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 highlighted:

- "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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Risk management Area</th>
<th>Organizational process management Area</th>
<th>Internal Audit/Control Area</th>
<th>Statistical Production process management Area</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Successful</strong></td>
<td>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</td>
<td>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</td>
<td>a) Senior Management/Top Management Commitment</td>
<td>a) Senior Management/Top Management Commitment b) Integrate risk management to planning, operations and decision making processes</td>
</tr>
<tr>
<td><strong>Difficult</strong></td>
<td>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</td>
<td>a) Maintaining the focus of Senior Management on risk management expectations</td>
<td>a) Promoting the implementation of a risk management system without a regulatory framework to support audit observations and recommendations</td>
<td>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</td>
</tr>
<tr>
<td><strong>Not to do</strong></td>
<td>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</td>
<td>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</td>
<td>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</td>
<td></td>
</tr>
</tbody>
</table>
### Cluster 1: Mandate & Risk Policy

<table>
<thead>
<tr>
<th>Item</th>
<th>Plus &amp; Minus</th>
<th>Risk Management Area</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mandate and commitment to manage risks</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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 overseeing 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

<table>
<thead>
<tr>
<th>Item</th>
<th>Plus &amp; Minus</th>
<th>Organizational process management Area</th>
<th>Statistical Production process management Area</th>
<th>Statistical Quality analysis Area</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk management Procedure</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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 maintaining sufficient flexibility for people to adapt 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 | |
<table>
<thead>
<tr>
<th>Item</th>
<th>Plus &amp; Minus</th>
<th>Organizational process management Area</th>
<th>Statistical Production process management Area</th>
<th>Statistical Quality analysis Area</th>
</tr>
</thead>
</table>
| **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/artifacts 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 |
| **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 AGIS and coordinating strategic risk management at the organizational level (the team offers support and advice on risk management rather than undertaking risk management activities)  
 c) Establishing a risk management committee which coordinates the RM team  
 d) RM unit reporting directly to the DG Finance and DG Statistics | a) Enabling adequate independence between internal audit and risk management functions  
 b) Managing a large risk management work program, with each RM team in which expertise is concentrated in a few key staff members  
 c) Overseeing cross-agency risks with a devolved risk management approach | 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 |
| **Risk Identification phase** | 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 | a) Clear guidance to apply the methodology  
 b) Aligning risk management cycle to field planning cycle  
 c) Use a framework that considers 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) Identifying emerging risks or planning for unanticipated risks  
 b) Not having a clear risk identification process and sticking to it for a few years  
 c) Brainstorm risk identification without necessary stakeholders in the discussion |
## CLUSTER 3 – RISK MANAGEMENT PROCESS

<table>
<thead>
<tr>
<th>Item</th>
<th>Plus &amp; Minus</th>
<th>Organizational process management Area</th>
<th>Statistical Production process management Area</th>
<th>Statistical Quality analysis Area</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Assessment phase</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 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 quantity, 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. |
| **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 adapting 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 affect multiple risks or required coordination among 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**

<table>
<thead>
<tr>
<th>Item</th>
<th>Plus &amp; Minus</th>
<th>Risk Management Area</th>
</tr>
</thead>
</table>
| 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, transformation, statistical, 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**

<table>
<thead>
<tr>
<th>Item</th>
<th>Plus &amp; Minus</th>
<th>Statistical Quality Analysis Area</th>
</tr>
</thead>
</table>
| 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**

<table>
<thead>
<tr>
<th>Item</th>
<th>Plus &amp; Minus</th>
<th>Statistical Quality Analysis Area</th>
</tr>
</thead>
</table>
| 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 gate 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**

<table>
<thead>
<tr>
<th>Item</th>
<th>Plus &amp; Minus</th>
<th>Internal Audit/Control Area</th>
</tr>
</thead>
</table>
| 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 delineation 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 based 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

<table>
<thead>
<tr>
<th>Item</th>
<th>Plus &amp; Minus</th>
<th>Services Supporting Statistical Production Area</th>
</tr>
</thead>
</table>
| 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 |
| 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 organisation 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 |
| 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, strategic 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 |