activities among the NSOs participating in the III Survey.

9.2 Cluster 1: Mandate to manage risks and Risk Policy

Successful:

Before implementing a risk management system a clear mandate is needed that shows the system's scope, objectives and limits, as well as that places its overall accountability at board level (i.e. risk management Committee), also locating all the necessary supporting resources, last but not least the HR and financial ones.

Risk policy directly comes from mandate and its success assumes that the Top and Senior management are involved in setting it out. The task of a risk policy is to gradually integrate Risk management within both statistical production and supporting processes and activities. Such integration can be achieved through:

- Risk policy endorsement by the Board and its spreading throughout the staff;
- Risk appetite and tolerance setting out by the Board, as well as, at an operational level, their cascading into expected so long as measurable behavior's;
- Integration between risk management system and both strategic and operational planning;
- Assigning specific objectives of risk management to the Senior managers, objectives to be taken into account when assessing their performance;
- Involving people in charge of… (strategic areas, project portfolios, projects and activity lines) into risk identification and assessment as well as risk treatment planning;
- Balancing workloads and resources to be assigned to Risk management according to the risk appetite set out;
- Creating a risk management information system integrated with the rest of management systems, in order to rationalize the workload on middle management, enhancing cooperation from this latter.

Difficult:

Some important difficulties in this Area concern the impact of the so-called soft skills[38] on the System's success.

Moreover, it is necessary to get through the distrust, mixed with misleading confidence, that risk owners following the same routines for a long time often have against a risk-based approach. It is not by chance that it can be much easier to focus on the risks out of one's own reach, because the contrary would challenge well-established routines, and then one's own ways to manage processes.

Another problem is keeping Senior managers on focusing on Risk management objectives, not only because such objectives are not submitted to performance measurement, but also for the above-mentioned reason, that is, even managers often believe that risks mostly come from processes out of their own reach.

Among difficulties there can also be found risk appetite and risk tolerance definition as well as clear communication, also considering that "a low appetite for risk, while necessary to protect the integrity of estimates, can stifle innovation".

Not to do:

Some of the main mistakes to be avoided when implementing a Risk management system are:

a) Dictating change by Top management instead of leading it, that is, instead of sharing expected benefits with external stakeholders as well as with all employees involved, in order to take all their suggestions into account;
b) Starting the implementation of a Risk management system without either a regulatory framework that clearly establishes accountabilities or a solid strategy according to the institution's priorities – while ensuring not to limit to a single office or individual the responsibility for the risk management system development.

[38] Soft skills are a combination of interpersonal skills, social skills, communication skills, personality traits, attitudes, career attributes and emotional intelligence quotient (EQ). They are all qualities not depending on the technical knowledge acquired.

9.3 Cluster 2: Risk management procedure and the role of risk management office

Successful

A risk management procedure is successful when inclusive, that is, when implies cooperation between risk management unit/office and the rest of involved employees, among which the risk owners in particular play an important role. Moreover, such a procedure should clearly detect and disclose the different roles and responsibilities, also envisaging a proper risk escalation[39] as well as defining the responsibilities for treatment in case of a risk impact on different processes (cross-cutting risks), and avoiding duplication of roles/functions within the Risk management process. Cooperation with Internal audit and Quality management is a relevant key for success, because of their valuable contribution to the whole process (see infra Area 3 -Integration).

Quality in a risk management procedure can be measured through the process tracking (detection of stages, deliverables, documents) and above all through its flexibility, intended as adaptability to the organizational context and related changes. Actually, if a procedure is too rigid it can harness the organization, thus lowering its potential.

Another task for a risk management procedure is defining the role of risk management unit/office consistently with tasks and goals designed by the mandate and risk policy. The unit/office must be formally embedded in the organization as well as formally allowed to act independently and to receive proper support (in terms of human and financial resources). Creation of a centralized office acting through a network of contact persons in order to maintain coordination seems to be the best choice. The risk management unit/office offers support and advice on Risk management to the risk owners who undertake risk management activities, being directly accountable for them.

The importance to keep a central coordination is also linked to the need to supervise cross-cutting risks impacting on different projects or processes, although such coordination is not easy to achieve.

[39] Risk escalation is the process of leading back risk treatment from a lower level of responsibility to a higher one. (i.e., from project to programme to portfolio)

Difficult

The main problem with a risk management procedure is flexibility, that is, adaptability to the organizational context, because it is not easy to balance prescription of steps with allowing people to adapt to the circumstances.

Another problem is to decide which risk management process phase is the right one to reconcile senior management and program management views, integrating top-down and bottom-up approaches. On the one hand, the senior managers consolidate bottom-up risks and define treatment priorities; on the other hand, the program managers cascade treatment actions through a detailed and viable planning.

Not to do

In drafting a procedure, it is not advisable:

a) Failing to consult customers across the organization about how the procedure can benefit them, and without a clear delivery timetable;
b) Completing stand-alone templates not linked to other documents (i.e., operational, financial and quality management planning);
c) Becoming overly focused on risk management documents losing sight of the importance of embedding the risk management approach into the daily work programming.

In creating a risk management unit/function, it is not advisable:

a) Assigning resources to the risk management unit/function that are not enough, in quality and/or quantity, with reference to the unit/office's objectives;
b) Duplicating the units/functions that give support to risk owners and supervise the Risk management process;
c) Failing to locate the risk management unit/function in a key place within the organizational chart.

9.3 Cluster 3: Risk management integration with other functions

I) With other organizational functions

Integrating a risk management function with the rest of functions and organizational areas is the key to make the system really embedded into production processes, hence more effective. Moreover, when using separate management systems across different areas of the

organization it's very difficult to make reporting at corporate level. Such an integration occurs both at risk area level (i.e. Strategic risk, Transformation risk, Statistical risk, Project risk, Fraud risk) and at function level (Quality Management, Internal auditing, P&C, ICT, Health & Safety, etc.).

However, an effective integration of a Risk management system implies a compromise, that is, giving up on creating the best risk management system while adapting it, instead, to the actual organizational structure, functions, processes and capabilities. In other words, it is the System that must adapt itself to the organization and not the opposite.

II) With Internal audit

In order to be more effective but also to best show its own potentials, risk management must be integrated with Internal auditing whenever possible. However, to do that the functions of risk management and Internal auditing must be clearly outlined in a whole framework as well as roles, responsibilities and accountabilities. One of the strength in integration is the cyclic hybridization of the two functions and related approaches, for example, using a risk based approach according to audit recommendations to determine priorities of treatment, while making risk treatment monitoring outcomes be reviewed by Internal auditing. In addition, when preparing audit recommendations it's crucial to periodically rely on risk assessments.

As regards problems, a relevant one is to keep managers' attention high against Internal auditing assurance on the effectiveness of a risk management system.

III) With Quality management

Risk management must be integrated with Quality management for the following reasons:

- the effectiveness of statistical risk treatment is higher if led by a quality expert team, because their identifying weaknesses in statistical surveys during quality reviews can result in finding potential risks within statistical processes, and then in planning improvements;
- the Quality Sector's recommendations best organize and prioritize the work of internal auditors and then help improve the overall quality of statistics;
- integration between the two systems is suggested by ISO 9001:2015, where the risk-based approach is considered as a supporting tool for quality improvement;
- definition of risk appetite and risk tolerance depends, among other things, on the kind of statistic outputs.

However, embedding the process of surveillance of quality guidelines into risk management is not always easy, because that depends on ability to persuade production areas that

development of the quality gates[40] as a component of the quality system would not be onerous and would add value to their current quality processes.

What not to do:

a) Trying to monitor implementation of quality guidelines on a basis which is too detailed, because quality must be monitored on the whole instead of on a single product or process;
b) Failing either to implement a Risk management system or to integrate it with the quality management system as well as doing it without a clear view of how to do it, or without sound understanding and knowledge of requirements for both systems, or about related standards and their application and – finally – without nominating a coordinator with clear responsibilities for the procedure.
c) Limiting risk management and quality responsibilities to a single office or individual.

9.4 Cluster 4: Risk management process

Risk identification

One of the best keys for a successful risk identification consists in involving all risk owners and internal as well as external stakeholders – first of all the Top management – to attend workshops on a regular basis. The workshops' task is to identify the main topic areas and within them, the risks. The SWOT analysis can be a sound tool to examine the NSOs' external and internal context and then facilitate brainstorming, because it helps detect the organization's strengths and weaknesses, as well as any possible threats and opportunities.

During the identification phase, the role of quality management team is crucial because, from the periodical quality audits on statistical products, the key statistical risks can be identified. Actually, the risk-based approach applied to statistical quality implies a holistic view, that is, a view involving all processes, not only the production ones, as well as all the internal and external stakeholders. Therefore, all people responsible for all processes – production as well as supporting ones – must attend the workshops.

Whatever the risks are identified, an identification procedure should be defined and kept for a while, in order to let participants adapt and fully deploy the potentials coming from knowing the risk management process.

[40] According to Australian Bureau of Statistics, quality gates are risk mitigation strategy designed to improve the early detection of errors or flaws in statistical production processes.

As regards identification techniques – which can be quite complex – it would be better to use "if… then…"-sentences, while also ensuring consideration of risk event sources outside the organization. The risk identification methodology should be explained to all participants in advance by personnel which must be expert and skilled on risk management.

The risk management process must be aligned with strategic, sector and operational planning, which means that key/priority risks must be aligned with the organization's short and long term strategic objectives. It would be better not to identify too many strategic risks, they could be less manageable. The operational risks, in turn, must be linked with the strategic ones.

Risk classification is definitely useful, as well as bringing risks together in clusters that are small enough to be analyzed, and using a framework that considers regular cyclical risks and long term program transformation risks as separate but linked groups.

The main problems during the risk identification phase concern:

- Choosing an identification methodology and letting the staff know it;
- Recognizing the interrelation among risks in order to be proactive in managing them, especially when they cross-cut more than one business area;
- Visualizing prospective risks, as well as risks that haven't occurred yet.

What not to do:

- Mistaking risks for criticalities;
- Either identifying too many risks or mistaking risks that are out of the organization's reach for actually manageable ones.

The higher the organization's risk maturity, the more workable the expected behaviors are against risk appetite in order to change the organization's culture: actually, if this latter is less mature, risks are considered as just threats instead of opportunities.

Risk assessment

In order to be successful the risk assessment phase should be led by the risk management team and supported by a specific tool. Its methodology must be shared and well understood in advance. Even the risk assessment process as well as the risk measurement criteria must be adapted to the organizational context, shared and standardized.

The risk matrix as an assessment technique has the benefit of allowing an intuitive measurement of risks as well as an easier review of it.

Risk assessment must be done by a multi-disciplinary team, especially if a qualitative assessment method is used, so that evaluation is not too affected by a single person or competency. Assessment must be preceded by a brainstorming whose task is to ensure that everybody has understood the two main risk measurement criteria, impact and likelihood. Regularly reviewing risk assessment – that is, not only concurrently with risk registers updating – by measuring both residual and inherent risk in order to keep it current is crucial.

Qualitative assessment can be integrated with quantitative one provided that updated information can easily be found. In some cases data collection could be quite expensive.

Risk assessment results (risk list and related measurement) must be shared with internal and external stakeholders, and then reviewed according to their observations. In some cases it will be useful to analyze impact from risk occurrence on particular kinds of stakeholders too (users, staff, data providers, etc.). Such assessment highly facilitates subsequent evaluation of the effectiveness of risk treatment actions.

To match bottom-up and top-down approaches, it is crucial that risk weighting at least is shared – through support from the risk management team – at Senior management board level.

Although difficult, it is useful to measure the impact from risk occurrence at both corporate and division level, according to risk interrelation, if identified in advance.

Here follow some mistakes to avoid (**what not to do**):

- Overestimating risks as well as under- or over- reporting in order to hide or artificially highlight particular risks;
- Prioritizing risks just according to their high value (likelihood to occur);
- Using complex assessment tools not easy to understand by the staff less skilled in risk management.

Risk Treatment

The responsibility for treatment planning and implementation of key-risks should be delegated to senior managers. In doing so they are supported by their own offices, both production and technical ones. Any treatment must be matched with objectives, indicators, deadlines, risk tolerance levels, and its implementation must be monitored and, if needed, adapted to different circumstances after a careful risk re-assessment.

Treatment effectiveness can be reached through matching different actions, both preventative and subsequent, at different stages of the statistical production process.

Sustainability for every treatment must be measured through cost-benefit analysis, while preferring treatment actions that could easily be embedded into production processes. To this purpose, aligning treatment operational planning with the financial one is essential.

One of the main problems concerns the difficulty of assigning resources for treatment plans that have cross-cutting effects in order to ensure an integrated organizational response, as well as a definition of duties and responsibilities for risk treatment in those cases where the risk is related to more than one process or to the whole organization.

Here follow some mistakes to avoid (what not to do):

- Keeping the Quality management team out of treatment planning;
- Failing to carry out cost-benefit analysis;
- Failing to monitor the progress of treatment actions.

9.5 Cluster 5: Risk management supporting processes

Training, communication and ICT systems have shown to be relevant strategic services supporting the risk management system implementation.

As regards **training**, including information on Risk management as a part of the welcome HR training programme, best if reiterating such training yearly at least, is something that really works.

Training delivery can be done through either workshops or e-learning, according to the target staff and/or the course arrangement. Risk management training needs a specific budget to be planned, best if a fixed one.

What not to do: delivering too general training to all staff and/or delivering risk management training every now and then, because both ways are ineffective.

As regards **ICT systems**, most NSOs agree on their relevance to support risk management implementation.

In cases where the risk maturity level is high, so is the need for an Enterprise risk management evolved software. Such software should be integrated with the other management information systems, as well as consistent with the Risk management standards and covering all the process phases. This choice entails the benefit of better managing cross-cutting risks as well as referring to the organization on the whole.

NSOs which are still implementing a risk management system prefer to use a simple tool not requiring complex computer knowledge to apply – i.e., an application like Microsoft Excel – and covering all the risk management process phases.

Whatever software is chosen, it would rather have an intuitive layout to grant dissemination and good usability throughout the staff.

One of the main challenges is the effort to integrate the risk management system with the rest of management systems used by an organization (project management, quality management, planning & control tool, etc.).

What not to do: believing that an information system, no matter how evolved, can replace mapping, analysis and management of processes.

Communication and staff consultation must be carried out at different levels and through a joint effort by all areas involved in the risk management implementation system; Risk management, Quality management and Internal auditing functions will have to play a key role in this effort.

The involvement of Top and Senior management is facilitated through regular workshops linking risk management topics with those related to performance improvement. At middle management level, it is important to get Risk management, Quality management and Internal auditing areas to cooperate – each of them according to its own know-how – to the activities aiming at engaging all management about the benefits coming from a RM system implementation. Managers, in turn, will spread the risk culture and risk-based approach to process management throughout the personnel.

Communication supports the system implementation process step-by-step through different channels (e-learning, seminars, internal communication tools, forums, workshops) according to the target – which also implies an executive and/or operational reporting.

One of the main problems is to balance the need to engage with the need to inform, thus avoiding any information surplus that can burden the routine process management in the long run.

What not to do: limiting communication and staff consultation to just a few staff categories, because the long-term task is to involve all personnel.

9.6 – Risk management integration into ongoing activities

Under closing the III Survey the respondents have been asked to give information to realize the actual level of risk management integration within their own organization. The answers have been analyzed and compared with some of the statements in the Risk maturity Multi-dimensional grid, which is contained in chapter 8 of the guidelines.

In particular, the answers have been compared with the following items and *descriptors* in the Risk maturity multi-dimensional grid:

- Risk framework (*Mandate, Risk strategy and policy, Approach to risk management, Management leadership and commitment*)
- Risk assessment (*Risk identification*)
- Controls (*Risk-based Control & Audit*)
- Risk dissemination policy (*Outcomes and deliverables, Benefits on the organization as a whole*)
- Risk management system integration (*Linkage to corporate and operational planning, risk management system integration, Integration with quality framework*)
- Roles & accountabilities in managing risks (*Roles and responsibilities of senior management, Staff Accountability*)
- Human resources (*Human resource adequacy*)
- Risk management Information system (*ICT tools, Document management*)

For example, according to the answers received the following features have been analyzed:

1) If Risk management and Quality management are aligned or completely integrated;
2) If Risk management is an integral part of strategic and business planning, at corporate and operational level;
3) If there is evidence that Risk management is supporting delivery of key outcomes in all relevant and key areas;
4) If senior managers take the lead to ensure that approaches for addressing risks are being developed and implemented in all key and relevant areas;
5) If allocation of suitable human resources for managing risk is regularly considered when planning budget and staffing;
6) If risk management responsibilities are formally stated in accountability agreements and/or governance documents and are communicated, applied and monitored at all levels;
7) If review and monitoring plans are independently monitored to determine progress and outcomes;
8) If each stage in the Risk management process is tracked in a web-based tool thoroughly integrated with other corporate information systems.

According to that, the NSOs' practices have been assigned with a Risk maturity stage from 1 to 4.

The following table shows the practices according to their own stage of risk maturity as well as the implementation "age" of their own Risk management system (the time spent implementing it – this latter information comes from the 1st Survey on risk management practices, delivered in May 2015). The table reports the number of practices that have been found, in connection with the two variables.

		Stage of Risk Maturity*			
		STAGE 1	STAGE 2	STAGE 3	STAGE 4
Years of implementation**	More than 4 years		**4**	**3**	**8**
	Less then four years		**2**		

* According to Risk Maturity multi-dimensional grid

** Information collected through the 1st Survey on Risk Management Practice

The table shows that most respondent countries, according to the information released in the 3rd Survey, place themselves at a medium-high risk maturity stage.

Acknowledgements

These guidelines have been drafted within the MCOFE Commission led by Jackie Mayda, Director Systems Engineering Division at Statistics Canada, coordinated by Steven Vale, Senior statistician at UNECE, and supported by Tetyana Kolomiyets, Statistics assistant at UNECE.

The guidelines have been drawn up by a Workgroup coordinated by Istat, (Italian National Institute of Statistics) with cooperation from the University of Rome "Tor Vergata", and composed of the following members (in alphabetical order):

1. ISTAT: Fabrizio Rotundi (coordinator), Marco Tozzi and Angela Leonetti, Directorate General – Risk Management; Eleonora Paolocci and Eleonora Rocchi, Directorate for Human Resources - Staff, Filomena Grassia, DCPS - International affairs;
2. University of Rome "Tor Vergata": Prof. Alessandro Hinna (coordinator), Ph.D. Federico Ceschel, and Dr. Danila Scarozza.

The three surveys on risk management have involved more than 60 among national and international statistical organizations.

Here follow all the participant countries:

1st survey on risk management (April – May 2015)

Albania, Andorra, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Mexico, Monaco, Mongolia, Montenegro, Netherlands, New Zealand, Norway , Poland, Portugal, Republic of Moldova, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Tajikistan, The former Yugoslav Republic of Macedonia, Turkey, Turkmenistan, Ukraine, United Kingdom, United States, Uzbekistan.

2nd survey - In-depth survey on risk management practices (September 2015)

Australia, Croatia, Austria, Ireland, Canada, The Netherlands, Lithuania, Sweden, Mexico, South Africa, New Zealand, United Kingdom, Romania, Italy

3rd survey – "What was most Successful, What was most difficult, What not to do when implementing risk management in NSOs' experiences" (July – September 2016)

Australia, Austria, Belgium, Canada, Croatia, Estonia, Eurostat, Finland, Iceland, Ireland, Italy, Lithuania Malta, Mexico, The Netherlands, New Zealand, Norway, Poland, Republic of Armenia, Romania, Slovakia, Slovenia, South Africa, Sweden, The Netherlands, United Kingdom, USA.

After the workshop on risk management practices in statistical organizations held in Geneva on 25-26 April 2016, the NSOs involved in reviewing the guidelines have sent observations and suggestions which have significantly contributed to draw up this final document.

This page has been left intentionally blank

- ANNEX -

FOCUS ON RISK MANAGEMENT PRACTICES

This page has been left intentionally blank

Index

Introduction 5
SECTION 1: RISK FRAMEWORK 7
Paragraph 1.2: Establishment risk policy. 7
FOCUS ON - Building-up a risk policy and a corporate risk profile in Statistics Canada 7
FOCUS ON: A behavioral approach to risk appetite 9
CASE STUDY 9
UK, Office for National Statistics (ONS) 9
Paragraph 1.3: Adopting an integrated risk approach connected to statistical quality management. 12
FOCUS ON: Integration risk and quality management 12
Australian Bureau of Statistics (ABS) 12
The Netherlands, Central Bureau of statistics (CBS) 14
SECTION 2: RISK MANAGEMENT PROCESS 15
Paragraph 2.1: Context analysis. 15
FOCUS ON: Measuring risk perception. 15
CASE STUDY 15
Italian National Institute of Statistics (ISTAT) 15
Paragraph 2.2: Process mapping 18
FOCUS ON: Process mapping methods 18
CASE STUDIES 18
Mexico, The National Institute of Statistics and Geography (INEGI) 18
Statistics Lithuania (SL) 19
Paragraph 3.2: Risk assessment 20
FOCUS ON: Risk assessment methodology 20
Statistics Austria 21
Italian National Institute of Statistics (ISTAT) 22
Chapter 4: Risk treatment 23
Case Studies 23
Chapter 7: Risk management information system 26
CASE STUDIES: 26
Statistics Austria 26
Statistics Lithuania (SL) 27

Statistics Sweden 28
Chapter 8: Risk management maturity model 29
CASE STUDIES: 29
UK, Office for National Statistics (ONS) 29
Italian National Institute of Statistics (ISTAT) 35
Chapter 9: Lessons learned 4343

Introduction

This Annex has to be considered an integral part of the guidelines for developing risk management practices coming from the survey analysis. Its goal is, on the one hand, to highlight the amount of information obtained, on the other hand, to show a more practical approach to the different domains of risk management.

Like the first, "theoretical" part, the Annex consists of two sections, risk framework and risk process; the paragraph arrangement also mirrors the guidelines in order to help the two parts in referring to each other.

Within both sections two categories of examples are shown:

1. Focus points on risk management core topics, in order to share practices, coming from the NSOs, able to substantiate "theoretical" information;
2. Case-studies, shortly reporting some NSOs' significant experiences on particular features of the risk management systems in order to, on the one hand, share the know-how gained from implementing risk management within the different organizational contexts, on the other hand, highlight any elements in common among the different experiences.

This page has been left intentionally blank

SECTION 1: RISK FRAMEWORK

Paragraph 1.2: Establishment risk policy.

Corporate risks are linked to the strategic objectives. In order to face each risk, a response strategy, organized in planning and actions, is developed. The example of Canada reflects the top-down approach to risk management, starting from the risk identification phase (please see the theoretical part of the guidelines for further information).

FOCUS ON - Building-up a risk policy and a corporate risk profile in Statistics Canada

At Statistics Canada, Integrated Risk Management (IRM) is an ongoing and dynamic activity that supports corporate decision-making, and is a central theme of the annual integrated strategic planning process. An integral part of Statistics Canada's risk management model is the corporate risk profile, a high-level summary of the most critical risks being managed by Statistics Canada. The development corporate risk profile was a comprehensive process that included a review of risk information from several sources and reflected recommendations from the Management Accountability Framework Round IX, as well as feedback from managers. The process also included an improved risk questionnaire, revised guidelines, and clearer definitions of risk sources. A communication strategy was developed and implemented involving information sessions, a documentation package and reinforcement of the importance of IRM in the Agency. The information sessions also served to remind managers of their roles and responsibilities in the IRM process and to address any questions and concerns they had.

All program area risk registers were reviewed and approved by the respective Field Planning Board to ensure that the risks were equally understood, explicitly identified in the long-term planning process and took into consideration interdependencies between projects. After having identified the key risks, the managers were also required to assess likelihood of occurrence and potential impact. The information collected from risk registers provided the Agency with a hierarchical risk assessment.

To ensure that the revised corporate risk profile reflected the major risks currently facing Statistics Canada, a number of significant documents were also reviewed (risk registers, program performance reports, project executive dashboards, program quality reviews, internal audit reports, the Report on Plans and Priorities, the Departmental Investment Plan, the Departmental Security Plan, and the Business Continuity Plan). This approach also

responded to the advice received from the Departmental Audit Committee (DAC), the Administrative Practices Committee (APC) and the Corporate Planning Committee of Policy Committee.

The draft corporate risk profile was developed following this advice and included the six key risks and the corresponding mitigation strategies, the risk's link to the Program Alignment Architecture and its link to organizational priorities (see example below).

Risk	Risk Response Strategy	Link to Program Alignment Architecture
Increased difficulties in reaching respondents	Mitigation strategies identified in the Agency's corporate risk profile for 2012/2013 to 2013/2014 comprise closely monitoring response rates and assessing potential biases in survey results; continuing the research and development of the dwelling-based household survey frame as an alternative to existing frames respondents; engaging respondents through various mechanisms (Statistics Canada, Government of Canada and other departments' websites as well as social media) to ensure high response rates; reviewing the possible use of administrative data sources, keeping in mind privacy concerns as these sources are used further; continuing to innovate to meet respondents' needs, which includes greater use of multi-mode data-collection options, such as e-questionnaires and mobile devices; continuing to investigate the possibility of conducting interviews by cellphone; undertaking additional studies; and incorporating lessons learned.	• Socio-economic Statistics • Labor, Education, Income and Tourism Statistics • Health and Justice Statistics • Demographic, Aboriginal and other Social Statistics • Analysis of Socio-economic Statistics • Censuses • Census of Population • Census of Agriculture • Professional and Statistical Services • Cost-recovered Services related to Socio-economic

Source: ***Corporate risk profile methodology and outcome*****. Statistics Canada: http://www.statcan.gc.ca/**

Once the 2012-13 and 2013-14 corporate risks were validated, functional leads and management committees were assigned to review existing and potentially new mitigating strategies and prepare action plans and timelines. The APC then reviewed and approved the full corporate risk profile, before it was presented to the DAC. After receiving final approval by the Corporate Planning Committee, the corporate risk profile was posted on Statistics Canada's Internal Communications Network.

The following list identifies and describes the Agency's (SC) three top corporate risks:

Increased difficulties in reaching respondents: An ongoing challenge to the quality of social statistics is the growing difficulty with collecting information from respondents. This risk was identified in both the 2012/2013 and the 2013/2014 Reports on Plans and Priorities.

Reputational risk related to respondent information: Any releases of confidential information, or real or perceived breaches of Statistics Canada's informatics infrastructure and related business processes, pose the risk of damaging reputation, credibility, image and

public trust. This risk was identified in both the 2012/2013 and the 2013/2014 Reports on Plans and Priorities.

Common tools and government wide priorities: At present, the Agency is not using any of the software tools that have been prescribed for corporate systems (i.e., the back-office systems that support human resource and financial administration and records management). The Agency's existing systems are efficient by any standard and, in the short term, re-assigning staff from core activities to implement new systems would pose a risk to providing the statistical program. This risk was identified in both the 2012/2013 and the 2013/2014 Reports on Plans and Priorities.

FOCUS ON: A behavioral approach to risk appetite

The practice described below concerns a behavioral approach to the definition of risk appetite in order to align the Institute's risk policy with the staff's risk approach.

CASE STUDY

UK, Office for National Statistics (ONS)

Risk appetite is defined as the amount of risk that an organization is prepared to accept, tolerate or be exposed to at any point in time. The Office for National Statistics has had in place an overall 'risk appetite statement' for some time. However in order to truly embed risk management in decision making, deliver the organization's strategy and respond appropriately to the pressures of an increasingly changing world, ONS decided to not only review its risk appetite but to use appetite as a catalyst for transforming its behaviors.

ONS recognized that, whilst a definition of risk appetite was essential to allow consistent and appropriate decision making, a single statement of risk appetite could be bland and open to interpretation. On a scale from 'averse' to 'actively seeking' risk, a single organization position seemed to end up at the mid-point as it would take account of areas at either end of the spectrum. Also, a statement along the lines of 'we are averse to risk in x area' is open to interpretation. What does this mean? How should staff act? What are the expectations of the organization's leaders?

To address these questions ONS ran an approach to redefine risk appetite and to ensure the strategic alignment of risk based decision making, to bring risk appetite to life, and to drive cultural change. The overall approach involved setting a level of risk appetite for each of the organization's highest level 'strategic risks', which themselves were aligned to the strategic aims within the organization's strategy. A fundamental part of the approach, however, was defining the expected and specific behaviors aligned to the level of appetite, therefore developing a clear framework for decision making.

The approach taken by the ONS risk management team was simple, it involved 1) inviting the Executive and Non-Executive Directors of the organization to individually assess risk appetite across risk types (on a matrix, see overleaf), 2) to challenge and explore their views through a series of one-to-one meetings, and 3) to discuss a consolidated view at Board level and to agree the levels of risk appetite with articulated behaviors.

The ONS experience has proven the benefits of this process. Thinking through specifically what risk appetite means for culture/behaviors has been of great benefit, by way of illustration:

- Under a 'Cautious' appetite for 'statistical quality' risks a potential behavior may be "Formal outputs must be of high quality to maintain reputation and confidence, but development and timeliness needs to be challenged in order to improve quality. Timeliness is recognized as an element of quality therefore we aim for timely statistics whenever possible."
- Under an 'Actively Seeking' appetite for 'innovation' a potential behavior may be "We recognize the risk of irrelevance without innovation and are relentlessly curious, investing considerable time in new approaches and being prepared to try new things even if many of them do not result in a viable product."

In order to ensure the success of this exercise in ONS there was a parallel approach with managers from across the organization. The idea of this was to gain buy-in to the approach and to highlight any potential disconnect between the view of the senior leadership team and that of the wider organization – therefore highlighting areas where the agreed appetite would be difficult to implement.

Following approval by the organization's Board the risk management team subsequently took the newly approved risk appetite statements and cascaded the new expectations throughout the business via seminars, risk training courses and the organization's intranet. The risk appetite matrix is also used to regularly challenge decision making and articulate Board expectations.

Redefining the ONS risk appetite through this approach has brought color to what can be a transactional and subjective process. As well as encouraging a more uniform approach to

risk taking within the organization, it supports the development of an organizational culture which is strategically aligned.

	Averse	**Minimal**	**Cautious**	**Open**	**Actively Seeking**
Risk Approach Definition	Avoidance of risk and uncertainty is a key organizational objective	Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have potential for limited reward	Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward	Willing to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward and value for money	Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk)
Risk Type 1			• Behaviors if we were to take less risk • …	• Agreed risk appetite and expected behaviors • …	• Behaviors if we were to take more risk • …
Risk Type 2			• Behaviors if we were to take less risk • …	• Agreed risk appetite and expected behaviors • …	• Behaviors if we were to take more risk • …
Risk Type 3				• Behaviors if we were to take less risk • …	• Agreed risk appetite and expected behaviors • …
Risk Type 4	• Behaviors if we were to take less risk • …	• Agreed risk appetite and expected behaviors • …	• Behaviors if we were to take more risk • …		

Paragraph 1.3: Adopting an integrated risk approach connected to statistical quality management.

Risk management must be integrated with: statistical quality management, strategic and operational planning cycle and performance assessment. Both examples proposed below have been selected because of their innovative approach to the themes of risk and quality management.

FOCUS ON: Integration risk and quality management

Australian Bureau of Statistics (ABS)

Statistical collections are often exposed to the risk that one or more of the components of the process fail to meet the quality standard expected, such that the quality or the integrity of the statistical outputs are affected. This kind of risk is the "statistical risk".

Statistical risk arises for various reasons, some of which may include inadequate inputs, processes not being well defined, changes to existing processes, or human error.

Errors in statistical outputs can be minimized by committing to quality management strategies, such as risk management. Risk management is concerned with identifying potential risks, analyzing their consequences, and devising and implementing responses, ensuring that corporate and business objectives are achieved while upholding quality.

ABS has endeavored to instigate better quality management practices through the development and use of the risk mitigation strategy known as quality gates.

The six components of a quality gate are:

1. **Placement,**
2. **Quality Measures,**
3. **Roles,**
4. **Tolerance,**
5. **Actions,**
6. **Evaluation.**

1. **PLACEMENT.** "Placement" is the first component of the quality gate. It refers to the placement of quality gates throughout a statistical process (also known as a business process cycle, or statistical process cycle). Placement of a quality gate is determined by the level of risk associated with given points in the production process. Specifically, the placement of a quality gate should occur where a risk assessment of the process reveals that there is a need for a quality gate due to the impact on the process and statistical outputs that would occur if the risk was realized.

   The ABS uses the Generic Statistical Business Process Model (GSBPM) as a guide to map the activities of statistical processes against. This is done to ensure all aspects of the statistical process are included for monitoring purposes.

   By identifying the key activities associated with each step of the statistical process, an assessment of whether there are any risks in those steps can be made up front. This assists with determining where best to place quality gates. Some common risky areas in a process include:

   - Hand-over or integration of data between multiple areas;
   - Data transformation;
   - Changes to processes, methods and systems.

The ABS has an overarching risk management framework, based on the International Risk Management Standard ISO 31000:2009, which details the ABS approach to risk management. The ABS has adapted this risk management framework to suit the business needs of the organization.

If a statistical risk assessment reveals that the risk rating is extreme or high it is recommended that a quality gate be utilized to mitigate the statistical risk.

For medium risk ratings it may be useful to utilize additional quality measures in existing quality gates that assist in monitoring the aspects which will highlight if the process isn't working correctly.

Routine procedures are generally sufficient for the monitoring of low risk ratings.

2. **QUALITY MEASURES.** Quality measures are a set of indicators that provide information about potential problems at a given point in the process. When determining what quality measures should be included in a specific quality gate it is important to consider the risks and what information would be required in order to make an assessment about fitness for purpose at that point in time.
3. **ROLES.** This component involves assigning tasks to various people or areas involved in the operation of a quality gate. Roles identifies areas or people who are directly connected to the quality gate and its operation, along with people or areas who are affected by issues with the process.

4. **TOLERANCE.** Tolerance refers to an acceptable level of quality. The acceptable level could be qualitative (e.g. Yes/No) or quantitative (e.g. 97%). Tolerance levels or thresholds are generally set by expectations of what should be observed at that point in the process for a given quality measure.
5. **ACTIONS.** Actions are predetermined responses to various outcomes for a quality gate. They provide a definition of what will be done if threshold or tolerance levels are met or not met with regards to each quality measure.
6. **EVALUATION.** As with any process that is undertaken an evaluation or review should occur to examine where improvements can be made for future use. At the end of each statistical process cycle is it recommended that the quality gates should be evaluated to determine what worked well, what didn't and where improvements can be made.

The Netherlands, Central Bureau of statistics (CBS)

Object Oriented Quality and Risk Management (OQRM) model (Nederpelt, 2012) is a quality framework developed in the field of official statistics in order to improve compliance with the European Code of Practice and deal with quality standards of statistical output.
One of the goals of OQRM was making CBS being able to decide on focus areas (60). For each of them, eleven steps can be made, including risk analysis and determining the right measures or actions to put the focus areas under control.
These measures, proposed by the managers, are integrated in the regular planning and control cycle of CBS:

1. Actions on corporate level: a set of high level objectives is identified on strategic, finance, operational and compliance level. Actions are identified to meet the objectives and assigned to the heads of divisions. Progresses of these actions are regularly monitored.
2. Action on process level: The audit framework is based on the quality guidelines for statistical processes. In these guidelines, international frameworks (CoP/QAF), national frameworks, (SN-law, privacy law, security regulations, archiving) and board decisions are integrated. Audits are also risk oriented.

The risk level is used to prioritize the recommendations in the audit report and these recommendations are converted into an action plan by the process owner.

SECTION 2: RISK MANAGEMENT PROCESS

Paragraph 2.1: Context analysis.

Risk philosophy, risk appetite e risk strategy should be always kept aligned, as one reflects the other. To this purpose it's necessary to "measure" risk perception by the management staff – as some managers may be prepared to take more risk while others are more conservative – as well as the risk maturity of organizational context, since this latter could be more or less resilient in facing risk.

FOCUS ON: Measuring risk perception.

The following example has been selected because of the experimental and iterative approach; the risk perception is strictly connected with the subjectivity of the human element and with the peculiarities of the organizational context whose impact on the risk management effectiveness is often underrated.

CASE STUDY

Italian National Institute of Statistics (ISTAT)

At Istat (Italian National Institute of Statistics), in order to measure risk perception, a questionnaire was submitted to the Top-Management in 2011. The survey was carried out 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 of the respondent; and it sometimes uses subjective terms, such as "substantially", "normally", "total", etc. as the survey is used to detect 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.

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 understanding and interpretation of data, 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:

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

Example: The risk perception by management

Figure 1 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). It also shows outliers, i.e. the maximum values (green bubbles) and minimum values (red bubbles), recorded for each dimension.

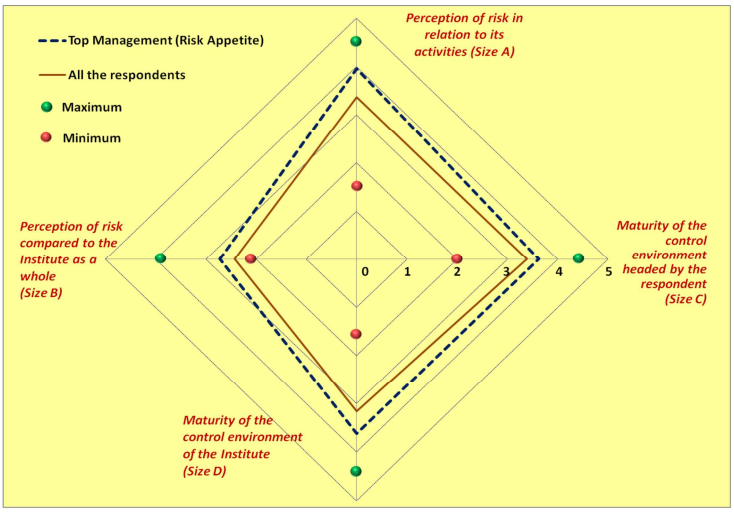


Figure 1 – Representation of the average of management profile

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. It is worth noting, however, a positive general judgment about the maturity level of the control environment, both the single structure of belonging and for 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).

Paragraph 2.2: Process mapping

FOCUS ON: Process mapping methods

CASE STUDIES

The mapping process is a crucial element of the document management system.

To exemplify the process mapping, the methodology applied by the Mexican Institute of Statistics (INEGI) and by the Institute of Statistics of Lithuania are described below.

- INEGI applies the IDEF standard; its characteristic is being modular, analytical and suitable for mapping processes involving a large number of people.
- Statistics Lithuania has focused on the interaction among production and organizational processes and on their impact on the statistical quality in terms of performance analysis; by doing so, this NSO considered the process mapping as the basis for quality management according to the standard ISO:9001**.**

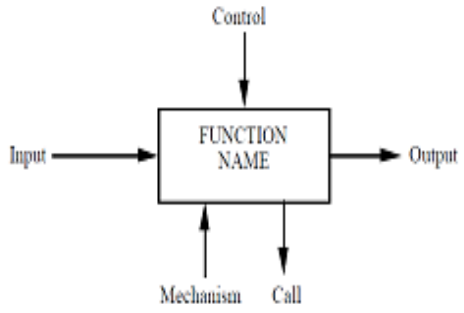
Mexico, The National Institute of Statistics and Geography (INEGI)

The National Institute of Statistics and Geography (INEGI) has been using the Standard 'Integration Definition for Function Modeling' (IDEF) to map processes since 2011. IDEF0 is an engineering technique for performing and managing functional analysis, systems design, needs analysis, and baselines for continuous improvement. The Standard has been issued by the National Institute of Standards and Technology after approval by the United States Department of Commerce.

IDEF0 is used to produce a "function model": a structured representation of the functions, activities or processes within the modeled system or subject area. The IDEF0 methodology includes procedures for developing and critiquing models by a large group of people, as well as integrating support subsystems into an IDEF0 Architecture. The result of applying IDEF0 to a system is a model that consists of a hierarchical series of diagrams, text, and glossary cross-referenced to each other. The two primary modeling components are functions (represented on a diagram by boxes) and the data and objects that inter-relate those functions (represented by arrows). An IDEF0 model is composed of a hierarchical series of diagrams that gradually display increasing levels of detail describing functions and their interfaces within the context of a system. There are three types of diagrams: graphic, text,

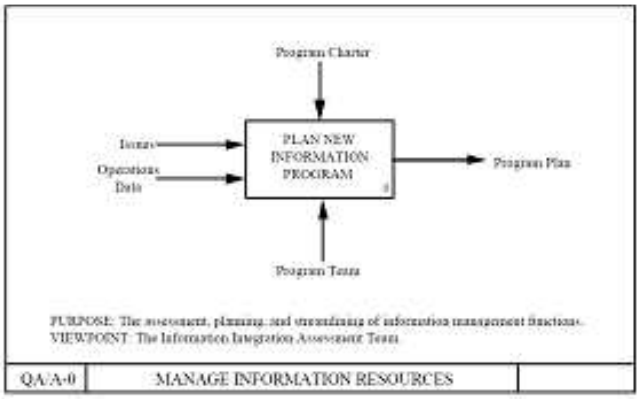
and glossary. The graphic diagrams define functions and functional relationships via box and arrow syntax and semantics. The text and glossary diagrams provide additional information in support of graphic diagrams.

Function Box and Data/Objects arrows



The graphic diagram is the major component of an IDEF0 model, containing boxes, arrows, box/arrow interconnections and associated relationships. Boxes represent each major function of a subject. These functions are broken down or decomposed into more detailed diagrams, until the subject is described at a level necessary to support the goals of a particular project. The top-level diagram in the model provides the most general or abstract description of the subject represented by the model. This diagram is followed by a series of child diagrams providing more detail about the subject.

Example of Top-Level diagram



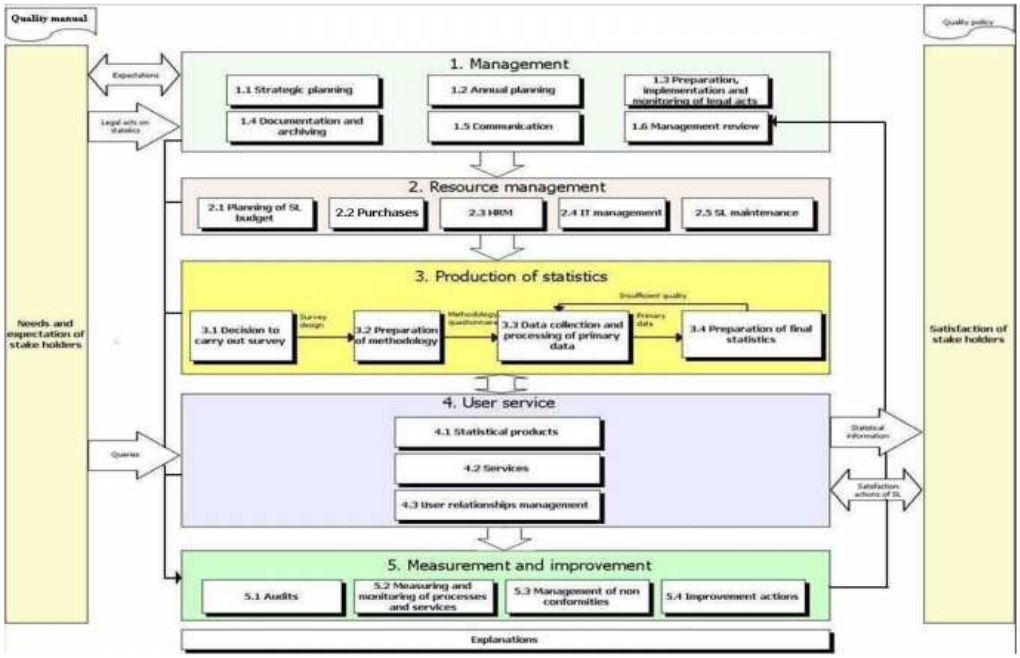
Statistics Lithuania (SL)

Process mapping in Statistics Lithuania (SL) has involved core processes, cross-cutting processes, operational activities in detail. As for the methodology followed in process mapping, ISO 9001 standard was used as a basis. Afterwards detailed analysis of performance was made, activities, their sequence and interactions were identified. In fact, ISO-certified Quality management system is based on process mapping.

Moreover, among the main elements of quality management system conforming to ISO there are: definition of the processes, identification of their interactions and sequences;

documentation of quality management system: process map, quality policy and quality tasks, quality manual. Quality management system is based on process management, which in turn is based on a detailed process map to which documented rules and guidelines on the various processes are linked. Management rules, structures, processes, activities, responsibilities, sequences and links, and associated documentation, are clearly defined and documented. The process map is a strong tool for standardization and the improvement of quality, and is also used as the backbone of the documentation system.

Processes of Statistics Lithuania: General Scheme



Paragraph 3.2: Risk assessment

FOCUS ON: Risk assessment methodology

The C & Risk Self-Assessment method involves:

- valuators are the same staff that have identified the risks;
- all assessment criteria must be the same by number and type.

In addition, the scale used for the evaluation of the likelihood and impact can be of 3, 5 or 6 levels. The higher the rating scale, the greater the distribution of the occurrences.

It is recommended to evaluate multiple types of impact, both qualitative (reputational) and quantitative (financial, operational). Each rating level must be described as objectively as possible to facilitate the task of the evaluators.

Statistics Austria

Risk indexes

Category	Range	Level
From very unlikely to impossible	0-10%	1
Unlikely or rare	10-20%	2
Possible	20-40%	3
Likely	40-60%	4
Very likely	60-80%	5
From pretty sure to sure	80-100%	6

Category	Impact (Loss)		Level
	Qualitative Interpretation	in Euro	
Very small to immaterial	Just or no substantial negative consequence on the project objectives, easily remedied	until 5.000	1
Small	Little negative impact on the project objectives	> 5.000 until 20.000	2
Remarkable/ tangible	Significantly adverse effect on the project objectives, remediable with additional expenses	> 20.000 until 100.000	3
Very remarkable/ tangible	Significant adverse impact on the project objectives, remediable with great additional expenses	> 100.000 until 200.000	4
Critical	Possible failure of the whole project or one of its fundamental part, remediable with great additional expenses	> 200.000 until 400.000	5
Extremely critical to catastrophic	Fearsome failure of the entire project, remediable with difficulty. Likely reputational damage and legal consequences	> 400.000	6

Italian National Institute of Statistics (ISTAT)

Risk indexes

ILLUSTRATIVE IMPACT SCALE		
Rating	**Descriptor**	**Definition**
5	Very high	1) Extra expenses or Financial Loss ≥ € 150.000 2) Additional human resources ≥ 30 days FTE. 3) Increasing workload ≥ 50%
4	High	1) Extra expenses or Financial Loss ≥ 100.000 and < 150.000 € 2) Additional human resources ≥ 20 and < 30 days FTE 3) Increasing workload ≥ 30% and < 50%
3	Medium	1) Extra expenses or Financial Loss ≥ 50.000 and < 100.000 € 2) Additional human resources ≥ 10 and < 20 days FTE 3) Increasing workload ≥ 20% and < 30%
2	Low	1) Extra expenses or Financial Loss ≥ 10.000 and < 50.000 € 2) Additional human resources ≥ 5 and < 10 days FTE 3) Increasing workload ≥ 10% and < 20%
1	Very low	1) Extra expenses or Financial Loss ≥ 5.000 and <10.000 € 2) Additional human resources ≥ 1 and < 5 days FTE 3) Increasing workload ≥ 5% and < 10%

ILLUSTRATIVE LIKELIHOOD SCALE		
Rating	**Descriptor**	**Definition**
5	Almost Certain	90% or greater chance of occurrence over life of asset or project
4	Frequent	a) 75% up to 90% chance of occurrence b) Once in one year
3	Likely	a) 50% up to 75% chance of occurrence b) Once in 2 years
2	Possible	a) 25% up 75% chance of occurence b) Once in 3 years
1	Rare	a) 10% up to 25% chance of occurence b) Once in 5 years

Chapter 4: Risk treatment

Decisions regarding the risks to be treated and the treatment / mitigation methods follow prioritization by top management. The response strategy to risks must include the improvement of statistical quality among the main objectives. To this end, the effectiveness of the implemented actions must be periodically assessed, also in terms of cost / benefit analysis. The treatment responsibilities are assigned and formalized at operational level.

Case Studies

Australian Bureau of Statistics (ABS)

In ABS (Australian Bureau of Statistics), accountability for risk treatment is determined by the risk owner and is often shared across a range of areas that are best placed to implement controls that can reduce the risk which may sit outside the risk owner's immediate span of control. The ABS bases the approach to risk management on the AS/NZS ISO 31000 standard. The ABS's risk appetite only tolerates high or extreme risks when treatment measures are unable to reduce the level of inherent risk to an acceptable level (i.e. Low or Moderate). Any extreme risk, such as a risk which would seriously threaten the credibility/reputation of the ABS and/or with the potential to result in a parliamentary enquiry, must be brought to the immediate attention of the Executive Leadership Group (ELG). The Senior Management Group (SMG) must be informed of any high risk, including those that may impact/tarnish the reputation of the ABS and/or achievement of program objectives e.g. through sustained media coverage. Treatment measures are essential for high and extreme risks. If strategies to mitigate the risk take time, they must be added as standing Agenda Items to ELG meetings (extreme risks) or SMG meetings (high risks) until the risk is reduced. All low or moderate risks will be managed within the specific area and/or routine procedures. All treatment measures are selected by considering the cost of implementing versus the benefits. In some cases, low and moderate risks might be accepted if the cost of treating the risk outweighs the benefit. Acceptable risks do not require treatment. Unacceptable risks will need to be treated. The Australian Bureau of Statistics (ABS) leads Australia's national statistical service, running hundreds of surveys and publishing thousands of pages of output every year. As with any large and complex organization, problems with processes do arise and the ABS has suffered errors in their data in the past with varying degrees of impact on the public domain. Most errors are detected in-house before publication, however this has at times resulted in intense last-minute work to correct the problems leading to delays in the release of data. Other errors have only been discovered after release, resulting in re-issue of statistical output. As a result of these errors the ABS has endeavored to instigate better

Quality management practices through the development and use of the risk mitigation strategy known as 'Quality gates'. Quality gates are designed to improve the early detection of errors or flaws in production processes.

Statistics Lithuania (SL)

In Statistics Lithuania (SL), according to approved descriptions of procedures, if any risky activity is identified, management is informed and improvement actions are defined and performed by responsible staff. On the base of the situation, improvement actions are implemented as soon as possible or deployed into the improvement action plan.

Process managers, appointed by the order of Director General of Statistics Lithuania, analyze identified risks, determine their causes and possible ways of their elimination, appoint staff responsible for improvements and monitor the effectiveness of improvement actions implemented. The priorities for risk treatment are set by Top management, according to the risk measurement results. The priority is given to the activities, which are the most risky for the process and process results. Usually, process managers are responsible for the risk treatment, if the risk was identified in their process. They analyze the problems, determine their causes and possible ways of their elimination, appoint staff responsible for improvements and monitor the effectiveness of improvement actions implemented.

Especially with reference to the preparation proposals for treatment, in concrete statistical areas cross-institutional commissions and working groups (e. g. group of experts in national accounts) established on the initiative of SL, play important role.

Statistics Sweden

In Statistics Sweden, risk treatment is documented in connection to the risk, specifying the treatment itself and the person responsible for carrying out the action (always a manager at department or unit level, in exceptions it can be the Director general). It also has to have a starting and finishing point. If treatment is more or less constant over time the end date is set to last of December and the action is carried over to the next year as are risks that have not been eliminated. Risks and treatments are included in the regular follow up of operations after each 4 month period with focus on effectiveness and deviations from plan. All risks that are critical require treatment unless they are impossible to prevent and/or too costly to mitigate. High value risks shall, as a rule, result in activities to mitigate the risk, either prevent it from happening or reduce the consequences. Under corporate risks are included the risks managed by the security organization. These risks have treatments that are different in characteristics and more of permanent solutions like insurance policies, contingency plans, fixed installations, firewalls and so on. Also some compliance risks are included here. They are documented in a separate module of the system since they have

other needs for follow up purposes than operational risks. All critical risks are to have treatment though and many of the medium and low risks also have treatments.

On corporate level treatments are in general delegated to the director of one or more departments and added to their risk lists. The director's comment on deviations and effectiveness and the comments are compiled by the risk manager who may suggest changes in risk values based on this. The updated risk report for the agency is presented to the DG, the deputy DG, the Director of the Director General's Office, the head of internal audit and the Head of Security by the risk manager and after discussions any adjustments are made. Once a year, after the second four month period follow up, the risk report is signed by the DG and a preliminary risk list for the coming year is set up based on the preliminary operational plan for the next year (operational risks at agency level). At the same time the risk list for corporate risks (the internal control plan) is signed by the DG.

The directors of each department are responsible for all risks within their department but can delegate carrying out treatment to unit managers. The units' risks shall be listed at department level though, since the central follow up only covers the department level and all operational risk are to be put forward to the Director general and be more easily analyzed by the risk manager. This means that the units' risk lists are generated from the departments' risk lists and they cannot add risks themselves at unit level according to the routine currently used.

Chapter 7: Risk management information system

FOCUS ON: The risk management information system

Efficient IT tool is crucial for an effective risk management. The information system must be modulated and integrated with the quality management and performance management system.

CASE STUDIES:

Statistics Austria

In Statistics Austria a specific software tool for RM and the Internal Control System (named OBSERVAR) is in place. In Statistics Austria the OBSERVAR system provides:

- modular architecture (risk management dealing with corporation-wide risks (strategic level), Internal Control System dealing with risk in operational processes, Compliance Management System dealing with compliance risks;
- the whole RM process covered;
- specialized, user-friendly and scalable software product covering over 25 modules for EGRC (Enterprise Governance, Risk and Compliance) and MIS (Management Information System) solutions;
- web-based, integration of RM, ICS and CMS;
- individually customizable system;
- prioritization approach, focus on the real important issues;
- using the tool including tailor-made risk catalogues and questionnaire forms.

Risk treatment actions are monitored by using OBSERVAR. Staff members who are responsible for risk treatment actions have to report periodically (e.g. monthly, quarterly, yearly) on the implementation/execution of actions, adherence to guidelines respectively, within OBSERVAR. The Internal Audit also uses OBSERVAR for internal audits. Risk catalogue steps (within OBSERVAR) are as follows: 1. Qualitative assessment (risk identification and risk analysis), 2. Prioritization, 3. Quantitative assessment (risk measurement). In the OBSERVAR catalogue risks are subdivided into 1. Leading Processes, 2. Core Processes, 3. Supporting Processes, 4. External Influences and Stakeholders. Statistical as well as organizational risks are included in Statistics Austria risk catalogue: both categories are integrated within the RM software tool.

Statistics Lithuania (SL)

The monitoring and control mechanism is performed via electronic document management system named SODAS and later the implementation of the actions is reported to the senior management. When risky activity is identified, the situation's causes are identified and analyzed via interviewing related staff, examination data from various systems (e.g. electronic document management systems SODAS, non-conformities and IT incidents registration system, time use recording system, providing detailed information on time used for different processes, and a specific system for recording quality characteristics of statistical surveys), performing causal-effect analysis or detailed statistical analysis. The monitoring and control mechanism is performed via electronic document management system SODAS.

The main features of the system are: effective and systematic documents management; fast and time cost saving sharing of documents; assurance of authenticity and reliability of stored documents; expeditious allocation of tasks and assignments, adequate monitoring of their implementation at all levels. The drawbacks and risky activities are registered online in special non-conformities recording system, which not only allows recording drawbacks and risky activities in a user friendly way, but also warns other staff members against possible threats.

Every staff member can inform process managers about the drawbacks and risks identified in their process via this system. It automatically informs Methodology and Quality Division, responsible for the management of the system, about new record. The system is also used for the documentation of the recorded risk analysis results and progress made in implementation of risk treatment actions.

From *Statistics Lithuania Annual Report 2010*: "As regards the realization of the vision of a paperless office, an electronic document management system Sodas was implemented at Statistics Lithuania at the end of 2009 and put into operation in 2010. The system – that has replaced the previously used system KONTORA – enables an efficient, automated and standardized management of institution's documents, control over tasks and assignments".

Statistics Sweden

All operational planning on agency/department/unit level, along with operational risks, are documented in a tool named STRATSYS that is an operational support software used in the various phases of the strategic planning, implementation, analysis, operational planning, reporting. All managers also report within the system. The internal control plan and the reports from internal quality audits are documented in the system too (certified according to ISO 20 252). It may include more things in the future. All employees have viewing rights to the agency's operational plan and to their own department's action plan and all its units' action plans. All managers have viewing access to everything, except quality audit reports concerning other units/departments than their own, and writing/creating permissions on everything on their unit/department level. Quality audits can be accessed by the auditors and the specific unit and department managers concerned. There are 3 business controllers at the Director General's Office who have admin permissions.

Most of the set up in the system is made in house by the administrator, but a contract for consultant aid from the provider is available if needed. All data is saved in a database on servers managed by the provider or its sub-contractors. The information stored is not considered to be sensitive and according to the contract the servers are guaranteed to be located within Sweden. When the contract is terminated the database shall be returned to Statistics Sweden.

Especially risks, but also plans concerning core activities are carried over between years. For the risks, values and comments for previous periods and years can be seen in the screen. Reports can easily be downloaded in different formats.

Chapter 8: Risk management maturity model

FOCUS ON: Risk management maturity model

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

CASE STUDIES:

UK, Office for National Statistics (ONS)

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

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

1. Knowledge & Skills;
2. Behaviors;
3. Metrics.

This page has been left intentionally blank

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

Level	Knowledge and Skills	Behaviors may include…	Metrics – for measuring progress
LEVEL 3 Application	Staff, managers and leaders know how to identify, assess, address, monitor and report risk in a consistent, structured manner, in line with Organizational guidance. Real ownership for risk and actions exists. Management at all levels in the organization have a clear understanding of how risk should be managed and they act in accordance with this. Management at all levels have visibility of the work they oversee, and have the skills to interpret and challenge what they see in order to expose risk. Key staff are aware of the need to manage risks with partners and have the skills and knowledge needed to manage these risks. All information asset owners have received basic training and understand: • The nature, value and benefits of the information assets they own; • the principles of risk management; and • the risks inherent in the data and systems they own. Information Asset Owners know who their risk coordinators are, and vice versa, and the IAOs know how to escalate IA risks within their business areas.	Risk workshops have been held to kick start the process. Staff are implementing basic risk management processes. Staff are using basic risk information to inform decision-making, e.g. information asset owners will typically ask why information is being requested and query which elements of the data they hold needs to be passed on. Information that is passed on will be done as safely as possible. Losses will be reduced, but not eradicated. SCS, G6 and G7 act as role models and lead on risk management. Heads of Directorate/Unit/Branch/ project/programme regularly ask: • Have you been to see for yourself how this risk is managed? • Has the risk severity changed in the last week? • What level of severity are you seeking to manage this risk down to? • What has been done about this risk in the last week? • Have you discussed this risk with your Director? • Managers: • Send a message to staff that they can be confident escalated risks will be acted upon. • Ensure risks are updated regularly, including information asset risks they are responsible for. • Identify and manage risks that cut across delivery silos. • Discuss risk each week with their staff and up the line, monitor actions weekly and check they are sufficient. • Communicate downwards what the top risks are. o Escalate risks from Divisional level • Link risk to discussions on finance – and stop/sequence projects to reduce risk as well as to cope with budget. • Demonstrate we really have an appetite for setting priorities – and stopping / slowing down the non priority areas. • Learn about good risk management from other organizations. • Send out a message that we are still ambitious but need to reduce our risk exposure. • Ensure we do not blame people for escalating risk. • Check regularly that processes are well controlled. Proactive "can do" attitude to problem solving. Leaders, managers and staff learning the lessons from past mistakes.	**We know what our top risks are, especially those affecting public protection and those escalated from the front line:** 1. Risk exist on the database at divisional, directorate and 95% of teams have recorded risks on the database. All divisions with responsibility for Agencies either have identified and recorded risks which take account of their risks shared with these bodies. This will include information asset risk registers. Risks clearly articulated in all cases 2. Risk registers, including information asset risks, are regularly updated and used at management meetings throughout the organization. 3. A process is universally and visibly in operation for escalating risks from the team level – through divisions, public bodies, suppliers, contractors, partners, projects and programmes, to directorate level and strategic level. Such risks can be tracked through the risk database. 4. Risks to data/reputation are foreseen, included on the risk database, and the extent of the risk is clearly articulated. The business is alert to risks, including those in low priority areas, e.g. such as small information systems. **Good risk behaviors – as well as good process:** 5. Risk is a standing item at management meetings throughout the organization. Managers regularly discuss risk with their staff – what the key risks are, what has changed since last week or month, how mitigating actions are being progressed. 6. Leaders and managers are visible, approachable and actively encourage staff to escalate risk. No one is blamed for escalating a risk and good risk management is recognized positively in Performance Agreement assessments. But staff are held to account for failing to escalate a risk or to take mitigating actions. 7. There is a risk champion and they support staff, actively promote good risk management behaviors and compliance with corporate standards throughout the business. 8. Key staff (project managers, SROs, business and strategic support staff) have been trained in Risk management to the appropriate level and can explain the benefits to other staff, which they do on a regular basis. Likewise, Information Asset Owners have all been trained in Risk management and can identify and escalate risks to their assets where necessary. **Planning for risks over the long term as well as the short term:** 9. All black and red risks have contingency plans, where appropriate. 10. Senior Board has been alerted to the risks including those identified on risk registers. Risks are discussed regularly (weekly) with Directors and are identified in submissions. 11. The business has defined its risk appetite, including those relating to information asset risks, and plans are in place to achieve this. 12. Risks that are three to five years away are identified and mitigating actions or contingency plans are in place. **Managing process, and information asset, risks as well as project risks and risks:** 13. Risks on the database identify process risks, especially (but not only) where: • the process is poorly defined or compliance is infrequently checked; • gaps exist between adjoining processes; • Data gets lost in the system; • the ownership of a process is not clear or is in dispute; • the process has been improved, but a legacy of old cases remains; • there is a backlog of casework; and • there are interactions between processes that are owned by different people. **14. Information asset owners are aware of the criticality of their information assets and the attendant legal requirements and are beginning to follow the published governance processes and guidance. Business areas can show the following:** • all new IS are subject to accreditation, as a matter of course; • where appropriate, Privacy Impact Assessments are used and effective contract mechanisms are used to apply IA through life; and information risks have been identified for all accredited in-service Information Systems.)

Level	Knowledge and Skills	Behaviors may include…	Metrics – for measuring progress
LEVEL 4 Embedding	In addition to the above, staff: Effectively manage those risks owned by or shared with partners, and can confidently press this point with partners. Ensure the Department communicates effectively on significant risks to the public which arise in their area. Formally review the effectiveness of all aspects of their Risk management activity. Senior management, including the Board, are actively engaged in broadening their horizons on risk through participation in internal events and training. The Organization is increasingly seen as an example of best practice across government. All information asset owners and managers are aware of the importance of managing information assets effectively and appreciate the benefits of doing so and the risks if they get it wrong.	Open communication internally on risk. Assessments of the effectiveness of risk management being undertaken. Longer term risks are integrated into the strategy and business planning functions. Business planners are beginning to think about whether enough resource has been allocated to the potential risks that may materialize during the planning cycle and allot money accordingly. Our people and workstreams are increasingly 'plugged in' to our partners. Share risk information with delivery and other business partners. Where risks are owned by others we are ready to challenge if appropriate and if we perceive there are weaknesses in their risk management. Risk workshops shared with partners. We are beginning to become more comfortable sharing risks with partners, when in the past we wouldn't. Discussions about risk are becoming increasingly more mature and widespread (and this is evidenced in minutes and notes). These discussions underpin the escalation process and form part of both the informal and formal escalation process. Executive Boards can be seen to be giving direction in the oversight and management of risk. An understanding of upside risk is beginning to be shown. Staff becoming noticeably more aware of the importance of management information and how to exploit it.	As LEVEL 3 above, but risk is becoming mainstreamed and less noticeable as a separate activity – can show evidence of this across all the business – quality of risk dialogue critical. Key elements from level 3 that are strengthened here are: • discussing, handling and escalation (metric 3 below; strengthening metric 2, 3 and 5 above); • strategic risks (metric4 below, strengthening metric 12 above); and • Process risk management (metric 6 below, strengthening metric 13 above). We know what our top risks are~~:~~ 1. We also share or discuss our critical risks amongst ourselves (cross-cutting risks) and in our key partnerships (OGDs; 3rd party contractors and suppliers), where appropriate, and we can evidence this. [In practice, this means business areas can evidence that in their top processes, (where shared, see metric 6 below); their top programmes and projects (as agreed between us and the business areas) and any other significant initiative or operational undertakings (not covered above, but agreed), assurance can be given that the top risks are discussed or shared as appropriate, supported by mapped and repeatable processes.] Good risk behaviors – as well as good process: 2. Risk management has been evaluated and judged to be effective and this can be shown through assurance and governance reporting. [In practice, this means that business can show through own governance mechanisms and/or external assurances. 3. Continuing embedment of the risk escalation process. [In practice this means that all the parts of the organization can show that there is a robust network and hierarchy for escalating risk with the 'dialogue' up and down the line as the linchpin of this framework i.e. discussions on risk take place, as regularly as the need dictates, throughout most of the organization. Escalated and de-escalated risks will be found at all levels. There is no one single model that is right, though evidence will be there through analysis/use of management info. An effective system will typically have evidence of risk discussions in the minutes and be backed up by audit returns showing the movements of risk through a business areas hierarchy.] Planning for risks over the long term as well as the short term: 4. Evidence of risk being taken account of in the business planning and resource allocation/budget setting process throughout the planning period. [Assessed as part of the business planning cycle, each business area can point to clear evidence that resources have been allocated to significant risks i.e. Risk management activity can be taken account of in the business and financial priorities for that coming year.] 5. Business Continuity Planning is in place, as required, so that: • All units, directorates and groups – where appropriate - have workable, up to date and tested BC plans in place; and • The Divisional BC Plan is on track against the prescribed timetable towards BS 25999. (This sub-metric not for individual business areas to report on, but measured centrally). Managing process, and information asset, risks as well as project risks and risks to organizational Units: 6. Where not assessed at Metric 1 above, process risks have been identified and mitigating actions are in place. [In practice this means that business areas will be expected to outline their key business processes and the attendant risks – PDU will assess if all significant threats have been identified and if they have, whether they are being adequately mitigated.] 7. All information systems that are critical to the business have been identified and subjected to Accreditation and the organization has effective information risk management processes in place to manage the residual risks* and the related, systemic IA risks. * NB In this instance, this has been taken to mean the residual risks identified by the Accreditation process. (Level 3 HMG IA Model) 8. Health and Safety improvements are on track against the Health and Safety improvement programme. (This metric for individual business areas to be marked on, but via the HO Health and Safety Sub-Committee, not via risk coordinators). 9. Compliance with information security management systems requirements - BS 27001 (Not formal accreditation).

Level	Knowledge and Skills	Behaviors may include…	Metrics - for measuring progress
LEVEL 5 Excellence	In addition to the above, staff: Embedded and long-term partnership working regimes and relationships in evidence. Use risk management to spot opportunities as well as threats. Senior management are actively engaged in broadening their horizons on risk through participation in external events. Have key staff who probably, either have professional qualifications in risk management or who have track record for proactivity in this area and an appetite for ongoing learning. These people are listened to. High profile individuals, such as DGs, noted for speaking at seminars on risk. Key risk coordinators or managers have skills to lecture and train other staff. The Organization is recognized as a centre of excellence and expertise across government. All staff at all levels is aware of the importance of managing information assets effectively and appreciates the benefits of doing so and the risks if they get it wrong.	Innovative and creative application of risk theory to everyday operations. Appreciate aspects of risk management that are not related to their day-to-day activities. Open communication internally on risk with little evidence of blame culture from raising risk issues. Regular 'stock takes' as to the effectiveness of their own risk management. Clearly recognize personal incentives for managing risk better. "It's my job to expose the errors". Staff at all levels act as a role model. Longer term risks are integrated into the strategy and business planning functions including policy making. Effective and regular public communications on potential threats. Excellent relationships with the most significant/strategic partners and stakeholders. Identification and prioritization of upside risk to actively pursue opportunities. Personal performance objectives include targets for risk management; performance appraisal and promotions include aspects related to risk management. Calculated risk taking the norm. Everyone is responsible for their own actions and their accountabilities are clearly understood. Can be used to 'showcase' risk as role models. Recognized by other organizations as leaders in risk management. Lecture and train other staff. Staff attitudes and behaviours towards assuring information are aligned to the needs of the business. Information is both 'exploited' and safeguarded, in equal measure, at all levels of the business.	*As LEVEL 4 above, but risk is mainstreamed and less noticeable as a separate activity – can show evidence of this across all the business –can point to evidence that they are 'not often 'surprised' as an organization and when this does occur, the threats are normally external in origin.:* **We know what our top risks are, especially those affecting public protection and those escalated from the front line:** 1. Ministers actively engaged in the process of risk identification and setting the organization's Risk appetite. 2. The Organization responds quickly and effectively to unanticipated risks. **3.** For all key information systems, the residual risks that are to be tolerated are quantified and the Board is aware of the level of residual information asset risk being carried. **(Level 4 HMG IA Model)** **Good risk behaviours – as well as good process:** 4. Stories of good risk management are in common currency. 5. Sustained monthly discussions on risk are long time established and routine throughout the organization. 6. Staff at all levels act as good role models with evidence of staff whom have identified risks being rewarded/recognized positively. **Planning for risks over the long term as well as the short term:** 7. Evidence of identified strategic risks being taken account of in, and giving direction to, the business planning and policy making mechanisms. 8. Risk exposure is in line with the leadership's appetite. **Managing process, and information asset, risks as well as programme/project risks and risks:** 9. Process risks have been identified and mitigating actions are in place. 10. For all IS, the residual risks that are to be tolerated are quantified and The Board is aware of the total level of information risk and systemic IA risk the organization is carrying. **(Level 5 HMG IA Model)**

Italian National Institute of Statistics (ISTAT)

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

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

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

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

Coherently with this framework, core areas / items are graded using a four-point scale, designed taking into account that each maturity level is a defined position in an achievement hierarchy establishing the attainment of certain risk management capabilities.

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	MULTIDIMENSIONAL ANALYSIS AND READING GRID: RM MATURITY			
			STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
RISK RATIONALITIES: RM FRAMEWORK AND PROCESSES	Risk Framework	*Attitude towards uncertainties (Risk Philosophy)*	No proactive though: the organisation is reacting to situations and risk issues after they occur and it is not able to distinguish between positive and negative risk	Risk is considered a static phenomenon instead of a dynamic one. Risk approch mainly focuses on past events	Opportunistic approach: a common and consistent definition of risk exists and is applied throghout the organisation, but risk approch mainly focuses on avoiding unexpected large loss events	Open and proactive approach to risk that considers both threat and opportunity. Risk based approach to achieve goals is used at all levels
		Mandate	The board does not feel the need for managing risk	Following an external demand (legislative or regulatory, government pressure, stakeholders' influence)	By an administrative or political board	Both by a strong administrative and political board
		Risk strategy and policy	The need for a risk strategy and related management policy has not been identified and accepted	A corporate risk strategy and policy has been drawn up and formally documented. It is interpreted as compliance. The need for formalizing risk tolerance and appetite is not understood	A corporate risk strategy and policy is organisation-wide documented, communicated and followed. Levels of acceptable risks are established for key and relevant areas	A risk policy states in a quantitative and multi-disciplinary way the level of risk acceptable to all organisational departments and units
		Approach to RM	No RM approach to dealing with uncertainties	Project-approach mainly based on previous organizational practices, methods, knowledge and routines	International standards and models	Customized / ad hoc model
		Management leadership and committment	Management is not committed to establishing risk management and has not assumed a leadership role in implementing it	Some risk management initiatives are supported by top management on ad hoc basis across the organisation	Senior managers take the lead to ensure that approaches for addressing risks are being developed and implemented in all key and relevant areas	The leadership for risk management is embedded at all levels of the organization. RM is a formal and regular senior management activity. Senior management also oversees all the risk management framework and is visible involved in risk management practices and initiatives
	Environmental analysis	*Internal and external context analysis*	A detection of internal (governance, organizational structure; policies, objectives, strategies; resources and knowledge; etc.) and the external RM context (regulatory / financial, technological, economic / competitive environment; key drivers and trends having impact on the organization's objectives; etc.) has been neither carried out nor planned	An internal and external context analysis has been planned or kicked-off in a fragmented / experimental or unstructured way by a core group of managers	A consultative team approach has been implemented to define the internal and external context, primary for the purpose of ensuring risks in key and relevant areas are identified effectively	The organization uses state-of-the-art methodologies for environmental scanning and accurately and periodically updates and documents the internal and external context for ensuring different views are appropriately considered in evaluating risks, for appropriate change management during risk treatment, to review policy to reflect changes in the internal and external environment

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators	Attributes / Performance indicators
RISK RATIONALITIES: RM FRAMEWORK AND PROCESSES	**Environmental analysis**	*Process Mapping*	An analysis concerning the organizational processes has been neither carried out nor planned	Some stand-alone processes have been identified at macro-level: their frame or boundaries (start / inputs and end / outputs) have been determined	A process analysis increasingly involves all key activities and relevant areas, while distinguishing among core and cross-cutting, down to operational activities in detail	All processes are broken down, analyzed and represented (while identifying objectives, inputs, information flows, roles and accountabilities, sequences and links among them / key cross-organizational dependencies and significant control nodes, outputs), combining different methods (e.g. Cause & Effect Diagram, Brainstorming, Job Shadowing , ICOR, Process Flowcharting, etc.)
		Staff risk perception evaluation	Never evaluated	A pilot evaluation is carried out with reference to a core group of people conscious of the need to manage risks and also having basic skills and knowledge	Evaluation is carried out regularly with reference to resources working in all key and relevant areas where risk management is being developed and implemented	Evaluation is carried out by expert people, regularly, at all staff levels and through advanced mixed-method approaches (e.g. questionnaires, focus groups, one-to-one focused interviews, etc.)
	Risk assessment	*Risk Identification*	No attempt is made to identify risks or to develop mitigation or contingency plans	People with appropriate knowledge have involved in identifying possible risks. Some stand-alone risk processes have been identified by central office or senior management only (Top-Down approach). The organization initiates attempts to identify and document risks and sometimes begin structuring mitigation activities	The executive and board consider risks elating to the achievement of key organisational goals and objectives. The organisation has applied a set of risk identification tools and techniques, usually of a qualitative nature. Information has been gathered from different sources to identify risks that result in key and relevant areas and events are associated with their process source	Risks are identified throughout the organization at any level and in consultation with external stakeholders (Bottom-up / Mixed approach). The organisation assesses the effectiveness of the risk identification process, identifies the drivers for identified risks and applies a set of advanced quantitative and qualitative methods. Research is performed to understand common NSO-specific risks. Risk identification is extended to all partners
		Risk Analysis & Measurement	Risk registers may have been produced by "experts" or as a one-off	Risk registers will tipically be mechanistic and compliance-focussed documents, which are up-dated on request of overseers	Risk Assessment is granular. Risk registers provide key-inputs for sharing and discuss top-risks and cross-cutting risks.	Escalated and de-esclated risks will be found at all levels. For all key information systems, the residual risks that are tolerated are quantified and the Board is aware of the level of residual information asset being carried
		Risk Treatment	Mitigation Actions and Contingency plans do not exist where they are needed	Mitigation Actions/Contingency plans exist only for some risks	Risk Treatment measures are periodically monitored and corrective plans exist for significant risks	Each business area can point to clear evidence that resources have been allocated to significant risks. All units, directorate and groups have workable, up to date and tested business continuity plans.
	Controls	*Risk Based Control & Audit*	There are no criteria in place to evaluate wheter risk management practices are efficient and effective	Controls are usde on ad hoc basis to respond to new risks and a changing environment	Ongoing oversight and monitoring of the risk function occurs on a regular bais to identify opportunities for improvement in the framework and processes of the entity. Regular reviews of compliance with the risk framework are undertaken by internal audit	Review and monitoring plans are indipendently monitored to determine progress and outcomes. Processes are assessed on a regular basis by an independent party

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	**Attributes / Performance indicators**	**Attributes / Performance indicators**	**Attributes / Performance indicators**
RISK RATIONALITIES: RM FRAMEWORK AND PROCESSES	**Risk dissemination policy**	*Outcomes and deliverables*	No evidence of improved outcomes	There is limited evidence that risk management is being effective in at least most relevant areas	There is evidence that risk management is supporting delivery of key outcomes in all relevant and key areas	There is clear evidence of very significantly improved delivery of all outcomes and showing positive and sustained improvement: RM arrangements clearly acting as a driver for change and linked to plans and planning cycles
		Impact on work and personnel	No impact on work and staff	Low impact on top / senior management culture with reference to awareness of priorities and attention to results	Middle and Low Management approach through which strategic goals are pursued is being changed. Human resources management policies related to key and relevant areas have improved	Full understanding of performance impacting factors within the organisation. Communication processes inside the organisation have significantly improved
		Benefits on the organization as a whole	No impact on the organisation	Some improvement of effectiveness related to some stand-alone processes	Key activities and quality of services in all relevant areas have improved and duplication in both activities and services have been removed	All ineffective / duplicated services and activities have been removed. All project and activity effectiveness and quality has improved.Strong sense of teamwork exists across the organization
	RM system integration	*Linkage to corporate and operational planning*	Programs operate independently and have no common framework, causing overlapping activities and inconsistencies	Risk Management is not linked with the strategic/operational planning process	Risk management is done as part of strategic/operational planning at the functional level, but non on a consistent basis throughout the organization	Risk Management is an integral part of strategic and business planning, at corporate and operational level. Risks are identified in the strategic and operational plans and mitigation plans are developed. Strategic and operational risks are aligned
	RM system integration	*Use of RM information in decision making*	Risk management information is not used in the decision making process	Risk management information is used in a fragmented and not regularly way or to fulfil a legal obligation with reference to specific processes	Information derived from the risk management process is used to assess the level of strategic goal attainment by business units, managers and employees dealing with all and relevant areas	Risk management information is used in a structured and regularly way to review corporate strategic priorities, decide on allocation of financial, HR and tangible assets, to concentrate relevant stakeholders' and employees' attention on particular key messages giving rise to change in their behaviors
		Integration with quality framework	No connection	Programs for compliance, quality management, process improvement and RM still operate independently and have no common framework, causing overlapping activities and inconsistencies	The functions are alligned but not completely integrated	The functions are completely integrated
		Connection with performance assessment system	No connection: performance in managing risks is not a factor considered in organisation / individual assessment system	Performance in managing risks is a residual factor considered in rewards and sanctions system with reference to a core group of people. Consistent organisational tracking of the performance is missing	Risk management is an objective in all senior management's performance agreements and in middle management's performance agreement in charge of key and relevant activities: roles in relation to risk are articulated in in the individual DPAs (Development and Performance Agreements). Sanctions are in place for knowingly ignoring risks	The personal performance review include assessment of risk management skills for all staff. Recognition and reward systems encourage employees to manage risks and take advantage of opportunities. Connection with both organization and individual performance assessment system is in place

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	**Attributes / Performance indicators**	**Attributes / Performance indicators**	**Attributes / Performance indicators**
RISK RATIONALITIES: RM FRAMEWORK AND PROCESSES	**Monitoring & Review**	*RM system Monitoring & Review*	A risk management system is not in place	Periodic review to ensure that risk management system is effective and continue to support organizational performance is not envisaged. Marginal and/or pilot RM implementation project monitoring activities may be carried out in a fragmented and unstructured way	A framework to measure progress in implementing risk management is in place (progress against and deviation from the RM policy and plan; review to ensure that policy and plan are still appropriate; RM process review), but performance indicators are not well refined and/or information collected to measure achieved is not available on a trend basis	A periodical and structured RM system review is carried out. The RM framework and processes are aligned to the objectives/priorities of the organisation, changes to the context are promptly addressed, resources are adequate and people have enough RM skills. Performance indicators and benchmars to measure outcomes are updated on an ongoing basis, measured regularly and results are tracked over time
UNCERTAINTY EXPERTS: PEOPLE, ROLES, STRUCTURES AND INTERACTIONS	**Organizational chart**	*RM function in the organization*	The board does not feel the need to manage risk and the related function is not included in the organisation chart	Top management / senior managers take the lead to ensure that a not-formalised core group of people have the basic knowledge to manage risk. An experimental / pilot function is being introduced	RM function is formalised within the organisation and a specific RM unit may be envisaged in the organisation chart	An independent operational risk management function exists. Staff responsible for implementing the entity's risk management framework are dedicated resources to the risk management function, with a well developed understanding of the entity and its operations
	Culture	*RM internal culture*	The focus is primarily on responding to crises and is reactive rather than proactive. Prevails a culture resistant to change witjh emphasis on protecting physical and financial assets	People tend to be risk adverse: a caution approach is taken to risk management overall (risk avoidance)	RM is done proactively and a culture of control is being disseminated	Individual and organisational expectations for RM are synchronised. The focus is on opportunities, not just risk avoidance. The organisation fosters a culture of continuous learning and participation and people are encourage to be innovative. Staff is highly committed to the success of the organisation
		Linkage to ethics and value	No ethics policy or guidelines in place. No clear statements of shared values or principles or attention to legal issues	Organisation may have an ethics statement but philosophy reflects legal and political considerations (compliance approach) and any written policies are applied inconsistently	Ethics and values principles/guidelines and legal/political considerations are understood by staff and risk management approach is aligned with them	Ethics and values are consistently reflected in RM organisation practices and actions. Regular surveys on this topic consider risk. An organisational climate of nmutual trust exists at all levels
	Stakeholders	*Internal stakeholders involvement in RM process*	No formal communication have been channels have been set up to report on risk issues.	Risk management information is shared within organisational units. Managers tend to work independently with some interaction	Risk management information is shared across organizational units and employess are encoruaged to discuss best practices and lessons learned within the organization	Best practices are shared between organizational units in a structure manner. A wide range of mediums are used to involvr all employess in managing risk
		External stakeholders involvement	Stakeholders have been identified, but there is no formal communication or understanding of theri information needs or risk tolerances	Ad hoc ommunication with stakeholders occurs and there is some understanding of theri information needs and risk tolerance	A process framework have been implemented to regularly communicate with stakeholders . Information is shared openly with stakeholders on a fully transaprent basis	The organization regularly report its strategic objectives, risks, tactics for managing risks and its performance on managing risks. Feedback from stakeholders is obtained and incorporated in the risk planning cycle.

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	**Attributes / Performance indicators**	**Attributes / Performance indicators**	**Attributes / Performance indicators**
UNCERTAINTY EXPERTS: PEOPLE, ROLES, STRUCTURES AND INTERACTIONS	**Roles & accountabilities in managing risks**	*Roles and responsibilities of senior management*	Corporate culture has no risk management accountability with process owners not defined	Specialists are responsible for managing risks and taking action in their area. Senior managers identify and respond to risks on an ad hoc basis	A formal process is in place whereby senior management assume responsibility for the overview risk management practices. Risks are identified by senior management on a collective basis, and plans of action developed	Risk management responsibilities are formally stated in accountability agreements and/or governance documents and are communicated, applied and monitored at all levels of organizations
		Staff accountability	Staff culture has no risk management accountability	Staff culture has little risk management accountability with process owners not well defined or communicated	Authorities, roles, responsibilities are identified: risk ownership is clearly defined and well communicated to all staff	The management of risk is everyone's responsibility
	Human Resources	*Human resource adequacy*	No resources are envisaged to implement a RM system	Human resources made available to manage risk are very limited and shared with other pilot programmes (not suitable or not yet evaluated)	Specific resources to support the implementation of the organisation's risk framework are envisaged but not yet adequate	The allocation of suitable human resources for managing risk is sistematically considered in the organisation's operating budget and staffing plan
		Specialist support	Specialists are not available	A core group of people understand risk concepts and principles and have skills to carry out basic, qualitative risk analysis on behalf of top management	Specialists are used on ad hoc basis to support management in key and relevant areas. They are known throughout the organisation, are seen as a key anabler in initiating change and are often called to provide services and advice with respect to specific risk management issues. Managers are aware of how best to use them	An integrated and multidisciplinary centre of excellence exists for risk management. There is a cross-fertilisation between specialists and all staff. Specialists have a broad understanding of strategic, operational and functional risk issues and are recognized externally.
	Relationship	*Internal Communication strategy*	No internal communication flows about risk	Communication issues are not considered strategic to fully inform RM policy and programme implementation	Internal communication and RM process are closely linked. RM plans/policy papers, methodological documents and information resulted from the RM system are disseminated. Clear communication protocols are in place aimed at ensuring there is a common understanding of the respective responsibilities	Open, transparent, inclusive and two-way communication to risks, uncertainty and opportunities exists. A reliable communication strategy about risk issues are in place. Interfaces are periodically reviewed. Unsolicited views are encouraged, acknowledged and appreciated
TECHNOLOGIES: SUPPORT	**RM Information system**	*ICT tools*	No RM information system has been envisaged	A specific pilot RM information system is being implemented as a part of other information systems	A generic software may be used to support management in tracking key and relevant process areas	Each stage of the risk management process is tracked in a Web based tool thoroughly integrated with other corporate information systems
		Document management	Record management supporting activities and decisions is focused on physical and financial assets. The organisation does not document information about risk	A document management system, mainly focused on past events, may be envisaged: 1. to comply with legal, regulatory and governance requirements; 2. to record information with reference to some stand-alone processes identified and related mitigation actions	Organization identify resources in terms of document systems to support management in recording key and relevant process areas	Information about risks are recorded in a consistent and secure way, establishing the policies and procedures needed to access, use and transfer information, as part of a structured Information Management Plan. Each stage of the risk management process is recorded appropriately

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	**Attributes / Performance indicators**	**Attributes / Performance indicators**	**Attributes / Performance indicators**
TECHNOLOGIES: SUPPORT	**Techniques**	*Risk Identification*	The effects of risky events might be identified but not associated with their process sources	Unstructured or informal qualitative methods since the know-how required could not be available from the staff (e.g. historical data review, semi-structured interview, prompt / check list)	Structured qualitative methods (e.g. brainstorming, Delphi method, scenario analysis, etc.) are used to determine what needs deeper quantitative methods	Multidisciplinary approach: structured qualitative and quantitative/statistical (e.g. Monte-Carlo analysis, Bayesian analysis, etc.) methods, tools and models since risks may cover a wide range of causes and consequences
		Risk Measurement	Managers tend to use their own individual approach, based on personal experience	Techniques have limited focus in specialized areas (financial risk; IT project management)	A wide range of qualitative and quantitavive tools is used for risk measurement. Knowledge transfers occurs between risk specialists and managers to balance benefits and limitations of available tools and models	Risk management tools are integrated with departmental management tools and techniques. Tools and models are assessed on a periodic basis and updated based on most recent technology
	Reporting system	*Internal Executive & Operative reporting*	Information about risk is not reported and used as a basis for decision making	Internal reporting, mainly focused on past events, may be envisaged: 1. to comply with legal, regulatory and governance requirements; 2. to disclose information with reference to some stand-alone processes identified and related mitigation actions identified but often not executed	The organization establish internal reporting mechanisms in order to support and encourage accountability and ownership of risk: internal reporting provides general information to interested internal audiences on the risk management processes in all key and relevant areas, without unnecessary detail	Comprehensive and periodic internal reporting on both significant risks and risk management performance and process is provided regularly, at both executive (board of directors) and operative level (management). It contributes to strategic oversight, decision-making and improved operational decisions. Reliability and detail of risk information has significantly increased
	Reporting system	*External reporting*	There might be some ad hoc reports are provided on specific external request (e.g. public bodies, users of statistical information through citizens' associations, media) about the effects of risky or disruptive events after they have occurred	External reporting, mainly focused on past events, may be envisaged to disclose RM information with top management / senior managers with reference to some stand-alone processes identified and related mitigation actions identified but often not executed	Organization assures external stakeholders that key risks related to relevant areas are well-managed through reports including the actions taken and why they are appropriate	There is alignment of externally and internally reported information. Both real-time and periodic risk reporting are provided to external stakeholders about the risks the organization is facing and the plans to capitalize on emerging opportunities. Periodically a review of the effectiveness of the RM system is also reported
	Training system	*RM Training and people's competence*	RM training program and activities are not evisaged. No understanding of risk principles or language. No information exists on RM competency requirements. RM is not perceived to be a formal competency	A pilot training programme on RM concepts and principle has been implemented and a core group of managers have skills to manage risk. Risk knowledge competencies have been identified	A specific training program for management is provided and personnel running RM matters in all key and relevant areas is equipped with necessary skills, guidance and learning tools. Most people have relevant skills & knowledge to manage risks effectively. Risk skills gap is being addressed	All staff at any level receives regular and appropriate guidance and training to rapidly address risks, on typical risks that the organisation faces in relation to their role/job, on the action to take in managing these risks. New staff receives early RM training. Skills transfer take place. RM competencies and training are an integral component of individual learning plans

READING KEYS	ITEMS / CORE AREAS	DESCRIPTORS	STAGE (LEVEL) 1	STAGE (LEVEL) 2	STAGE (LEVEL) 3	STAGE (LEVEL) 4
			Attributes / Performance indicators	**Attributes / Performance indicators**	**Attributes / Performance indicators**	**Attributes / Performance indicators**
TECHNOLOGIES: SUPPORT	**Communication system**	*RM internal communication instruments and tools*	No specific internal means for communicating about risk are envisaged	Some internal tools to share knowledge among a core group of people about risk have been implemented (e.g. Knowledge sharing systems such as wiki platforms, sharepoint sites)	An Internal Communication plan and a team responsible for communicating about organization's policy and ownership have been defined. Meetings with all the organizational divisions involved are organized. Other tools to share RM information are face-to-face discussion, field debriefing sessions	Adequate and efficient communication plan and tools to share RM knowledge, information and practices with all internal stakeholders and to promote co-operation and dialogue are in place (e.g. regular internal meetings, workshops and seminars, web info sessions, Intranet site regularly updated about RM issues, RM newsletter, etc.)
		RM external communication instruments and tools	No specific external means for communicating about risk are envisaged	Some external tools to share knowledge among a core group of selected stakeholders about risk may be used	Specific external tools to communicate with stakeholders about how the organisation is dealing with key risk related to relevant areas are envisaged (e.g. meetings, web info sessions, other according to selected target-audience)	Adequate plan and tools to communicate with all external stakeholders and to promote co-operation and dialogue are in place (e.g. annual meetings, annual report, workshops and seminars, Internet site regularly updated about RM issues, RM newsletter, etc.)
	Financial Resources	*Financial resources adequacy*	No resources are envisaged to implement a RM system	Finanical resources made available to manage risk are very limited and shared with other pilot programmes	A specific RM budget is provided but not yet adequate. It includes primary financial resources such as the allocation of staff to support the implementation of the organisation's risk framework and a budget to treat specific risks related to key and relevant areas	The allocation of suitable resources for managing risk is sistematically considered in the organisation's operating budget: senior executive management discusses target maturity levels for each critical component of RM and a decision is made about the necessary investments. This includes the costing of opportunities for improved processes or additional programmes and resources to implement, monitor and review the framework

Chapter 9: Lessons learned

FOCUS ON: Lessons learned from the NSOs experiences in implementing Risk management

The following summary table shows more details about the answers to each of the survey items, which have been then grouped together in the following 5 affinity clusters to facilitate analysis:

- Cluster 1 - MANDATE & RISK POLICY. Items: Mandate and commitment to manage risks; Defining a risk policy
- Cluster 2 - RISK MANAGEMENT PROCEDURE AND ORGANIZATIONAL SET-UP. Items: risk management Procedure; Setting up of a risk management Unit/Office
- Cluster 3 - RISK MANAGEMENT PROCESS. Items: Risk Identification phase; Risk assessment phase; Risk treatment phase
- Cluster 4 - RISK MANAGEMENT INTEGRATION. Items: Risk management Integration with other Organizational Functions; Risk management Integration with Quality Management; Risk management Integration with Internal Control/Internal Audit;
- Cluster 5 - RISK MANAGEMENT: SUPPORTING SERVICES. Items: Training; ICT System Supporting the RM process; Communication & Consultation.

For each ITEM the following features are higlighted:

- "WHAT WAS MOST SUCCESSFUL": Which have been the best effects on the organization coming from introducing risk management;
- "WHAT WAS MOST DIFFICULT": Which have been the main stumbling blocks in developing risk management;
- "WHAT NOT TO DO": According to the experience gained by NSOs participating in the Survey, which errors are best not to be repeated in implementing risk management.

This page has been left intentionally blank

CLUSTER 1- MANDATE & RISK POLICY					
Item	**Plus & Minus**	***Risk management Area***	***Organizational process management Area***	***Internal Audit/Control Area***	***Statistical Production process management Area***
Mandate and commitment to manage risks	Successful	a) Senior Management/Top Management Commitment b) Embedding systematic risk management into business processes c) Management engagement in risk plan at strategic, portfolio and operational level	a) Senior Management/Top Management Commitment b) Definition or risk appetite at board level and particularly the articulation of behaviors expected c) Defining the scope and boundaries of risk management	a) Senior Management/Top Management Commitment	a) Senior Management/Top Management Commitment b) Integrate risk management to planning, operations and decision making processes
	Difficult	a) Getting risk made part of Senior management objectives b) Communicating clearly scope and objectives c) The process of making the staff aware of the analysis of risk in an objective manner to counter the sense of confidence that generates the knowledge and experience of work they have done for a long time, so staff commonly considered that all tasks were under control and nothing unfortunate can happen	a) Maintaining the focus of Senior Management on risk management expectations	a) Promoting the implementation of a risk management system without a regulatory framework to support audit observations and recommendations	a) Balancing additional work load with effectiveness of risk management activities, consistently with risk appetite b) Design an integrated approach an oversight of risk management to limit additional burden on program managers c) Setting a mandate that envisages the total elimination of risk, with a limited budget
	Not to do	a) Imposing risk management without sharing expected benefits with staff b) Do not set a mandate of the RM Committee without proper resources to support it		a) Do not start the implementation of a risk management system without a regulatory framework that clearly establish responsibilities of the participants b) Do not limit RM responsibilities to a single office or individual	a) Not to consider non statistical risks (organizational risks) b) Ad hoc monitoring of risks response and tailored approaches for each divisions/programs c) Not consulting broadly with relevant stakeholders' expectations in the risk management plan development process

CLUSTER 1- MANDATE & RISK POLICY		
Item	**Plus & Minus**	**Risk management Area**
Mandate and commitment to manage risks	Successful	a) Risk policy and framework have been endorsed by senior executives, as well as across the whole organization b) The Policy includes risk management goals, context and purpose, a risk appetite statement and articulates accountabilities and responsibilities for risk management, providing instructions for staff on how to carry out risk assessments c) It's accessible to all staff and it is formally approved by the Board d) Standardizing RM process at all levels of the organization e) Establishing RM Committee, responsible for oversighting the implementation of RM system f) Clear definition of role and accountabilities
	Difficult	a) Changing the behaviors across the organization when our risk appetites were reviewed b) A low appetite for risk, while necessary to protect the integrity of estimates, can stifle innovation. c) Clear definition of risk appetite and risk tolerance
	Not to do	a) Not adapting risk policy to the official statistics business environment b) Start the implementation of risk management without having a proper regulatory framework and without a solid strategy according to the institution's priorities. c) Do not set a procedure that can be perceived as a supplementary administrative burden that demotivates management and staff

CLUSTER 2- RISK MANAGEMENT PROCEDURE AND ORGANIZATIONAL SET-UP				
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk management Procedure	Successful	a) Consolidation of risks, with high level risks and detailed underpinning (treatment) actions b) Including risk into organizational planning c) Traceability of the process (stages, deliverables, documents) d) One central and integrated IT system for risk management (RM), Internal Control System and Compliance Management System covering all phases of the processes e) Monitoring that risk management procedure is flexible at all levels f) Having a senior executive staff member allocated to each strategic risk ensures accountability for the management of each area of strategic risk	a) Active involvement of risk owners in the RM process b) Cooperation of the RM unit with other relevant units (QM, IA, Controlling) c) Defining clear accountabilities d) Process Mapping help highlight key areas of focus for quality gates and where the program is most exposed to risk, aligning risk management plans to key issues and priorities	a) Risk management procedures integration with the existing quality management system b) Quality Indicators should be useful to inform the risk management process. c) Understanding and communicating risk appetite; d) Agreeing on appropriate escalation process (including roles and accountabilities) e) Ensuring that the data is used only for statistical purposes, minimizing the risk of data disclosure f) Linking of risks vertically to Strategic Risks and aligning expected behaviors through risk appetite. Also horizontal linking of risks to identify dependencies within the portfolio and wider Organization. g) Risks are managed within Total Quality Management framework
	Difficult	a) Adequacy of the risk escalation in the RM process b) Motivation of staff due to lack of financial and human resources, as the process is resource-intensive c) Achieving balance between being overly prescriptive and mantaining sufficient flexibility for people to adopt and adapt to the circumstances	a) Defining when and how to reconcile senior management and program management views (i.e. integrating top-down and bottom up approach) b) Communicating to the organization that any change could be a source of a statistical impact and therefore require effective risk management	a) Defining, developing, producing and monitoring/analyzing the appropriate quality indicators for all statistical programs to inform the risk management process b) Changing attitudes from one of expecting risk management to be a compliance issue to one where all management levels are engaged and the documents are seen as central tools in the production process, which need to be regularly revisited and refreshed c) Engaging with stakeholders to provide input into final risk management plans d) Definition of duties and responsibilities for risk treatment in cases where the risk is related to more than one process or the whole organization

CLUSTER 2 - RISK MANAGEMENT PROCEDURE AND ORGANIZATIONAL SET-UP				
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk management Procedure	Not to do	a) Develop a procedure without consulting customers across the organization about how it can benefit them b) Completing stand-alone templates not linked to other documents c) Not integrating central system and tool d) Not relying on point in time assessments, such as once a year.	a) Not becoming overly focused on risk management documents/artefacts and losing sight of the importance of embedding the risk management approach into the work program	a) Not to distinguish between the risk management procedures and performance management b) Not have risk and quality management integrated with the financial planning process. c) Begin implementing a new process without a clear delivery timetable (the dates, areas involved and required deliverables changed several times during implementation of new risk management process) d) Have multiple areas assigned to provide similar support for the same risk/quality management plan development process without publicizing clear roles and responsibilities at the outset.

CLUSTER 2 - RISK MANAGEMENT PROCEDURE AND ORGANIZATIONAL SET-UP		
Item	**Plus & Minus**	***Risk management Area***
Setting up of a Risk management Unit/Office	Successful	a) Formal integration of the risk management in each department in the organizational chart b) The RM team operates as a centralized function area responsible for overseeing the implementation of the risk management framework in the ABS, and coordinating strategic risk management at the organizational level The team offers support and advice on risk management rather than undertaking risk management activitiesc) Establishing a risk management committee who coordinates the RM team d) RM unit reporting directly to the DG Finance and DG Statistics
	Difficult	a) Ensuring adequate independence between Internal audit and risk management functions b) Managing a large risk management work program, with a small RM Team in which expertise is concentrated in a few key staff members c) Overseeing cross-agency risks with a devolved risk management approach
	Not to do	a) Making the risk team invisible: it needs to be prominently placed and given sufficient senior support to prevent the team being viewed as a corporate burden, instead, a corporate enabler to delivery b) Underestimate funding and resources required to effectively operate the risk management office c) Not creating too many RM bodies d) Focusing more on operational risks rather than strategic ones

CLUSTER 3 - RISK MANAGEMENT PROCESS				
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk Identification phase	Successful	a) Focus on the real important issues through yearly workshops b) Implementation of an ad hoc reporting for risks system within the RM information tool c) Ensuring risks align with other corporate strategies d) Using simple “if” … “then” … statements, and considering factors external to the organization e) Flexibility of the identification model to guarantee more points of view f) Workshop approach to identification	a) Clear guidance to apply the methodology b) Aligning risk management cycle to field planning cycle c) Use a framework that considered regular cyclical risks and long term program transformation risks as separate but related groups d) Framing quality risks in an holistic manner to ensure the risks best reflected the totality of key stakeholder expectations around quality	a) Involvement of quality management into risk management workshops to identify key risks b) The results of SWOT analysis (performed to detect context of institution) are used as one of the sources for risk identification, getting Top Management involved in identification c) Performing regular quality review of statistical surveys d) Staff motivation and appropriately collaboration to identify risks and describe them in terms of statistical quality objective
	Difficult	a) Identify the interdependencies between the risks b) To imagine risky situations that have never materialized c) Ensuring everyone has the same understanding of terminology d) Determining risk owners when risks occur in different areas of activities e) Grouping risks into small enough groups f) Choosing the appropriate risk identification methodology	a) Common understanding of risks b) Establishing relation/link between strategic and operational risks	a) Identifying emerging risks or planning for unanticipated risks
	Not to do	a) Identifying too many risks and risks which aren't risks. b) To consider the process is safe and not susceptible to risks. c) Have too many strategic risks; d)Identify risks that can’t realistically be treated and managed (i.e. risks that are beyond the control of the organization)	a) Use non-knowledgeable/amateur resources to train and support program managers b) Focus only on one dimension of risk (for example, cyclical risk) or on only a narrow view of quality	a) Don't see risks only as threaths but also as opportunities b) Not having a clear risk identification process and stick to it for a few years. c) Brainstorm risk identification without necessary stakeholders in the discussion

CLUSTER 3 – RISK MANAGEMENT PROCESS				
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk Assessment phase	Successful	a) Prioritization at the Senior Management Board b) Qualitative assessment and prioritization of risks with support of IT tool c) Using a relatively simple risk assessment matrix d) Regular reviews of risks to prevent escalation e) Performing (for risk owners) training to support risk management process as well as a definition of risk identification and risk assessment criteria	a) Clear guidance to apply the methodology b) Having a small team made up staff from different work areas within the branch worked best for assessing the risk c) Evaluating and assessing selected risks by the especially created group consisting of the top management of the office and representatives of different departments within the office d) Sharing the results of risks management process with key stakeholders	a) While assessing the risk it is useful to evaluate its impact not only on the image of the institution, on the achievement of strategic objectives, etc., but also on the each group of interested parties (e.g., users, staff, data providers, etc.). Such assessment highly facilitates subsequent assessment of the effectiveness of the risk treatment actions.
	Difficult	a) Quantitative assessment of risks b) Encouraging staff to consider risks in areas outside their technical proficiency c) Getting personnel involved d) Risks prioritization	a) Keeping the risks current b) Measuring risk based on residual exposure c) Measuring the appropriate impact level of risk on the corporation vs division	
	Not to do	a) Over quantify, a lot of risk management is subjective and qualitative, this needs to be recognized b) Not to consider new emergent risks c) Not define risk evaluation criteria d) Not to discuss with regard to a common understanding of risks, as well as the probability of occurrence and impact of risks e) Overestimating risks f) Not relying on point in time assessments, such as once a year g) Under or over reporting in order to hide or artificially highlight risk	a) Do not rely on a single stakeholder to assess risks on behalf of the program or keep assessment limited within the one work area b) Using complex tool and irrelevant examples c) Not applying a standard approach to risk assessment	a) Push for only compliance (i.e. review frequency) and also focus on just high scoring risk.

CLUSTER 3 - RISK MANAGEMENT PROCESS				**1/2**
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk treatment phase	Successful	a) Development of clear mitigating actions and a regular update on progress against them b) The integration of preventive and corrective controls at different stages of the process c) Cost-benefit analysis d) Systematic approach for definition of risk mitigation actions including responsibility and timetables, involving Top Management. e) Adaption of existing risk mitigation actions if necessary. f) Assigning senior managers as strategic risk owners and giving them responsibility for developing treatment plans g) Mutual cooperation, based on the determination of the probability of the risk and the cost-benefit analysis	a) Regular reassessment of risks b) Identifying risk treatments that could easily be embedded into processes c) Monitoring the implementation of improvements in statistical production processes	a) Involvement of quality management and top management in planning risk mitigation actions b) Risk treatment procedures integration with the existing quality management system c) Definition of target risk level which has to be achieved until the end of the reporting period after treatment actions are implemented allows clear assessment of treatment actions effectiveness. d) Having the full attention of senior management when addressing a key risk e) Getting business areas to understand what tolerate means. Also aligning expected behaviors to appetite statements f) Integration of risk treatments with budgetary program

CLUSTER 3 - RISK MANAGEMENT PROCESS				**2/2**
Item	**Plus & Minus**	***Organizational process management Area***	***Statistical Production process management Area***	***Statistical Quality analysis Area***
Risk treatment phase	Difficult	a) Assigning resourcing for treatment plans that have cross-agency effects to ensure an integrated whole of organizational response is achieved b) Cost-benefit analysis	a) Cost benefit analysis b) Transferring risks appropriately following staff changes c) Finding time to incorporate risk treatments with business as usual priorities d) Exploring and adopting of a combination of response options	a) Aligning expected behaviors to appetite statements b) Definition of duties and responsibilities for risk treatment in cases where the risk is related to more than one process or the whole organization c) Tendency to address a small risk on a large/important survey rather than a larger risk that may affect several smaller programs d) Agreeing on controls and accountabilities for risks outside direct line management e) Having a global view of risks to quality, (i.e. across a set of programs, rather than a local view). f) Describing complex treatments for risk (e.g. controls that affected multiple risks or required coordination across multiple operational areas); g) Getting the right input from stakeholders to shape controls.
	Not to do	a) Don't keep track of progress of the implementation of treatment plans b) Not clearly identifying responsibility for treatment and timeframe of individual risk treatments c) Not monitoring of risks treatment	a) Not consider the systematical documentation of risks in case they occur b) Not reporting on progress of implementation	a) Not providing cost-benefit analysis b) Not defining appropriate deadlines for risk treatment c) Not ignoring the quality management staff when planning risk treatment

CLUSTER 4 - RISK MANAGEMENT INTEGRATION		
Item	**Plus & Minus**	***Risk management Area***
Risk management Integration with other Organizational Functions	Successful	a) Risk management integration with the internal audit function b) Different Areas of risks integrated within the organization: Strategic risk, Transformation risk, Statistical risk and Project risk c) Integration with other corporate functions such as planning, business continuity, and work health and safety d) Focus on statistical production and formal integration in all operational organizational functions e) Risk owners' responsibilities for specific risk areas
	Difficult	a) Making reporting at corporate level is difficult, when using separate management systems across different areas of organization b) To integrate RM with strategic planning, project management and quality management
	Not to do	a) Do not create an idealistic RM system that does not consider the actual organizational structure, functions, processes and capabilities

CLUSTER 4 - RISK MANAGEMENT INTEGRATION **(1/2)**		
Item	**Plus & Minus**	***Statistical Quality analysis Area***
Risk management Integration with Quality Management	Successful	a) Taking the recommendations made by the Quality Management team and storing them on the risk database, to focus audits b) Good collaboration in error treatment management c) Risk management integration with the existing quality management system based on the ISO 9001:2015 standard as this standard promotes the risk-based thinking through the whole organization d) Articulation of risk appetite for different statistical products e) Identification of weaknesses of statistical surveys by quality experts during quality reviews means discovery of potential risks that could occur in statistical processes and elaborating preventive program of improvements f) Quality review by outside organizations g) Risks are managed within Total Quality Management (Framework) h) Commitment at all management level to quality risks management

CLUSTER 4 - RISK MANAGEMENT INTEGRATION		**(2/2)**
Item	**Plus & Minus**	***Statistical Quality analysis Area***
Risk management Integration with Quality Management	Difficult	a) Getting the output managers to understand the value in recording and documenting the recommendations on the risk database b) Embedding process of surveillance of quality guidelines into risk management (or internal control system) c) Assuring production areas that development of the quality gates component of the quality system would not be onerous and would add value to their existing quality processes
	Not to do	a) Trying to monitor quality guidelines on a basis which is too granular b) Not implementing the risk management system, as well as no to try to integrate it with the quality management system without clear vision how to do it, without sound understanding and the knowledge of requirements defined for the both systems, related standards and their application and without designated coordinator with clear responsibilities for the procedure. c) Do not limit risk management and quality responsibilities to a single office or individual

CLUSTER 4- RISK MANAGEMENT INTEGRATION		
Item	**Plus & Minus**	***Internal Audit/Control Area***
Risk management Integration with Internal Control/IA	Successful	a) Close cooperation and coordination of Risk Management Unit and Internal Audit Unit b) Clear roles, responsibilities and accountabilities of risk management and internal audit outlining them in a framework c) Clear delimitation between the auditing and risk management functions outlined in a framework d) Use a risk based approach in determining priorities of treatment, according to audit recommendations: formal consultation of the RM by the Internal Audit during the audit planning process; Risk treatment monitoring outcomes are reviewed by Internal Auditing e) Using a risk base approach in determining priorities in recommendation in case of audits f) More awareness for staff around their responsibilities, accountabilities and how internal audits and internal controls work in the organization
	Difficult	a) Definition of risk areas for selected (planned) audit engagements b) Cooperation between IA and departmental structures, without a formal RM unit c) Fitting Expectations from management that Internal Audit would provide “assurance” on risks
	Not to do	a) Not to rely periodically on risk assessments

CLUSTER 5 - RISK MANAGEMENT: SUPPORTING SERVICES		
Item	**Plus & Minus**	***Services Supporting Statistical Production Area***
Training	Successful	a) Including information on risk management as a part of the initial HR training programme b) Establishing a competency model c) Annual training is mandatory, ongoing reminders are provided when appropriate. d) Approved funding for dedicated resources to support RM activities e) E-learning modules on risk management targeted on specific recipients f) The presence of a widespread culture of risk management as part of the work inherent in statistical production
	Difficult	a) Matching training to specific audiences needs b) Remain current and fit for purpose c) Ensuring that there is sufficient promotion of education materials for staff, including about training modules, and monitoring that staff undertake the training
	Not to do	a) Focusing training only on the transmission of knowledge about risk b) Not relying on one-time training

CLUSTER 5 - RISK MANAGEMENT: SUPPORTING SERVICES		
Item	**Plus & Minus**	***Services Supporting Statistical Production Area***
ICT System Supporting the RM process	Successful	a) ERM software covers all steps taken in connection with risk management, internal control system and compliance management (risk identification, risk assessment, risk mitigation, monitoring, audits, reporting). All information entered is unchangeably stored and recoverable for audit procedures ERM software integrates the criteria of relevant standards and frameworks (ISO 31000 ERM, COSO II ERM & Internal Control, ISO 19600) b) Mandatory IT security training for new employees before they are granted access to IT resources c) Plans to leverage existing tools, templates and project risk management web tool d) Awareness of importance of supporting tool/application in risk management process e) Using a simple tool that does not require complex computer knowledge to be used and operates as an application in Microsoft Excel, covering all the phases of the risk management process
	Difficult	a) Managing cross-agency risks and reporting at the whole of organization level without an ERM software b) Intuitive software layout c) Lack of a specialized software integrated with planning, internal control system, quality management system, compliance management
	Not to do	a) Not relying on tools as a replacement to processes

CLUSTER 5 - RISK MANAGEMENT: SUPPORTING SERVICES		
Item	**Plus & Minus**	***Services Supporting Statistical Production Area***
Communication & Consultation	Successful	a) Implementation of regular risk management workshops for top and middle management employees b) Leveraging Field Portfolio Managers to disseminate information and coordinate input from fields c) Risks discussions integrated with performance d) The risk management Framework Communicated and dissemination to staff and to external stakeholders through different channels (e-learning, seminars, internal communication channels, forum, workshops) and at different levels (strategic, operational) through the support of Quality Assurance Section e) Consultation with staff to support the implementation of the risk management framework through the Risk Team at strategic and project level (fraud risk, transformation risks, project risks, statistical risks), the Quality Assurance Section at the operational/program level (statistical risks), Internal auditors and external consultants to assist in conducting a series of risk workshops
	Difficult	a) Managing burden associated with additional monitoring and reporting requirements b) Engagement of staff to active participation during the implementation phase
	Not to do	a) Establish a limit to the participation of staff

REFERENCES

Research INVESTIGATION / AD HOC ANALYSIS ..... **III**

Complementary documentation provided by the respondent countries throughout the research was carried out by: IV

National / International Standards, Models and Guidelines ..... **V**

ISO (International Organization for Standardization) XI

Academic sources, institutional papers and professional handbooks: ..... **XVII**

This page has been left intentionally blank

Research INVESTIGATION / AD HOC ANALYSIS

UNECE (The United Nations Economic Commission for Europe)
High-Level Group for the Modernisation of Official Statistics
Modernisation Committee on Organizational Framework and Evaluation

- *Survey on Risk Management Practice*, April, 2015
- *In-Depth Survey on Risk Management*, September, 2015

Short summary

In 2015 two surveys have been carried out by the Italian Institute of Statistics in cooperation with University of Rome Tor Vergata and UNECE, in order to analyze to what extent Risk management systems are adopted among NSOs members of UNECE as well as among countries and international organizations not belonging to UNECE but yet participating in Commission's activities. The surveys were aimed at building criteria through which the practices could be identified and classified. Due to the complexity of the matter as well as in order to get more solid achievements, a multi-method model was chosen in order to use heterogeneous yet complementary approaches for analysis. According to the explorative approach, both qualitative and quantitative-descriptive tools were used: a mixed model allows to include context factors that enable a deeper understanding of phenomena, also taking into account the strategic components of the practices observed. The first Survey was submitted in May 2015 to 60 countries and 4 organizations; the response rate was around 57%. Among all respondents, thirteen countries were selected for an In-depth analysis of the Risk management most interesting practices from a NSO point of view. The selected countries were invited to answer to a second questionnaire during September 2015.

To validate as well as underpin the Guidelines, a closing survey has been designed to get a full picture of the implementation routes for Risk management systems among statistical organizations.

This Survey has been made up of six different questionnaires addressed to as many organizational areas (*Risk management; Statistical quality analysis; Statistical production process management; Organizational process management; Internal control and/or internal auditing; Services supporting statistical production*). The sample selected has consisted of organizations presenting different levels of *Risk maturity*; therefore, the approach has been comprehensive enough to catch the diverse perspectives and so to help bring out elements that are as much as possible representative of the different contexts analysed. A dedicated Survey section made up of no more than 6 (six) questions has been provided for each target-audience area.

The third Survey was submitted in July 2016 to 26 NSOs and 1 statistical organization; the average of the responses rate of the all sections was around 53%.

1. *UNECE – MCOFE Survey on Risk Management Practice,* April, 2015

Respondent countries / organizations: Australia, Austria, Canada, Croatia, Eurostat, Ireland, Italy, Lithuania, Poland, Norway, México, Romania, The Netherlands, Belgium, Estonia, Cyprus, Finland, Germany, Hungary, Iceland, Israel, Japan, New Zealand, Republic of Armenia, Republic of Macedonia, Republic of Moldova, Russia, Serbia, Slovakia, Slovenia, South Africa, Spain, Sweden, Turkey, United Kingdom.

2. *In-Depth Survey on Risk Management,* September, 2015

Respondent countries: Australia, Austria, Canada, Croatia, Ireland, Lithuania, México, Romania, The Netherlands, Sweden.

3. *Final Survey on Risk Management,* July, 2016

Respondent countries: Armenia, Australia, Austria, Canada, Estonia, Finland, Lithuania, Malta, Mexico, Norway, Poland, Republic of Armenia, Romania, Slovenia, The Netherlands, United Kingdom, USA, Croatia.

Complementary documentation provided by the respondent countries throughout the research was carried out by:

(*In most cases, the following documents are intended for the internal use of recipients only and may not be distributed or reproduced for external distribution)

Statistik Austria:

- *Risikobewertung – Risikokatalog (Observar, angepasst). 2015*
- *Data Collection for Social Statistics Project - Erhebungsinfrastruktur (EIS) Neu (Survey infrastructure). New Risk Management. 2015*
- *Risikomanagement-Katalog. Assessment von Chancen und Risiken. 2013*
- *Summary Event Catalogue, 2009.*

Australian Bureau of Statistics (ABS), Australia:

- *Risk Management Framework. Part A - The Risk Policy.* 2015
- *Risk Management Framework. Part B- The Risk Guidelines.* 2015
- *Corporate Plan 2015-2019.* 2015
- *Quality Management of Statistical Processes Using Quality Gates.* 2010
- *ABS Internal Control Framework.*
- *Accountable Authority Instructions. 01-01 Managing Risk and Internal Accountability.*

Statistics Canada:

- Corporate Risk Profile methodology and outcome (http://www.statcan.gc.ca/)
- Corporate Risk Profile 2012-2104. 2012

Statistics Lithuania:

- Extraction from SL risk register

Instituto Nacional de Estadística, Geografía e Informática (INEGI), México:

- *Matriz de Administración de Riesgos.* 2015
- *Selected items of Risk Matrix for the 2015 Intercensal Survey.* 2015
- *Manual de integración y funcionamiento del comité de auditoría y riesgos del instituto nacional de estadística y geografía. 2014*
- *Metodología para la Administración de Riesgos en el INEGI. 2014*
- *Acuerdo de la junta de gobierno del instituto nacional de estadística y geografía, por el que se establecen las normas de control interno para el instituto nacional de estadística y geografía. 2014*
- *Draft Federal Information Processing Standards Publication 183. Standard for Integration Definition for Function Modeling (IDEF0). 1993*

Institutul National De Statistica, Romania:

- *Ordin nr 1038-2011 - procedura sistem management riscuri.* 2011

National / International Standards, Models and Guidelines

ANAO (The Australian National Audit Office)

Reference published Guide:

- *Public Sector Audit Committees. 2.1 Risk Management.* August, 2011

Highlights

The Guide updates and replaces the Australian National Audit Office's (ANAO) 2005 *Public Sector Audit Committees Better Practice Guide*. While many of the principles and practices remain the same, this Guide incorporates a number of enhancements. These include a discussion on: a committee's responsibilities in relation to Risk management and other portfolio entities; the benefits of periodically engaging with the entity Chief Executive/Board, including in relation to the committee's responsibilities for reviewing high risk programs and projects. This Guide is intended to complement the Fraud Control Guidelines, and to augment the key fraud control strategies referred to in the Guidelines. While this document is an important tool for senior management and those who have direct responsibilities for fraud control, elements of this Guide will be useful to a wider audience, including employees, contractors and service providers. The aim of the Guide is to provide guidance on the operation of the Audit Committees of public sector entities operating under both the *Financial Management and Accountability Act 1997* and the *Commonwealth Authorities and Companies Act 1997*. As with all of the ANAO's Better Practice Guides, each entity is encouraged to use it to identify, and apply, better practice principles and practices that are tailored to its particular circumstances. The Guide discusses a range of functions and responsibilities, grouped under nine broad areas, that are appropriate for an Audit Committee.

Available:

www.anao.gov.au/html/Files/BPG%20HTML/BPG_PublicSectorAuditCommittees/2_1.html

AS/NZS (Joint Australian New Zealand International Standard). Joint Technical Committee OB-007, Risk Management

Reference published Guide:

- *AS/NZS ISO 31000:2009. Risk Management – Principles and guidelines*. November, 2009

Highlights

The Standard is a joint Australia/New Zealand adoption of ISO 31000:2009, and supersedes AS/NZS 4360:2004. It was approved on behalf the Council of Standards Australia on 6 November 2009 and on behalf of the Council of Standards New Zealand on 16 October 2009. Its predecessor, AS/NZS 4360 *Risk management*, was first published in 1995. After AS/NZS 4360 was last revised in 2004, the joint Australia/New Zealand committee OB-007 decided that rather than undertake a similar revision in 2009, it would have promoted the development of an international standard on risk management, which could then be adopted locally. The standard provides organizations with guiding principles, a generic framework, and a process for managing risk. New to this edition is the inclusion of 11 risk management principles an organization should comply with, and a management framework for the effective implementation and integration of these principles into an organization's management system. Emphasis is given to considering risk in terms of the effect of uncertainty on objectives, rather than the risk incident. This edition also includes an informative annex that sets out the attributes of enhanced risk management for those organizations that have already been working on managing their risks and may wish to strive for a higher level of achievement.

Available:

https://shop.standards.govt.nz/catalog/31000%3A2009%28AS%7CNZS+ISO%29/view

Basel Committee - Risk Management Sub-group

Reference published guidance:

- *Framework for Internal Control Systems.* September, 1998

Highlights

The Basel Committee on Banking Supervision, which includes supervisory authorities from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States, introduced the *Framework for Internal Control Systems* in 1998. The Basel Committee distributed this Guidance to supervisory authorities worldwide in the belief that the principles presented will provide a useful framework for the effective supervision of internal control systems. More generally, the Committee wished to emphasize that sound internal controls are essential. The five elements of internal control are: management oversight and control culture, risk recognition and assessment, control activities and segregation of duties, information and communication, and monitoring activities and correcting deficiencies. The effective functioning of these five elements is key to an organization achieving its performance, information, and compliance objectives. The guidance does not focus on specific areas or activities within a banking organization. The exact application depends on the nature, complexity and risks of the organization's activities. While closely linked to the specific sector, the principles of this guidance can be taught and effectively applied throughout different areas.

Available:
www.bis.org/publ/bcbs40.htm

CIMA (The Chartered Institute of Management Accountants)

Reference published Guide:

- *Introduction to managing risk.* Topic Gateway series no. 28. February, 2008

Highlights

The Chartered Institute of Management Accountants is the world's largest and leading professional body of management accountants. It has more than 229,000 members and students in 176 countries. It has strong relationships with employers and sponsor leading research. The Chartered Institute of Management Accountants supports its members and students with its Technical Information Service (TIS) for their work and needs. Topic Gateways are intended as a refresher or introduction to topics of interest to CIMA members. They include a basic definition, a brief overview and a fuller explanation of practical application. Finally they signpost some further resources for detailed understanding and research. The Guide was prepared by Technical Information Service.

Available:
www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_intro_to_managing_rist.apr07.pdf

CNRMA

Reference published Guidance:

- *OPNAVINST 3500.39 (series), Operational Risk Management (ORM)*. July, 2010

Highlights

ORM is the guiding Navy instruction for implementing the Operational Risk Management program. CNRMA manages and oversees shore installation management support and execution within the Mid-Atlantic region. The naval vision is to develop an environment in which every individual (officer, enlisted and civilian) is trained and motivated to personally manage risk in everything they do on and off duty, both in peacetime and during conflict, thus enabling successful completion of all operations or activities with the minimum amount of risk. Commands have a number of responsibilities relative to ORM, including designating

the Executive Officer as the ORM Program Manager to oversee command ORM training and implementation and ensuring that at a minimum one officer and one senior enlisted are qualified as ORM instructors. While closely linked to this specific sector, the principles of this guidance can be taught and effectively applied throughout different areas: many ORM techniques can be incorporated into operational planning and decision making processes related to various sector of activity.

Available:
www.public.navy.mil/airfor/nalo/Documents/SAFETY/OPNAVINST%203500.39C%20OPERATIONAL%20RISK%20MANEGEMENT.pdf

COSO (The Committee of Sponsoring Organizations of the Treadway Commission)

Reference published Guidance:

- *Enterprise Risk Management (ERM) – Integrated Framework.* September, 2004

Reference published papers:

- *Risk Assessment in Practice*. October, 2012
- *Developing Key Risk Indicators to Strengthen Enterprise Risk Management.* December, 2010.
- *Strengthening Enterprise Risk Management for Strategic Advantage*. 2009

Highlights

COSO is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance. The members of COSO are: the American Institute of Certified Public Accountants, the American Accounting Association, Financial Executives International, the Institute of Management Accountants and The Institute of Internal Auditors. ERM is a widely used framework in the United States and around the world. Over two decades ago, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued "Internal Control – Integrated Framework" to help businesses and other entities assess and enhance their internal control systems. That framework has since been incorporated into policy, rule and regulation and used by thousands of enterprises and organizations to better control their activities in moving toward achievement of their established objectives. In 2001, COSO initiated a project, and engaged *PricewaterhouseCoopers*, to develop a framework that would be readily usable by managements to evaluate and improve their organizations' enterprise risk management. COSO engaged PricewaterhouseCoopers after concluding there was a need for a broadly recognized enterprise risk management framework. *PricewaterhouseCoopers* was assisted by an advisory council composed of representatives from the five COSO organizations. Because of the importance of the project, the Framework was exposed for public comment before final publication. COSO recognized that while many organizations may be engaged in some aspects of enterprise risk management, there has been no common base of knowledge and principles to enable boards and senior management to evaluate an organization's approach to risk management and assist them in building effective programs to identify, measure, prioritize and respond to risks. "ERM – Integrated Framework" expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management for all organizations, regardless of size. The framework defines essential enterprise risk management components, discusses key principles and concepts, suggests a common language, and provides clear direction and guidance for enterprise risk management.

Available:
www.coso.org/ERM-IntegratedFramework.htm
www.coso.org/documents/COSO_09_board_position_final102309PRINTandWEBFINAL_000.pdf
www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf
www.coso.org/documents/COSOKRIPaperFull-FINALforWebPostingDec110_000.pdf

A (Chartered Professional Accountants of Canada)

Reference published Guide:*Guidance on Control. CoCo (Criteria of Control) Framework.* 1995

Highlights

Chartered Professional Accountants of Canada (CPA Canada) is the national organization established to support a unified Canadian accounting profession. As one of the world's largest national accounting bodies, with more than 200,000 members across the country and around the world, CPA Canada carries a strong influential voice: it plays an important role in influencing international accounting, audit and assurance standards. CoCo was introduced in 1992 with the objective of improving organizational performance and decision-making with better controls, risk management, and corporate governance. In 1995, *Guidance on Control* was produced and described the CoCo framework and defining controls. The framework includes 20 criteria for effective control in four areas of an organization: purpose (direction), commitment (identity and values), capability (competence), monitoring and learning (evolution). This model describes internal control as actions that foster the best result for an organization. These actions, which contribute to the achievement of the organization's objectives, focus on: effectiveness and efficiency of operations; reliability of internal and external reporting; compliance with applicable laws and regulations and internal policies. CoCo indicates that control comprises: "Those elements of an organization (including its resources, systems, processes, culture, structure, and tasks) that, taken together, support people in the achievement of the organization's objectives."

Available: https://www.cpacanada.ca/

FRC (The Financial Reporting Council)

Reference published Guidance:

- *Guidance on Risk Management, Internal Control and Related Financial and Business Reporting (The Turnbull Guidance).* September, 2014

Highlights

The Financial Reporting Council is the UK's independent regulator responsible for promoting high quality corporate governance and reporting to foster investment. It promotes high standards of corporate governance through the UK Corporate Governance Code. It sets standards for corporate reporting, audit and actuarial practice and monitor and enforce accounting and auditing standards. The FRC issues guidance and other publications to assist boards and board committees in considering how to apply the UK Corporate Governance Code to their particular circumstances. These publications cover, among others: "Risk management, Internal Control and Related Financial and Business Reporting". This guidance revises, integrates and replaces the previous editions of the FRC's *Internal Control: Guidance to Directors* (formerly known as the *Turnbull Guidance*) and the *Going Concern and Liquidity Risk: Guidance for Directors of UK Companies* and reflects changes made to the UK Corporate Governance Code. It links the traditional *Turnbull* guidance on internal control with emerging good practice for risk management reflected in the conclusions of both the FRC's *Boards and Risk* report and the final recommendations of the *Sharman Panel of Inquiry into Going Concern and Liquidity Risk*. *Internal Control: Guidance for Directors on the Combined Code* (The *Turnbull guidance*) was first issued in 1999. In 2004, the Financial Reporting Council established the Turnbull Review Group to consider the impact of the guidance and the related disclosures and to determine whether the guidance needed to be updated. In reviewing the impact of the guidance, consultations revealed that it had very successfully gone a long way to meeting its original objectives. Boards and investors alike indicated that the guidance had contributed to a marked improvement in the overall standard of risk management and internal control since 1999. The second version was issued in 2005 (*Internal Control: Revised Guidance for Directors on the Combined Code*). Consistent with the amendments to any Principles in the 2014 edition of the Code and with the aim of aligning the terminology, a new version of the Guidance was issued in 2014.

Available:
https://www.frc.org.uk/Our-Work/Codes-Standards/Corporate-governance/UK-Corporate-Governance-Code/Guidance-for-boards-and-board-committees.aspx#biscuit3

GAO (U.S. Government Accountability Office)

Reference published Standard:

- *Standards for Internal Control in the Federal Government (The Green Book).* September, 2014

Highlights

The standards provide guidance on assessing risks and internal controls system for federal agencies in programmatic, financial, and compliance operations. On September 10, 2014 GAO issued its revision of *Standards for Internal Control in the Federal Government*. The 2014 revision will supersede GAO/AIMD-00-21.3.1, *Standards for Internal Control in the Federal Government* (November 1999). Federal Managers' Financial Integrity Act (FMFIA) requires that federal agency executives periodically review and annually report on the agency's internal control systems. FMFIA requires the Comptroller General to prescribe internal controls standards. These internal control standards, first issued in 1983, present the internal control standards for federal agencies for both program and financial management. *The Green Book* may also be adopted by state, local, and quasi-governmental entities, as well as not-for-profit organizations, as a framework for an internal control system. *Green Book* revisions involved an extensive, deliberative process, including public comments and input from the Green Book Advisory Council. GAO considered all comments and input in finalizing revisions to the standards. The standards in *The Green Book* are organized by the five components of internal control. Each of the five components contains several principles. Principles are the requirements of each component. Contol environment (5 principles); Risk assessment (4 principles); Control activiteis (3 principles); Information and communication (3 principles); Monitoring (2 principles).

Available:
www.gao.gov/greenbook/overview

Institute of Risk Management (IRM); Association of Insurance and Risk Managers (AIRMIC); Alarm (The Public Risk Management Association)

Reference published Standard:

- *A Risk Management Standard.* 2002

Highlights

The Risk Management Standard was originally published by the Institute of Risk Management (IRM), The Association of Insurance and Risk Manager (AIRMIC) and The Public Risk Management Association (Alarm) in 2002. It was subsequently adopted by the Federation of European Risk Management Association (FERMA). The Standard is the result of work by a team drawn from the major risk management organizations in the UK. In addition, the team sought the views and opinions of a wide range of other professional bodies with interests in risk management, during an extensive period of consultation. Despite the publication of ISO 31000, the Global Risk Management Standard, IRM has decided to retain its support for the original risk management standard because it is a simple guide that outlines a practical and systematic approach to the management of risk for business managers (rather than just risk professionals).

Available:
www.theirm.org/knowledge-and-resources/risk-management-standards/irms-risk-management-standard/

ISO (International Organization for Standardization)

- *ISO/IEC 27001:2005. Information technology -- Security techniques -- Information security management systems -- Requirements*
- *ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements*

Available:
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Technical Committee TC 262 - Risk management
Reference published Standards:

- *ISO Guide 73:2009. Risk management - Vocabulary*
- *ISO 31000:2009. Risk management - Principles and guidelines*
- *ISO/TR 31004:2013. Risk management - Guidance for the implementation of ISO 31000*
- *IEC 31010:2009. Risk management - Risk assessment techniques*

Available:
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=629121

Technical Committee TC 176/SC 1 - Concepts and terminology
Reference published Standard:

- *ISO 9000:2000. Quality management systems - Fundamentals and vocabulary*

Technical Committee TC 176/SC 2 - Quality systems
Reference published Standard:

- *ISO 9004.4:1993. Quality management and quality system elements - Part 4: Guidelines for quality improvement*

Available:
www.iso.org/iso/catalogue_detail?csnumber=29280
www.iso.org/iso/catalogue_detail.htm?csnumber=16544

Joint Technical Committee ISO/IEC JTC 1/SC 7 Software and systems engineering
Technical Committee ISO/TC 159/SC 4 Ergonomics of human-system interaction
Reference published Standards:

- *ISO/IEC 9126-1. Software Engineering - Product quality - Part 1: Quality model*
- *ISO 20282-1:2006. Ease of operation of everyday products - Part 1: Design requirements for context of use and user characteristics*
- *ISO/IEC TR 9126-4:2004. Software Engineering - Product quality - Part 4: Quality in use metrics*

- *ISO 9241-11. Part 11: Guidance on Usability*
- *ISO/IEC TR 9126-2. Software Engineering - Product quality - Part 2 External metrics*
- *ISO/IEC TR 9126-3. Software Engineering - Product quality - Part 3 Internal metrics*
- *ISO/IEC 18019:2004. Guidelines for the design and preparation of user documentation for application software*
- *ISO/IEC 15910:1999. Software user documentation process*
- *ISO 13407:1999. Human-centered design processes for interactive systems*
- *ISO/IEC 14598-1:1999. Software product evaluation*
- *ISO/TR 16982:2002. Usability methods supporting human-cantered design*

Available:

www.iso.org/iso/catalogue_detail.htm?csnumber=22749

www.iso.org/iso/catalogue_detail.htm?csnumber=34122

www.iso.org/iso/catalogue_detail.htm?csnumber=39752

www.iso.org/iso/catalogue_detail.htm?csnumber=16883

www.iso.org/iso/catalogue_detail.htm?csnumber=22750

www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=22891

www.iso.org/iso/catalogue_detail.htm?csnumber=30804

www.iso.org/iso/catalogue_detail.htm?csnumber=29509

www.iso.org/iso/catalogue_detail.htm?csnumber=21197

www.iso.org/iso/catalogue_detail.htm?csnumber=24902

www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31176

Highlights

ISO has developed more than 16,000 international standards for stakeholders such as industry and trade associations, science and academia, consumers and consumer associations, governments and regulators, and societal and other interest groups.

Specifically, as for the family of Standards developed and published under the direct responsibility of TC 262, the first editions of ISO 31000 and ISO Guide 73 were published in 2009. ISO 31000 has been adopted as a national standard by more than 50 national standards bodies covering over 70 % of the global population. It has also been adopted by a number of UN agencies and national governments as a basis for developing their own risk-related standards and policies. All the terms and definitions in ISO 31000 are contained in ISO Guide 73, so any changes to the terms and definitions in ISO 31000 must be identical in both documents. At this end, ISO 31000, and its accompanying Guide 73 on risk management terminology come up for revision every five years.

The family of Standards developed by TC 176 are particularly relevant to support organizations in the process mapping activity and has been used as a reference source for drawing up that section. Its scope is the standardization in the field of quality management (generic quality management systems and supporting technologies), as well as quality management standardization in specific sectors. ISO/TC 176 is also entrusted with an advisory function to all ISO and IEC technical committees to ensure the integrity of the generic quality system standards and the effective implementation of the ISO/IEC sector policy on quality management systems deliverables.

The family of Standards published under the direct responsibility of JTC 1/SC 7 and TC 159/SC 4 are particularly useful to support organizations in the design and implementation of the RM Information systems. JTC 1/SC7 has the following mandate from ISO and IEC: standardization of processes, supporting tools and supporting technologies for the engineering of software products and systems. As for the TC 159/SC 4, its scope is the standardization in the field of ergonomics, addressing human characteristics and performance.

OCEG

Reference published Standard:

- *The GRC Capability Model 3.0 (Red Book).* 2015

Highlights

OCEG is a global, nonprofit think tank and community. It informs, empowers, and helps advance more than 50,000 members on governance, risk management, and compliance (GRC). Its members include c-suite, executive, management, other professionals from small and midsize businesses, international corporations, nonprofits and government agencies. Founded in 2002, OCEG is headquartered in Scottsdale, AZ. The OCEG framework is centered on the GRC Capability Model (commonly known as the *Red Book*). It describes key elements of an effective GRC system that integrates the principle of "Good governance", "Risk management", "Compliance". The first *Red Book* was released in 2004: after months of analysis, collaboration, and vetting, the first OCEG standard emerges. Originally called the OCEG Capability Model, the cover was a deep red. It quickly became known as the OCEG *Red Book*. This standard provided both high-level and detailed practices that helped organizations address compliance and ethics issues. The standard gained wide adoption with over 100,000 downloads in a single year. Version 2.0 was published in 2009; version 2.1 was issued in 2012. The *Red Book* version 3.0 reflects 10 years of use and consideration by OCEG's global membership, which is now approaching 50,000 individuals worldwide. The Red Book Steering Committee attended several drafting and review sessions and prepared comments on each draft of the Red Book documents throughout the development process.

Available:

www.oceg.org/resources/red-book-3/

The British Standards Institution (BSI)

Reference published Guidance:

- *BS 31100:2011 Risk Management: Code of practice and guidance for the implementation of BS ISO 31000*. June, 2011

Highlights

Formed in 1901, BSI was the world's first National Standards Body. The BSI Kitemark was first registered by BSI on 12 June 1903. Originally known as the British Standard Mark, it has grown into one of Britain's most important and most recognized consumer quality marks. Through more than a century of growth, BSI now delivers a comprehensive business services portfolio to clients, helping them raise their performance and enhance their competitiveness worldwide. Based on the consensus of the UK committee of risk management experts, BS 31100 provides practical and specific recommendations on how to implement the key principles of effective risk management as specified in ISO 31000. According to British Standards Institute (BSI), "BS 31100 will provide a basis for understanding, developing, implementing and maintaining risk management within any organization, in order to enhance an organization's likelihood of successfully achieving its objectives". This British Standard establishes the principles and terminology for risk management, and gives recommendations for the model, framework, process and implementation of risk management. The recommendations of BS 31100 are generic and intended to be applicable and scalable to all organizations across the public and private sector, regardless of type, size and nature. How recommendations are implemented will depend on an organization's operating environment and complexity. BS 31100 is intended for use by anyone with responsibility for: ensuring that an organization manages to achieve its objectives; ensuring risks are managed in specific areas or activities; overseeing risk management in an organization; providing assurance on an organization's risk management". The first edition was issued in 2008: this version was replaced by the 2011 edition.

Available:
http://shop.bsigroup.com/ProductDetail/?pid=000000000030228064

The Institute of Directors in Southern Africa (IoDSA)

Reference published Models:

- *King Report on Corporate Governance (King III).* September, 2009
- *King Code of Governance Principles (King III).* September, 2009

Highlights

The Institute of Directors in Southern Africa (IoDSA) established in July 1993 the King Committee on Corporate Governance: it produced the first *King Report on Corporate Governance* which was published in 1994. The first *King Report* was recognized internationally, when published, as the most comprehensive publication on the subject embracing the inclusive approach to corporate governance. The *King Report on Corporate Governance for South Africa* – 2002 (*King II Report*) was launched at an Institute of Directors (IoDSA) Conference attended by 700 persons at the Sandton Convention Centre, 26 March 2002. The Institute of Directors in Southern Africa (IoDSA) formally introduced the *King Code of Governance Principles* and the *King Report on Governance (King III*) at the Sandton Convention Centre in Sandton, Johannesburg, in 2009. *King III* came into effect on 1 March 2010 – until then *King II* applied. The new *Code* and *Report* also falls in line with the Companies Act no 71 of 2008, which became effective on 1 May 2011. Like its 56 commonwealth peers, *King III* has been written in accordance to comply or explain principle based approach of governance, but specifically the apply or explain regime. This regime is currently unique in the Netherlands and now in South Africa. Whilst this approach remains a hotly debated issue globally, the *King III* Committee continues to believe it should be a non-legislative code on principles and practices.

Available:
https://iodsa.site-ym.com/store/ListProducts.aspx?catid=177819
https://jutalaw.co.za/uploads/King_III_Report/#p=1

UNECE High-Level Group for the Modernisation of Official Statistics (HLG-MOS)

Modernisation Committee on Standards

Reference released Models:

- *Generic Activity Model for Statistical Organizations (GAMSO), Version 1.0.* March, 2015
- *Generic Statistical Business Process Model (GSBPM), Version 5.0.* December, 2013

Highlights

The UNECE High-Level Group for the Modernisation of Official Statistics (HLG-MOS) was set up by the Bureau of the Conference of European Statisticians in 2010 to oversee and coordinate international work relating to statistical modernisation. It promotes standards-based modernisation of statistical production and services. It reports directly to the Conference of European Statisticians and received its mandate from this body. The mission of the HLG-MOS is to oversee development of frameworks, and sharing of information, tools and methods, which support the modernisation of statistical organizations. The aim is to improve the efficiency of the statistical production process, and the ability to produce outputs that better meet user needs.

The Joint UNECE / Eurostat / OECD Work Sessions on Statistical Metadata (METIS) have prepared a Common Metadata Framework (CMF). Part C of this framework is entitled "Metadata and the Statistical Cycle". This part refers to the phases of the statistical business process and provides generic terms to describe them. Since November 2013, this work has been taken over by the *Modernisation Committee on Standards*, under the HLG-MOS. During a workshop on the development of Part C of the CMF, held in Vienna in July 2007, the participants agreed that the business process model used by Statistics New Zealand would provide a good basis for developing a Generic Statistical Business Process Model. Following several drafts and public consultations, version 4.0 of the GSBPM was released in April 2009. It was subsequently widely adopted by the global official statistics community, and formed one of the cornerstones of the HLG vision and strategy for standards-based modernisation. In December 2012, a complementary model, the Generic Statistical Information Model (GSIM) was released. The work to develop and subsequently implement the GSIM resulted in the identification of several possible enhancements to the GSBPM. During 2013, the HLG launched a project on "Frameworks and Standards for Statistical Modernisation" which included a broader review of the GSBPM and the GSIM, to improve consistency between the documentation of the models, and to incorporate feedback based on practical implementations. The current version of the GSBPM (version 5.0) is the direct result of this work. Whilst it is considered final at the time of release, it is also expected that future updates may be necessary in the coming years, either to reflect further experiences from implementing the model in practice, or due to the evolution of the nature of statistical production.

The *Generic Activity Model for Statistical Organizations* (GAMSO) Version 1.0 was endorsed for release by the HLG-MOS on 1 March 2015. Statistical organizations are invited to use GAMSO and provide feedback based on practical implementations on the GAMSO Review. GAMSO will be reviewed in 2016 taking into account this feedback. GAMSO describes and defines the activities that take place within a typical statistical organization. It extends and complements the GSBPM by adding additional activities needed to support statistical production. When the GSBPM was developed, such activities were referred to as over-arching processes, and were listed, but not elaborated in any great detail. Over the years there have been several calls to expand the GSBPM to better cover these activities. The GAMSO was therefore developed to meet these needs.

Available:

http://www1.unece.org/stat/platform/display/GAMSO/GAMSO+v1.0

http://www1.unece.org/stat/platform/display/metis/The+Generic+Statistical+Business+Process+Model

UK HM Treasury - Government Financial Management Directorate

Reference published Guidance:

- *The Orange Book Management of Risk - Principles and Concepts*. October, 2004

Highlights

In central government a number of reports, particularly the National Audit Office's 2000 report "Supporting innovation – managing risk in government departments" and the Strategy Unit 2002 report "Risk – improving government's capacity to handle risk and uncertainty", have driven forward the risk management agenda and the development of Statements on Internal Control. In 2001 Treasury produced "Management of Risk – A Strategic Overview" which rapidly became known as the *Orange Book*: it provided a basic introduction to the concepts of risk management that proved very popular as a resource for developing and implementing risk management processes in government organizations. This Guidance is the successor to the 2001 *Orange Book*. It continues to provide broad based general guidance on the principles of risk management, but has been enhanced to reflect the lessons learned about risk management through the experience. The most significant shift since the publication of the 2001 is that all government organizations had, in 2004, basic risk management processes in place. This means that the main risk management challenge did not lie in the initial identification and analysis of risk and the development of the risk management process, but rather in the ongoing review and improvement of risk management. It focuses on both internal processes for risk management and consideration of the organization's risk management in relation to the wider environment in which it functions.

Available:

https://www.gov.uk/government/publications/orange-book

Academic sources, institutional papers and professional handbooks:

Aabo, T., Fraser, J., & Simkins, B. J. (2005). The rise and evolution of the chief risk officer: Enterprise risk management at hydro one. *Journal of Applied Corporate Finance*, 17(3), 62–75.

Alarm, The Public Risk Management Association – UK (2010). *The National performance Model for Risk Management in the Public Services.*

Ariff, M. S. M., Zakuan, N., Tajudin, M. N. M., & Ismail, K. (2015). A conceptual model of Risk Management Practices and organizational performance for Malaysia's Research Universities. *The Role of Service in the Tourism & Hospitality Industry*, 153.

Australian Government, (2013). *Comcover Risk management Maturity Model*

Bodein, S., Pugliese, A. & Walker, P. A road map to risk management. *Journal of Accountancy*, December 2001, Volume 192, Issue 6, pp 65-70.

Bruce, R. (2005). Swift message on risk management. *Accountancy* (April), 22.

Bruno-Britz, M. (2009). The age of ERM. *Bank Systems & Technology*, 1 (February), 20.

Burton, E. J. (2008). The audit committee: How should it handle ERM? *The Journal of Corporate Accounting & Finance*, 19(4), 3–5.

Chenhall, R. H., & Euske, K. J. (2007). The role of management control systems in planned organizational change: An analysis of two organizations. *Accounting, Organizations and Society*, 32, 601–637.

Chua, W. F. (2007). Accounting, measuring, reporting and strategizing – Re-using verbs: A review essay. *Accounting, Organizations and Society*, 32(4–5), 487–494.

CMMI Product Team (2002). *Capability Maturity Model Integration (CMMI)*, Software Engineering Institute (SEI).

Curtis, E., & Turley, S. (2007). The business risk audit – A longitudinal case study of an audit engagement. *Accounting, Organizations and Society*, 32, 439–461.

Drennan, L. T., McConnell, A., & Stark, A. (2014). *Risk and crisis management in the public sector*. Routledge.

Epstein, M.J., & Rejc, A. (2006). *The reporting of organisational risks for internal and external decision makers*, Management Accounting Guideline, Canada: The Society of Management Accountants of Canada (CMA-Canada)

European Statistical System Committee (ESSC) - Vision Implementation Group & Vision Implementation Network (2015). *Identification and Evaluation of Risks to ESS Vision 2020 Implementation*.

Fraser, I., & Henry, W. (2007). Embedding risk management: Structures and approaches. *Managerial Auditing Journal*, 22(4), 392–409.

Gates, S. (2006). Incorporating strategic risk into enterprise risk management: A survey of current corporate practice. *Journal of Applied Corporate Finance*, 18(4), 81–90.

Gephart, R. P., Van Maanen, J., & Oberlechner, T. (2009). Organizations and risk in late modernity. *Organization Studies*, 30(02&03), 141–155.

Government Centre for information Systems (1993) *Introduction to the Management of Risk.* HMSO, Norwich.

Greenwood, R., & Hinings, C. R. (1993). Understanding strategic change: The contribution of archetypes. *The Academy of Management Journal*, 36(5), 1052–1081.

Griffioen, R., van Delden, A., & de Wolf, P.P. (2012). BLUE-Enterprise and Trade Statistics- SP1-Cooperation-Collaborative Project Small or medium-scale focused research project FP7-SSH-2009-A Grant Agreement Number 244767 SSH-CT-2010-244767. *Deliverable 7.3*.

Hillson, D. A. (1997) '*Towards a Risk Maturity Model*'. The International Journal of Project & Business Risk Management, Vol.1

Holton, G. A. (2003). *Value-at-risk: Theory and practice*. San Diego, CA: Academic Press.

Hopkin, P. (2014). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.

Hopkinson, M. (2000) *Risk Maturity Models in practice*. Risk Management Bulletin, 5.

Hutter, B. M., & Power, M. (2005). *Organizational encounters with risk*. Cambridge University.

IACCM – The International Association for Contract & Commercial Management (2002), *Business Risk Management Maturity Model (BRM),* Business Risk Management Working Group.

IIRM (Investors in Risk Management), (2015). *Risk Management Maturity Model (RMMM)*.

IMA – Institute of Management Accountants (2006). *Enterprise risk management: Frameworks, elements, and integration, statements on management accounting*.

Jaafari, A. (2001). Management of risks, uncertainties and opportunities on projects: Time for a fundamental shift. *International Journal of Project Management*, 19(2), 89–101.

Lam, J. (2003). *Enterprise risk management: From incentives to controls*, Hoboken. New Jersey: Wiley.

Lam, J. (2006). *Emerging best practices in developing key risk indicators and ERM reporting*. James Lam & Associates, Inc..

Lampel, J., Shamsie, J., & Shapira, Z. (2009). Rare events and organizational learning. *Organization Science*, 20(5), 835–845.

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, 6(1), 37–52.

Martin, D., & Power, M. (2007). *The end of enterprise risk management*. Aeibrookings Joint Center for Regulatory Studies, August.

MC Connell, P. (2012). *Operational Risk Management Maturity Model (ORMMM)*

Mikes, A. (2005). Enterprise risk management in action. *Centre for the analysis of risk and regulation (CARR) discussion paper report series no. 35*.

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, 20(1), 18–40.

Miller, K. D. (1998). Economic exposure and integrated risk management. *Strategic Management Journal*, 19(5), 497–514.

Miller, K. D. (2009). Organizational risk after modernism. *Organization Studies*, 30(2/3), 157–180.

Miller, P., Kurunmaki, L., & O'Leary, T. (2008). Accounting, hybrids and the management of risk. *Accounting, Organizations and Society*, 33(7–8), 942–967.

Orsini, B. (August 2002) *Mature Risk Management Diagnostic Tool,* The Internal Auditor.

Page, M., & Spira, L. F. (2004). *The turnbull report, internal control and risk management: The developing role of internal audit*. Institute of Chartered Accountants: Scotland.

PMI Risk Significant Interest Group (2002), *Risk Management Maturity Model (RMMM)*, RiskSIG.

Porter, M. E. (1990). The Competitive Advantage of Nations. *Harvard Business Review 68*, no. 2 (March–April 1990): 73–93.

Power, M. (2004). *The risk management of everything*. London: Demos.

Power, M. (2007). *Organized uncertainty designing a world of risk management*. Oxford University Press.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, 34(6–7), 849–855.

Power, M., Scheytt, T., Soin, K., & Sahlin, K. (2009). Reputational risk as a logic of organizing in late modernity. *Organization Studies*, 30(2–3), 301–324.

Price, T. (2008). Uncovering unknown risk. *Wall Street & Technology*, 1 (December), 36.

PricewaterhouseCoopers (2004). Managing risk: An assessment of CEO perspectives. New York: PwC.

Pritchard, C.L. et al. (2014). *Risk management: concepts and guidance*. CRC Press.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, 27(2/3), 183–213.

Rieger, L. (2005). Success factors for implementing enterprise risk management. *Bank Accounting and Finance*, 18(3), 21–26.

Risk and Insurance Management Society and LogicManager (2008). *Risk Maturity Model for Enterprise Risk Management* (RIMS).

Rittenberg, L., & Covaleski, M. A. (2001). Internalization versus externalization of the internal audit function: An examination of professional and organizational imperatives. *Accounting, Organizations & Society*, 26(7–8), 617–641.

Sarma, M., Thomas, S., & Shah, A. (2003). Selection of value-at-risk models. *Journal of Forecasting*, 22(4), 337–358.

Scapens, B., & Bromwich, M. (2009). Editorial: Risk management, corporate governance and management accounting. *Management Accounting Research*, 20(1), 1.

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing and Accountability Journal*, 16(4), 640–661.

Statistics Netherlands. van Nederpelt, P.W.M. (2010). *A new model for quality management*. The Hague/Heerlen.

UK HM Treasury - Government Financial Management Directorate, (2009). *Risk Management assessment framework: a tool for departments*.

Taleb, N. N. (2007). The Black Swan: The impact of the highly improbable. Random House.

The Institute of Internal Audit, (2010). *Risk management Maturity Model*

Walker, P. L., Shenkir, W. G., & Barton, T. L. (2003). ERM in practice. *Internal Auditor*, 60(4), 51–55.

Walker, P., Shenkir, W., & Barton, T. (2002). *Enterprise risk management: Pulling it all together*. Altamonte Springs: Institute of Internal Auditors Research Foundation.

M Wheatley, (2007) *"Maturity Matters"*, PM Network.

Widener, S. K. (2007). An empirical analysis of the levers of control framework. *Accounting, Organizations, and Society*, 32(7–8), 757–788.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research*, 20(1), 69–81.

Zolkos, R. (2008). Financial crisis shows real need for ERM. *Business Insurance*, 6(October), 6.

Glossary

Acceptable risk III
Communication and consultation III
Control III
Enterprise-wide risk management (ERM) III
Establishing the context III
Event IV
External context IV
Identified risk IV
Inherent risk IV
Internal context IV
Impact V
Level of risk V
Likelihood V
Monitoring V
Residual risk V
Risk V
Risk analysis VI
Risk appetite VI
Risk assessment VI
Risk attitude VI
Risk aversion VI
Risk criteria VI
Risk exposure VI
Risk identification VII
Risk management VII
Risk management framework VII
Risk management plan VII
Risk management policy VII
Risk management process VII

Risk map VIII
Risk maturity VIII
Risk measurement VIII
Risk owner VIII
Risk profile VIII
Risk register/risk log VIII
Risk source VIII
Risk Strategy VIII
Risk tolerance IX
Risk treatment IX
Risk weighting IX
Review IX
Stakeholder X
Total risk X
Unacceptable risk X
Unidentified risk X

Acceptable risk

the part of identified risk that is allowed to persist after controls are applied. Risk can be determined acceptable when there is slack of money or when further efforts to reduce it would cause degradation of the probability of success of the operation, or when a point of diminishing returns has been reached.

Communication and consultation

continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with **stakeholders** and others regarding the management of **risk**. The information can relate to the existence, nature, form, **likelihood**, severity, evaluation, acceptability, treatment or other aspects of the management of risk. Consultation is a two-way process of informed communication between an organization and its stakeholders or others on an issue prior to making a decision or determining a direction on a particular issue. Consultation is:

- a process which impacts on a decision through influence rather than power; and
- an input to decision making, not joint decision making

Control

any action taken by management, the board, and other parties to manage **risk** and increase the likelihood that established objectives and goals will be achieved. These actions may be taken to manage either the impact if the risk is realised, or the frequency of the realization of the risk. Controls include any plan, process, policy, device, practice, or other actions which modify risk, and organize and direct the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. Controls may not always exert the intended or assumed modifying effect. Risk treatments become controls, or modify existing controls, once they have been implemented.

Enterprise-wide risk management (ERM)

a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.

Establishing the context

defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** for the **risk management policy.**

Event

occurrence or change of a particular set of circumstances. An event can be one or more occurrences, and can have several causes. An event can consist of something not happening. An event can sometimes be referred to as an "incident" or "accident".

External context

external environment in which the organization seeks to achieve its objectives. External context can include:

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the organization; and
- relationships with, and perceptions and values of, external **stakeholders** .

Identified risk

that risk that has been determined to exist using analytical tools. The time and costs of analysis efforts, the quality of the risk management program, and the state of the technology involved affect the amount of risk that can be identified.

Inherent risk

the risk to an entity in the absence of any actions management might take to alter the risk's likelihood or impact. These risks may result from an entity's industry, strategy, and environmental factors.

Internal context

internal environment in which the organization seeks to achieve its objectives. Internal context can include:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- perceptions and values of internal stakeholders;
- information systems, information flows and decision-making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
- the organization's culture, the integrity, ethical values;
- standards, guidelines and models adopted by the organization;

- form and extent of contractual relationships.

Impact

represents the potential effects and consequences that a given **event** could have on an entity and its objectives. An event can lead to a range of consequences. A consequence can be certain or uncertain and can have positive or negative effects on objectives. Events that have positive effects represent opportunities and those with negative effects represent risks. Consequences can be expressed qualitatively or quantitatively. Entities often describe events based on severity, effects, or monetary amounts. Initial consequences can escalate through knock-on effects.

Level of risk

magnitude of a **risk**, expressed in terms of the combination of **consequences** and their **likelihood**.

Likelihood

the possibility that an event may occur. It can be defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and it can be described using qualitative terms (such as high, medium, and low) or quantitative measures (such as a percentage and frequency).

Monitoring

continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected. Monitoring can be applied to a **risk management framework**, **risk management process**, **risk** or **control**.

Residual risk

the portion of total **risk** remaining after **risk treatment** has been applied. Residual risk comprises **acceptable risk** and **unidentified risk**. Management must decide whether this residual risk is within the entity's risk appetite. Residual risk is also known as "retained risk".

Risk

the possibility of an event occurring that will have an effect on the achievement of objectives. An effect is a deviation from the expected (positive and/or negative). Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). All activities of an organization involve risk. Organizations manage risk by

identifying it, analysing it and then evaluating whether the risk should be modified by risk treatment in order to satisfy their risk criteria. Risk is often characterized by reference to potential **events** and **impact**, or a combination of these. Risk is measured in terms of impact (including changes in circumstances) and **likelihood** of occurrence. Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequences, or likelihood.

Risk analysis

process to comprehend the nature of **risk** and to determine the **level of risk**. Risk analysis provides the basis for **risk evaluation** and decisions about **risk treatment**. Risk analysis includes risk estimation.

Risk appetite

amount and type of **risk** that an organization is willing and prepared to accept as it tries to achieve its goal and provide value to stakeholders. Risk appetite is a higher level statement that considers broadly the levels of risks that management deems acceptable. It reflects the enterprise's risk management philosophy, and in turn influences the entity's culture and operating style. Many entities define their risk appetite qualitative, while other take a more quantitative approach.

Risk assessment

overall process of **risk identification**, **risk analysis, risk measurement** and **risk weighting.**

Risk attitude

organization's approach to assess and eventually pursue, retain, take or turn away from **risk.**

Risk aversion

attitude to turn away from **risk.**

Risk criteria

terms of reference against which the significance of a **risk** is evaluated. Risk criteria are based on organizational objectives, and **external** and **internal context**. Risk criteria can be derived from standards, laws, policies and other requirements.

Risk exposure

the consequences, as a combination of impact and likelihood, which may be experienced by an organization if a specific risk is realized.

Risk identification

process of finding, recognizing and describing **risks**. Risk identification involves the identification of **risk sources**, **events**, their causes and their potential **consequences**. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder**'s needs.

Risk management

coordinated activities to direct and control an organization with regards to **risk.**

Risk management framework

the totality of the structures, methodology, procedures and definitions that an organization has chosen for designing, implementing, **monitoring**, reviewing and continually improving **risk management** throughout the organization. The foundations include the policy, objectives, mandate and commitment to manage **risk**. The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities. The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

Risk management plan

scheme within the **risk management framework** specifying the approach, the management components and resources to be applied to the management of **risk**. Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.

Risk management policy

statement of the overall intentions and direction of an organization related to **risk management.**

Risk management process

systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** and reviewing **risk** in order to provide reasonable assurance regarding the achievement of the organization's objectives.

Risk map

a graphic representation of likelihood and impact of one or more risks. Risk maps may plot quantitative or qualitative estimates of risk likelihood and impact. Often, risk maps are referred to as "**heat maps**" since they present risk levels by color, where red represents high risk, yellow moderate risk, and green low risk.

Risk maturity

measuring the level of development of risk management practices within an organization, based on different variables and / or dimensions characterized by organizational behaviors and indicators.

Risk measurement

assigning values to each risk using the defined criteria. Most organizations define scales for rating risks in terms of impact, likelihood, and other dimensions.

Risk owner

person or entity with the accountability and authority to manage the **risk.**

Risk profile

description of any set of **risks**. The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.

Risk register/risk log

a master document that records identified risks, their severity, and the responses to be taken.

Risk source

element which alone or in combination has the intrinsic potential to give rise to **risk**. A risk source can be tangible or intangible.

Risk Strategy

the overall organizational approach to risk management as defined by the entity governing risk management. This should be documented and easily available throughout the organization.

Risk tolerance

the acceptable level of variation relative to achievement of a specific objective. This variation is often measured using the same units as its related objective. In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with **risk appetite**. Therefore, an entity operating with its risk tolerances, narrow boundaries, is operating within its risk appetite, wide boundaries.

Risk treatment

means by which an organization elects to manage individual risks. Risk treatments can also be called risk responses. As part of enterprise risk management, for each significant risk an entity considers potential responses from a range of response categories. Risk treatment can involve:

- **Avoidance/Terminating** is a response where you exit the activities that cause the risk. Some examples of avoidance are exiting product line, selling a division, or deciding against expansion.
- **Treating/Reduction** is a response where action is taken to mitigate the risk likelihood and impact, or both.
- **Transferring/Sharing** is a response that reduces the risk likelihood and impact by sharing or transferring a portion of the risk. An extremely common sharing response is insurance.
- **Tolerance/Acceptance** is a response where no action is taken to affect the risk likelihood or impact.
- Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". Risk treatment can create new risks or modify existing risks.

Risk weighting

process of comparing the results of **risk analysis** with **risk criteria** to determine whether the **risk** and/or its magnitude is acceptable or tolerable. It's the process of determining risk management priorities by comparing the level of risk against predetermined target risk levels and tolerance thresholds. Risk evaluation assists in the decision about **risk treatment.**

Review

activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Review can be applied to a **risk management framework**, **risk management process**, **risk** or **control**.

Stakeholder

person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity. A decision maker can be a stakeholder.

Total risk

the sum of identified and unidentified risk. Ideally, identified risk will comprise the larger proportion of the two.

Unacceptable risk

the portion of identified risk that cannot be tolerated, but must be either eliminated or controlled.

Unidentified risk

that risk that has not yet been identified. Some risk is not identifiable or measurable. Mishap investigations may reveal some previously unidentified risks.