Risk Management in Statistics Austria


UNECE-Workshop on Risk Management Practices in Statistical Organisations
Content

- Introduction, background

- Risk Management System in Statistics Austria
  - Institutional setup, Governance

- Tool and methods used: OBSERVAR©

- Current practices
  - Risk Identification - Risk Assessment
  - Risk Mitigation – Monitoring - Reporting

- Summary: Lessons learned, future plans
Introduction, background (1)

- **Statistics Austria**
  - separated from public administration since January 2000

---

**Statistics Council**
- Work programme Committee
- Quality Committee

**Economic Council**
- Audit Committee
- Calculation Committee

= Supervisory Board

15 Technical Sub-Committees
Introduction, background (2)

- **Legal obligations** for Statistics Austria concerning Risk Management (RM) and Internal Control System (ICS)
  - Article 67 (1) lit. 2, Federal Budget Act 2013: Risk Controlling (RM)

- Statistics Austria has to comply with the **Federal-Public Corporate Governance Code** (RM incl.)

- Recommendation of the **Austrian Court of Auditors** to Statistics Austria for implementation of RM and ICS

- **Self-commitment** (ESS and national requirements, compliance, quality etc.)

*) Annual financial statements, management report (incl. reporting on RM and ICS)
Risk Management System – Institutional setup, Governance (1)

Director General - Statistics
Konrad Pesendorfer

Director General - Finance
Gabriela Petrovic

Risk Management
Werner Holzer

since 2011
Risk Management System – Institutional setup, Governance (2)

**Tasks** of the Risk Manager in Statistics Austria:

- **Risk Management (RM)**
  - corporation-wide (strategic level)
  - for specific statistical projects/processes

- **Internal Control System (ICS)**
  - operational processes

- **Compliance Management System (CMS)**

- **Implementation of Strategy 2020**
  (Statistics Austria, ESS Vision 2020 (VIN))
  - Risk Identification
  - Risk Assessment
  - Risk Mitigation
  - Monitoring, Audits
  - Reporting

- **Horizontal projects, analyses and optimisation of processes**
Risk Management System –
Institutional setup, Governance (3)

Management (DG)
- responsible for ensuring an appropriate risk management

Risk owners
- have overall responsibility for specific risk areas
- responsible for risk mitigation actions, reporting

Risk Management cooperation
- RM: Supplement to the existing management and supporting system for the top management
- close cooperation of RM, QM Unit (Quality Audits), Internal Audit Unit, Controlling Unit, Data Protection Officer, IT Security Officer etc.
- Specialised, 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
- integrates the criteria of relevant standards and frameworks:

---

ISO 31000 ERM

- Mandate and commitment (E.3)
- Design of framework for managing risk (E.2)
- Continual improvement of the framework (E.4)
- Process (Clause 5)
- Monitoring and review of the framework (E.4)

COSO II ERM & Internal Control

- Identification of internal and external issues (II.A.1)
- Identification of interested parties requirements (II.A.2)
- Establishing compliance policy (II.A.2)

ISO 19600 (Compliance Management)

- Leadership commitment independent evaluation (III.6)
- Responsibilities at all levels (III.1)
- Support functions (III.7)
Milestones 2009-2016

- 2009: First assessment of strategic and operational risks with OBSERVAR
- 2010: Evaluation of other software products
- Nov. 2010: First risk workshop with the new web-based Version of OBSERVAR
- 2011: Implementation of 4 Modules (Qualitative Risk Assessment, Quantitative Risk Assessment, Process Module, Project Module)
- 2014: Compliance-Module added
- 2011-April 2016: 5 Risk workshops, ongoing risk controlling
Tool and methods used: OBSERVAR© (3)

Main screen

Select one module from the menu and the language to be displayed

If you encounter problems with the display on your screen - please refresh the page with F5. This can happen after updates if the browser has old settings in the cache. (click on F5)

Managing all relevant basic settings, reference data for all modules and description of the company / users / catalogues etc.

Master

IKS-ZD, IT-Abt.
Risikomanagement (EROM)
IKS-Fachstatistik (Dir./Abt.REG)
Compliance / Statements

Process Modules
Reporting and documenting the accomplishment of process steps / periodic controls. Requesting modifications for improvement.

Project Modules
Reporting and documenting the progress of Projects / degree of conversion of new measures. Requesting modifications for improvement.

Analysis of the users reports / accomplished messages and the non-compliances. Managing with modification suggestions. Documentation of functional and design audits.

Analysis of the Project status reports and the non-compliances. Managing with modification suggestions. Documentation of Project audits.

Analysis of the qualitative assessment. Prioritization of the Top Opportunities and Top Risks on the basis of configurable Key Figures.

Analysis of the qualitative valuations and generation of reports. Moderation of transparent workshops with key employees - to pin point potentials for better achievement of the objectives.

EROM Preparation

EROM Assessment

Qualitative Assessments
Completion of questionnaire for qualitative assessment of Opportunities and Risks. Posting comments regarding potential impacts on objectives / targets.

Quantitative Valuations
Assessing quantitative valuations of potential impacts on objectives / targets (Quantification of Risks and Opportunities). Register existing Processes and define new Projects.

Different roles
Current practices - Risk Identification (1)

- Risk identification and risk assessment are carried out in workshops with external assistance (Co. OBSERVAR)
  - RM: corporation-wide risks (strategic level) – biennially
  - ICS: risk in operational processes – biennially
  - CMS: compliance risks – lower frequency

- by the management team (risk owners):
  DG Finance, DG Statistics, Directors, Heads of Departments, Risk Manager, Quality Manager, Heads of Units of the Central Services; Internal Audit as observer - (20-25 persons)

- using the tool OBSERVAR© including tailor-made risk catalogues and questionnaire forms
Current practices - Risk Identification (2)

Prioritisation approach, focus only on important items

- **External**
  - **Risks** - corporation-wide risks (strategic level)
  
  - Risk mitigation actions
    - ongoing processes
    - internal rules, guidelines
    - projects

- **Internal**
  - **RM**
  - **Risks** - in operational processes
  
  - Risk mitigation actions
    - ongoing processes
    - internal rules, guidelines
    - projects

- **ICS**
  - **Risks** - in operational processes
  
  - Risk mitigation actions
    - ongoing processes
    - internal rules, guidelines
    - projects

- **Procurement**
- **Statistical Production**
- **Accounting**
- **Etc.**
Risk catalogues

Customized risk catalogues for
- RM: corporation-wide risks (strategic level)
- ICS: risk in operational processes
- CMS: compliance risks
Risk catalogues (details, examples)

Risk Management - Catalogue (October 2015)

Key | Risk areas | Key terms
--- | --- | ---
A  | Leadership Processes |  
 a  | Strategy |  
 01 | Strategy development | Strategy finding process, consistency of sub-strategies, consideration of all relevant success factors, inclusion of all relevant stakeholders, consideration of all relevant and legal requirements and developments  
 02 | Strategy implementation | Operational targets, implementation controlling, coordination of resources, communication of the strategic targets  
 b  | HR |  
 02 | Key employees | Dependence on key employees, fluctuations, deputy regulations, succession planning, deputy regulations, training  
 04 | HR qualifications, education and training | Employee qualification, employee education & training, training of apprentices, change management, HR cost  
 c  | IT, Data protection |  
 04 | Data protection (confidentiality, integrity, availability) | Protection of data, statistical confidentiality, data privacy policy and guidelines, data security, measures against technical loss, archiving, e-mails, backup, hacker/cracker  
 d  | Information und Kommunikation |  
 05 | Knowledge management | Collecting knowledge, administration of knowledge, use of existing knowledge, dependency on single persons, availability of knowledge, institutionalised knowledge
Current practices - Risk Identification (5)

Risk catalogues – Compliance topics

- Corporate Governance
  - Data protection, statistical confidentiality, data security
  - Statistical Production
    - incl. Quality, Dissemination
  - IT
    - incl. IT-Security, E-Mail, Web usage etc.
  - Security (in general)
    - incl. safety at work
- Anti-Corruption, fraud/money laundering prevention
- Tax compliance, fees (as applicable)
- Procurement, supplier management
- labour law, staff
- Environment protection
Current practices - Risk Identification (6)

Risk Identification | Risk Assessment | Risk Mitigation | Monitoring | Reporting

**Module** RM: Identification of areas with **high residual risks**

- Analysis of the qualitative assessment. Prioritization of the Top Opportunities and Top Risks on the basis of configurable Key Figures.

**EROM Preparation**

- Individually customisable questionnaires for qualitative judgement/prioritisation of important topics
Current practices - Risk Identification (7)

Results (scoring, indicators), agreement on TOP 10 areas with high residual risks (RM)

Customisable key figures (with individual settings of scoring points for selected questions) - resulting in a ranking of risk areas in a mid-term view and a long-term perspective
Current practices - Risk Assessment (1)

Quantitative assessment of TOP 10 risks

Opportunity = over-achievement of planned amounts

Risk = under-achievement of planned amounts

Identification and Valuation of major Opportunities. Are there possible additional measures to seize the Opportunities?

Identification and Valuation of major Residual Risks. Is this acceptable or is improvement needed?

Identification and Valuation of major Riskpotentials. Are existing actions really appropriate to reduce the Riskpotential to the Worst Case as quantified?
Current practices - Risk Assessment (2)

Risk Identification  | Risk Assessment  | Risk Mitigation  | Monitoring  | Reporting

Module

Quantitative assessment of TOP 10 risks

EROM Assessment

Analyseren Sie die Geldbewertungen und erstellen Sie Berichte. Moderieren Sie transparente Workshops mit Know-How Trägern - und finden Sie die vorhandenen Optimierungsmöglichkeiten.

Quantitative Bewertung

Erfassen Sie Geldbewertungen der möglichen Auswirkungen von Chancen und Risiken auf die Zielsetzungen. Erfassen Sie Prozess Massnahmen und Aktionspläne.

Current practices - Risk Assessment (3)

Risk Identification
Risk Assessment
Risk Mitigation
Monitoring
Reporting

Quantitative assessment: Results, automatically generated reports, examples)
Current practices - Risk Assessment (4)

Risk Identification
Risk Assessment
Risk Mitigation
Monitoring
Reporting

Other example screens of automatically generated reports: Assessment module (quantification)

On the left side:
Example of a corridor graph showing the uncertainty of quantified risk values (the higher the bar – the higher is the unpredictability of the risk amount)
Current practices - Risk Mitigation (1)

- **Processes** (including internal rules, guidelines) and
- **Projects**

for risk mitigation are defined and monitored on a regular basis with the IT-Tool OBSERVAR

**OBSERVAR modules**

**Analysis of the users reports / accomplished messages and the non-compliances.** Managing with modification suggestions. Documentation of functional and design audits.

- IKS-ZD, IT-Abt
- Risikomanagement (EROM)
- IKS-Fachstatistik (Dir./Abt.REG)
- Compliance / Statements

**Process Modules**
Reporting and documenting the accomplishment of process steps / periodic controls. Requesting modifications for improvement.

**Project Modules**
Reporting and documenting the progress of Projects / degree of conversion of new measures. Requesting modifications for improvement.
Current practices - Risk Mitigation (2)

Definition of risk mitigation measures

RM/ICS ≈ 420 active
CMS ≈ 210 active
Current practices - Monitoring

Risk Identification → Risk Assessment → Risk Mitigation → Monitoring → Reporting

Staff responsible for risk mitigation measures have to report periodically on implementation of risk mitigation measures, resp. on compliance.

Electronic messages/feedback (per year)
RM/ICS/CMS ≈ 2,300
Current practices - Reporting (1)

Overview

Compliance Management System (CMS)

Risk Management (RM)
- corporation-wide risks (strategic level)
- 2012 - March 2013
- 2013 - February 2014
- 2014 and 2015 - February 2016

Internal Control System (ICS)
- Risks within operational processes
- 2012 - March 2013
- 2013 - February 2014
- 2014 and 2015 - February 2016

* B-PCGK = Federal-Public Corporate Governance Code
Current practices - Reporting (2)

Risk Management Reports (incl. ICS) addressed to

- DG, Management Team, QM, IA, etc.
- Audit Committee of the Economic Council
- Economic Council (Supervisory Board)
- External auditors
Current practices - Reporting (3)

Reports on Compliance addressed to

- DG, Management Team, QM, IA, etc.
- Audit Committee of the Economic Council
- Economic Council (Supervisory Board)
- External auditors
- General public *(planned, B-PCGK-report only)*
Aim of the project:
Establishment of a new Survey Infrastructure for Data Collection for Social Statistics

- **Risk identification and risk assessment by**
  - Project team
  - Head of Directorate Social Statistics and head of IT-Departement
  - Controller, Risk Manager

- **Risk catalogue: 66 risks identified, ref. to following risk areas**
  - External risks, stakeholders, image
  - Project organisation, project management
  - Resources, costs
  - Quality (deliverables), time schedule
Risk assessment (example)

- with regard to residual risks
- based on risk descriptions
  - causes of risks
  - early-warning indicators
  - existing risk mitigation measures
RM: Data Collection Project (3)

Risk map, example
„Project organisation, project management“
Definition of risk mitigation measures ≈ 30 (at the project start)
Staff responsible for risk mitigation measures have to report periodically on implementation of risk mitigation measures.
Risk Management Reports

addressed to

- Project team
- Project steering group
  (quarterly)
Summary: Lessons learned, future plans (1)

Important aspects (1)

- „Tone from the Top“: Clear commitment and support of RM by Top Management (DG) is essential
- **Cooperation** with other relevant units (Quality Management, Internal Audit, Controlling, Subject Matter Units, ...)
- **Active involvement** of risk owners in the RM process
- High **risk awareness** of each individual employee
Important aspects (2)

- Efficient **IT tool** is crucial for effective RM. In Statistics Austria the **OBSERVAR** system provides
  
  - modular architecture
    (RM, ICS, CMS resp. the whole RM process covered)
  
  - individually customisable system
  
  - web-based system, simple handling
  
  - prioritisation approach, focus on the real important issues
External auditors (reporting to the supervisory board) gave a **positive assessment** concerning the proper functioning of the risk management system in Statistics Austria.

However, **further developments** are envisaged:

- Risk Management Handbook
- more detailed description of risks
- consideration of content-related overlapping of risks and risk mitigation actions
- pay more attention to interrelation of risks
- provision of more supporting information for quantitative risks assessments
- enhancement of RM concerning key statistical projects and processes
Thank you for your attention!

Please address queries to:
Werner Holzer

Contact information:
Guglgasse 13, 1110 Vienna
werner.holzer@statistik.gv.at
phone: +43 (1) 71128-7269

Working at Statistics Austria since 1994
(various positions)

Risk Manager since 2011
(ISO 31000 and ONR 49000 certified, senior RM)