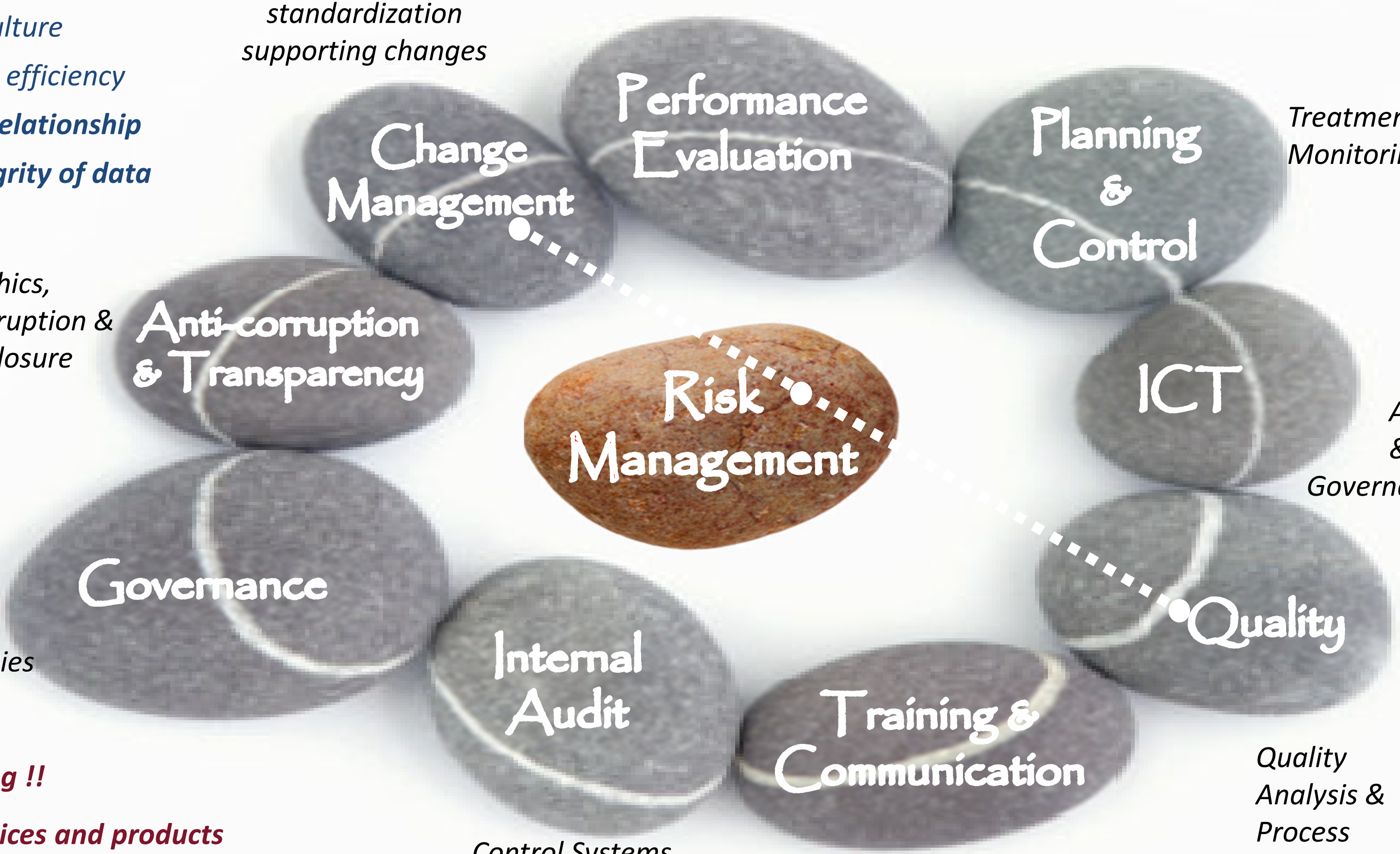
WORKSHOP ON RISK MANAGEMENT SYSTEMS AND PRACTICES

Risk Management in Istat: from the project to the process

Genève, 25-26 April 2016

Management System Network

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



Methods and procedures standardization supporting changes

Staff and Organization Assessment

Treatment & Monitoring

Ethics, anticorruption & disclosure

Audit & ICT Governance

Goals & Strategies

Quality Analysis & Process Management

Control Systems Checks

Organizational culture

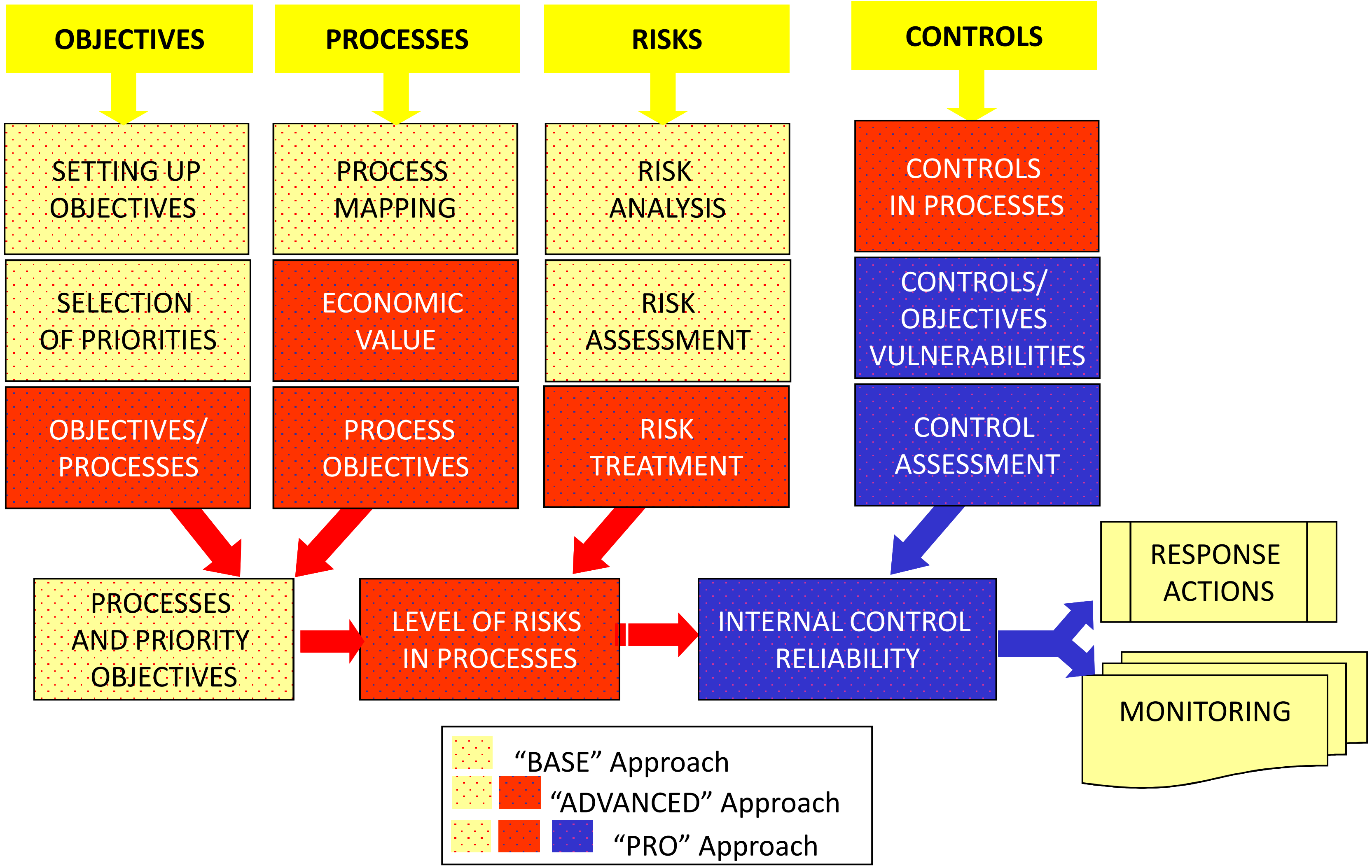
☑ **No overlapping !!**

☑ **Quality of services and products**

☑ **Supporting decision-making processes**

☑ **Enhancement of transparency**

Risk Management approach in ISTAT



OBJECTIVES

SETTING UP OBJECTIVES

SELECTION OF PRIORITIES

OBJECTIVES/ PROCESSES

PROCESSES

PROCESS MAPPING

ECONOMIC VALUE

PROCESS OBJECTIVES

RISKS

RISK ANALYSIS

RISK ASSESSMENT

RISK TREATMENT

CONTROLS

CONTROLS IN PROCESSES

CONTROLS/ OBJECTIVES VULNERABILITIES

CONTROL ASSESSMENT

PROCESSES AND PRIORITY OBJECTIVES

LEVEL OF RISKS IN PROCESSES

INTERNAL CONTROL RELIABILITY

RESPONSE ACTIONS

MONITORING

🟨 "BASE" Approach

🟨 🟥 "ADVANCED" Approach

🟨 🟥 🟦 "PRO" Approach

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

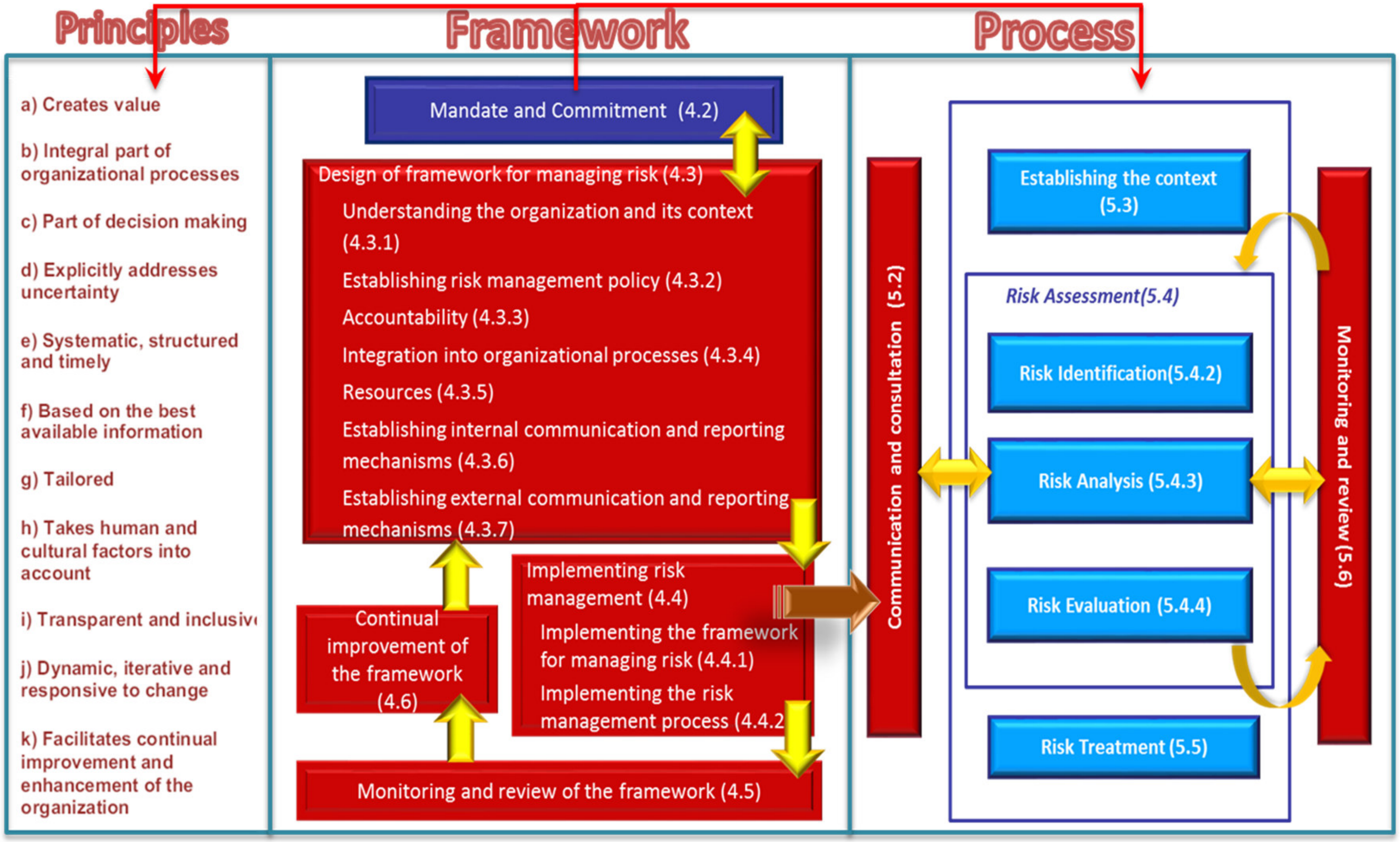
2009	2010	2011	2012	2013-2014	2015-2016
Project launched	**Approach trial**	**Experimental phase**	**Experimental phase**	**Full implementation**	**Developments**
• Analysis and comparison of practices and models • Identification of appropriate approach • Establishing ISTAT’s RM model	• **Survey on Risk perception** • Pilot and rollout of risk management approach • RM training and dissemination	• Creation of risk registers • Risk assessment • RM training and dissemination	• Revision of risk registers • Identification of risk treatments • RM training and dissemination	• Integration w/ operational planning • Risk treatment monitoring • **Information System start-up**	• **From a bottom-up to top-down vision** • Adapting model to Risk of Corruption • Cooperation in International projects • Dissemination

The project developed following some parallel but related paths:

1. ***Organization***: Both the President and the Directorate General endorsed and sponsored the project. A business unit was involved in implementing and coordinating risk management system
2. ***Training and dissemination*** program in order to improve management culture and promote a common language and understanding throughout the organization
3. ***All Risk Management process** has been implemented*
4. ***Information System** has been developed to support the process*
5. ***Change of perspective**: Bottom-up/Top-down mixed approach*

Risk Management System architecture in Istat

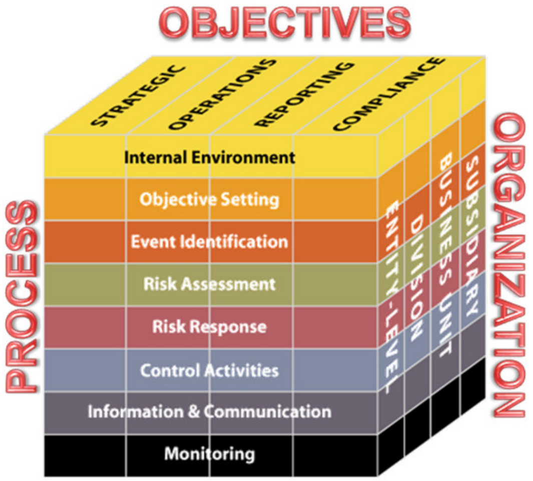
*According to the **ISO 31000:2009**, **Istat**'s Risk Management system refers to the **architecture used to manage risks** that includes **Principles, Framework, and Process**.*


Principles
Framework
Process
a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured and timely
f) Based on the best available information
g) Tailored
h) Takes human and cultural factors into account
i) Transparent and inclusiv
j) Dynamic, iterative and responsive to change
k) Facilitates continual improvement and enhancement of the organization
Mandate and Commitment (4.2)
Design of framework for managing risk (4.3)
Understanding the organization and its context (4.3.1)
Establishing risk management policy (4.3.2)
Accountability (4.3.3)
Integration into organizational processes (4.3.4)
Resources (4.3.5)
Establishing internal communication and reporting mechanisms (4.3.6)
Establishing external communication and reporting mechanisms (4.3.7)
Continual improvement of the framework (4.6)
Implementing risk management (4.4)
Implementing the framework for managing risk (4.4.1)
Implementing the risk management process (4.4.2
Monitoring and review of the framework (4.5)
Communication and consultation (5.2)
Establishing the context (5.3)
Risk Assessment(5.4)
Risk Identification(5.4.2)
Risk Analysis (5.4.3)
Risk Evaluation (5.4.4)
Risk Treatment (5.5)
Monitoring and review (5.6)

Risk Definitions and Standards used in Istat’s RM system

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

- **ISO 31000:2009:** *Risk Management Principles and Guidelines*
- ISO/IEC 31010:2009: *Risk assessment techniques*
- ISO TR 31004:2013: *Guidance for the implementation of ISO 31000:2009*
- **COSO Model 2004/2013,** *a multidimensional standard that develops along three sides of the cube:* ***1) Objectives; 2) Organization; 3) Process.***



Co.SO. ERM, 1992/2004/2013

The selected Model defines:

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

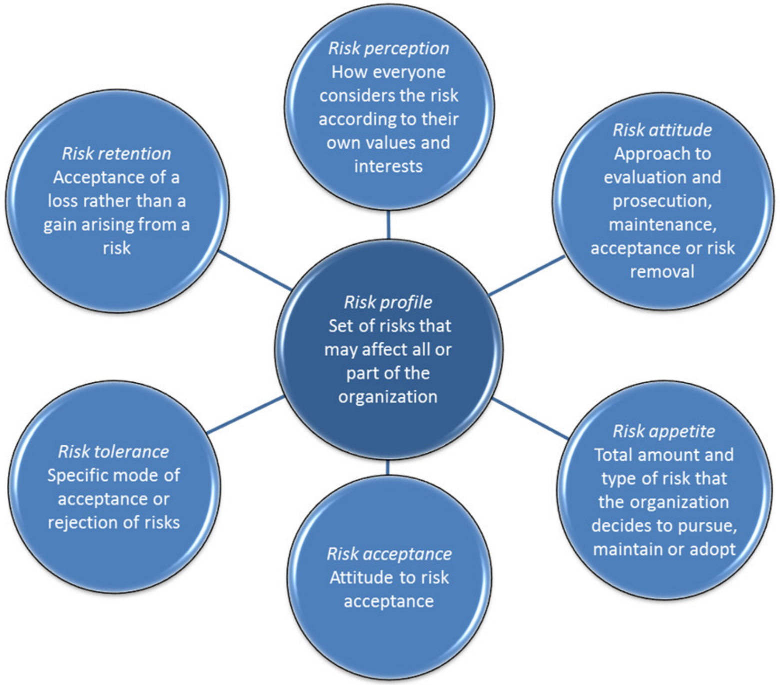
❑ **Risk:** “**the effect of** uncertainty on objectives, where an effect is a deviation from what is expected (positive and/or negative), often **expressed** in terms of a combination of the consequences of an event and the associated likelihood of occurrence”.

Risk Profile and Risk Complexity

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

Risk Profile takes into account:

- **Risk Appetite,** which could be expressed either qualitatively or quantitatively, maybe in terms of ranges, and explored going through the impacts of past events and the reactions of key stakeholders (customers, employees, regulators, ..).
- **Risk Attitude** (Existing Risk Profile). If an organization is particularly effective in managing certain types of risks, it may be willing to take on more risk in that category, conversely, it may not have any appetite in that area.
- **Risk Acceptance**, which refers to the maximum potential impact of a risk event that an organization could withstand. Often, appetite will be well below acceptance.



Risk perception
How everyone considers the risk according to their own values and interests

Risk retention
Acceptance of a loss rather than a gain arising from a risk

Risk attitude
Approach to evaluation and prosecution, maintenance, acceptance or risk removal

Risk profile
Set of risks that may affect all or part of the organization

Risk tolerance
Specific mode of acceptance or rejection of risks

Risk appetite
Total amount and type of risk that the organization decides to pursue, maintain or adopt

Risk acceptance
Attitude to risk acceptance

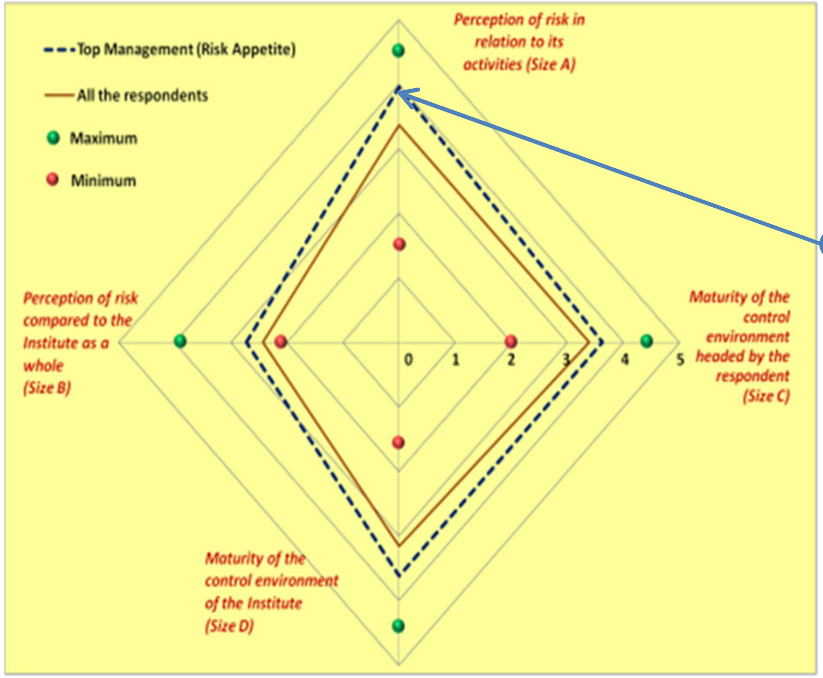
- **Risk Perception**, which describes how people perceive risks according to their values and interests
- **Risk Tolerance**, which is the level of variation that the entity is willing to accept around specific objectives.
- **Risk Retention** considers stakeholders' conservative return expectations and a very low appetite for risk-taking.

Step 1: Survey on Risk perception

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

❖ composed **of about 70 questions** and divided into **four sections**:

1. **Internal control environment** and organizational culture;
2. **Objectives** of the organization and Risk Management;
3. **Identification and classification** of risk factors;
4. **"Cataloging"** risks



❖ investigating **four dimensions**:

I. the **risk perception** compared to the activities of each manager;

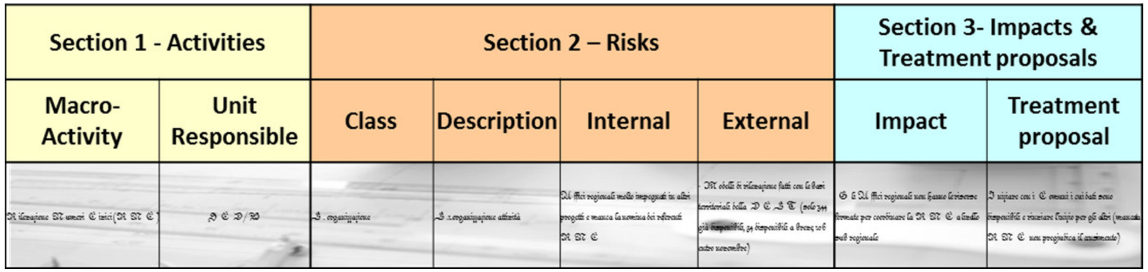
II. the risk perception in the Institute **as a whole**;

III. the **maturity of the control environment** in the structure leaded by each manager;

IV. the **maturity of the control environment** in the Institute as a whole

Step 2: Risk Identification

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



Section 1 - Activities		Section 2 – Risks				Section 3- Impacts & Treatment proposals	
Macro-Activity	Unit Responsible	Class	Description	Internal	External	Impact	Treatment proposal
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

To describe risks **some criteria have been taken into account**:

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

Event	Description
Risk	Uncertain organisational factor that, if it occurs, prevents the accomplishment of results
Criticality	Real hindering event that determines an actual situation of management inefficiency and / or operational

Response action	Description
Preventive action	Action finalysed to prevent the possible occurrence of a critical event, or to eliminate or reduce the damaging effects before they occur
Subsequent action	Action aimed at removing or reducing the effects of the damaging event, after its occurrence
Improvement action	Remedial action responding to a critical event that produce problematic situations or negative effects on the organization

Istat’s Risk Register

Examples of risk register pertaining to “**Organization**":

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

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

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

Main priorities Areas

Some areas were identified as particularly exposed to risks:

1. Management and administrative procedures: obsolescence, non-compliance, waste of resources, inefficiencies in sharing and disseminating information;
2. Recognition and quantification of project costs in order to properly deploy the available resources;
3. Integration among the management systems to support decision making and sector plans;
4. Tendering procedures: requirements, preparation of specifications (technical and legal), tender's award;

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

Results

- ❑ Risks and organisational criticalities:

  more than 96% of the total (100% in the **Prioritization Areas**)

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

Risks	All Areas		**Prioritization Areas**	
	N.	***%***	***N.***	***%.***
TOTAL	**359**	**100,0%**	**170**	**100,0%**
Nature				
Risks	65	18,1%	33	19,4%
Criticalities	279	77,7%	137	80,6%
Others	15	4,2%	0	0,0%
Type				
Strategic	22	6,1%	6	3,5%
Compliance	6	1,7%	2	1,2%
Operatives	310	86,4%	155	91,2%
Reporting	13	3,6%	6	3,5%
Exogenous	8	2,2%	1	0,6%

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

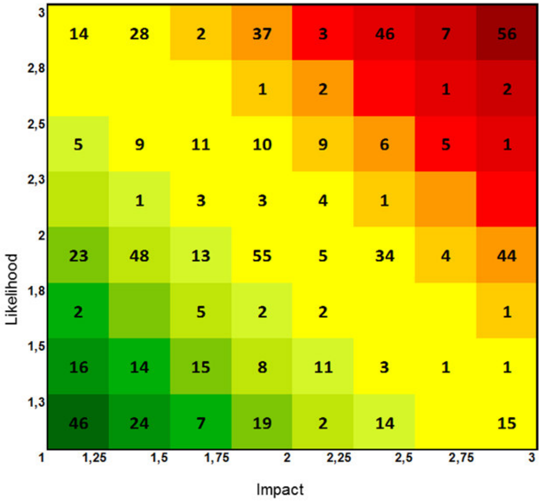
Step 3: Risk Assessment - C&RSA

The risks were assessed by the same personnel who contributed to identify them, using the **Control & Risk Self Assessment** (C&RSA) method to measure the risk's likelihood and impact on the organization.

2 factors were considered to assess the risks

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

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



14	28	2	37	3	46	7	56
			1	2		1	2
5	9	11	10	9	6	5	1
	1	3	3	4	1		
23	48	13	55	5	34	4	44
2		5	2	2			1
16	14	15	8	11	3	1	1
46	24	7	19	2	14		15

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

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

Step 4. Risks Treatment

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

Treatment	**All Areas**		**Prioritization Areas**	
TOTAL	**466**		**231**	
Risks and Criticalities	***V.A.***	***%.***	***V.A.***	***%.***
TOTAL	**450**	**100,0%**	**231**	**100,0%**
Types				
Preventive	36	8,0%	24	10,4%
Subsequents	6	1,3%	3	1,3%
Improvement	261	58,0%	143	61,9%
To deepen	83	18,4%	42	18,2%
Others	64	14,2%	19	8,2%
Responsabilities				
Internal	170	37,8%	101	43,7%
External	44	9,8%	22	9,5%
Cross-cutting	172	38,2%	89	38,5%
Not attributable	64	14,2%	19	8,2%

❑ 58% of the proposals refers to organisational or production improvement (about 62% in the p.a.);

❑ Nearly 38% of the actions are internal (about 44% in the p.a.);

❑ Over 38% of the actions requires the collaboration of different structures (about 39% in the P.A.)

From the Bottom-up to the Top-Down approach

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

Top-down
+
Bottom-up

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

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

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

Corporate risks are **specifically monitored** by appropriate output and performance indicators.

Top-Down approach: «Corporate» risks

Critical Events	2013		2014		2015		2015 Corporate	
Risks	65	18,1%	34	16,3%	17	15,3%	7	35,0%
Criticalities	279	77,7%	175	83,7%	89	80,2%	13	65,0%
Others	15	4,2%		0,0%	5	4,5%		
TOTAL	**359**		**209**		**111**		**20**	

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

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

Treatments - Responsability	2013		2014		2015		2015 Corporate	
Internal	170	37,8%	128	50,4%	62	48,4%	12	48,0%
External	44	9,8%	21	8,3%	14	10,9%	0	0,0%
Cross-cutting	172	38,2%	105	41,3%	52	40,6%	13	52,0%
Other	64	14,2%		0,0%		0,0%		
TOTALE	**450**		**254**		**128**		**25**	

Top down approach: Roles and accountabilities

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

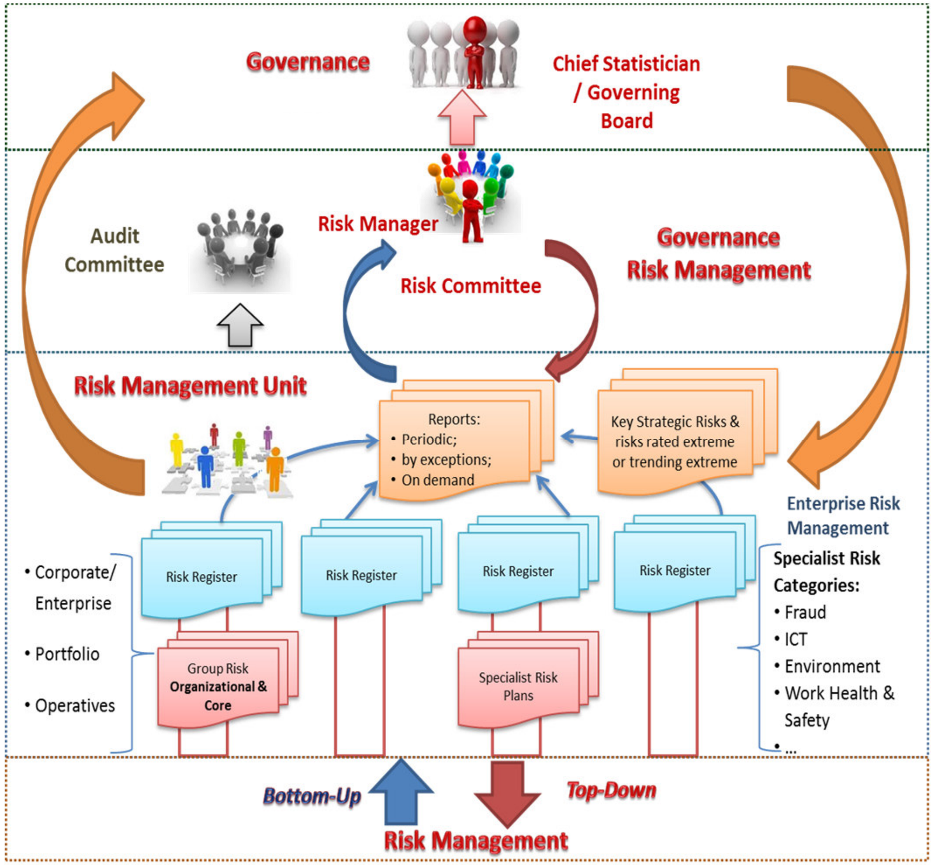
2) Risk management is driven by the **organizational units**;

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

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

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

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



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

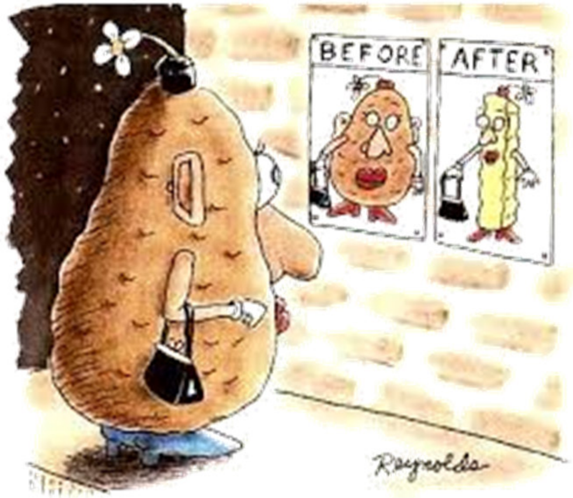
Where we are going to

Implementing three levels of Controls:

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

Improving the Risk Management System:

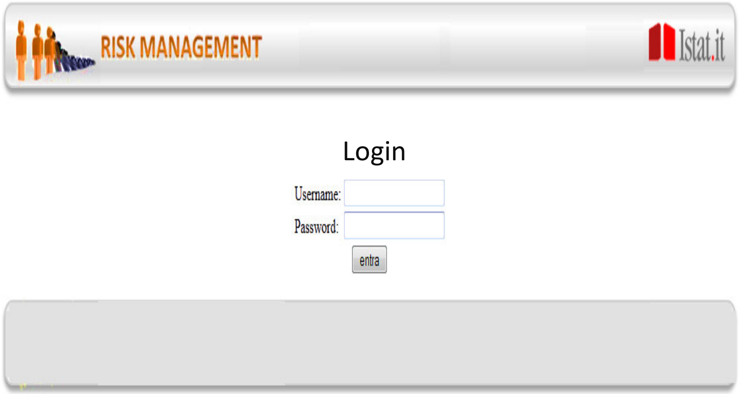
- Connecting Risk Management System to GAMSO
- Designing a set of Key Risk Indicators tailored for GSBPM standard
- Adopting the Model for Fraud risks
- Improving ERM supporting software
- Fostering link with Performance Evaluation
- **Improving Quality through Risk Management**
- **Moving to a centralized organizational Model**
- **Deeper integration (Internal controls & Management information system)**



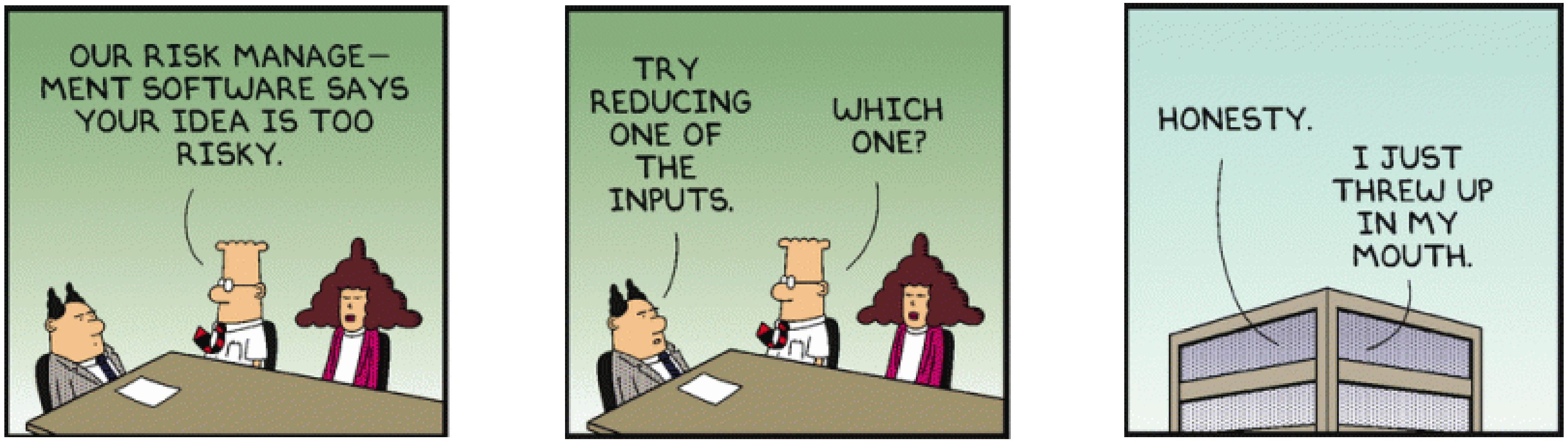
Reporting and Communication: the «RiskInIstat» tool

The information system **RiskInIstat** has been implemented to manage risks via web with the main objective to let Management edit and view the necessary information, in an intuitive and immediate way.

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



provided that "RELIABLE" information is uploaded !!!


OUR RISK MANAGE-MENT SOFTWARE SAYS YOUR IDEA IS TOO RISKY.
TRY REDUCING ONE OF THE INPUTS.
WHICH ONE?
HONESTY.
I JUST THREW UP IN MY MOUTH.

Thank you for your attention !!!

Fabrizio ROTUNDI

rotundi@istat.it

fabrizio.rotundi@gmail.com