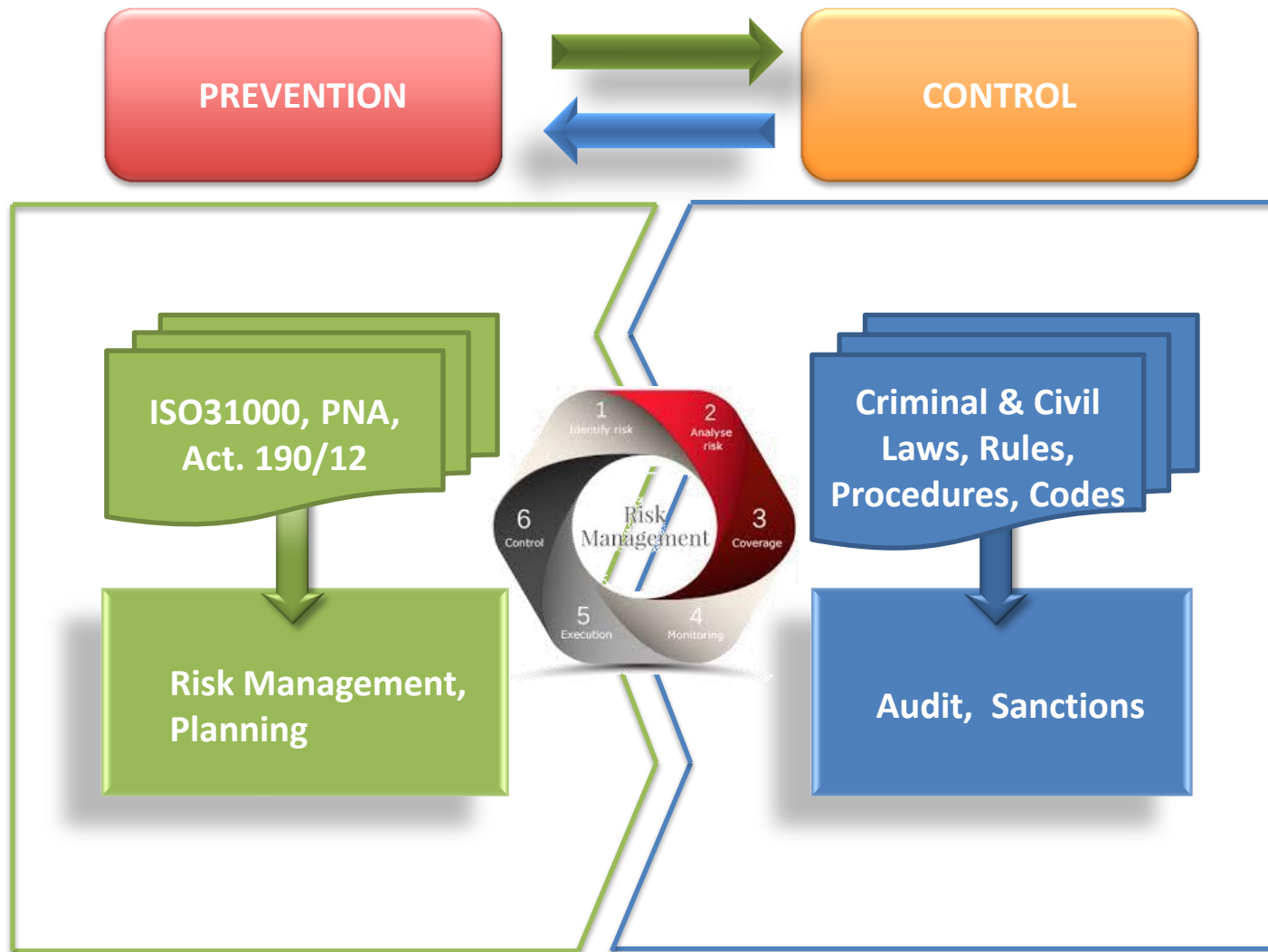# Workshop on Efficiencies and Quality

Ethics and organization
Istat's Fraud Risk Management System

(Geneve, 27/29 September 2017)

Anti-Corruption approaches

PREVENTION → CONTROL

PREVENTION

ISO31000, PNA, Act. 190/12

Risk Management, Planning

Risk Management
1 Identify risk
2 Analyse risk
3 Coverage
4 Monitoring
5 Execution
6 Control

CONTROL

Criminal & Civil Laws, Rules, Procedures, Codes

Audit, Sanctions

Ethical culture

Survey: What people think about corruption in Italy

	Italy	EU
- is a widespread phenomenon	**97%**	**76%**
- is normally suffered in daily activities	**42%**	**26%**
- is the easiest way to get public services	**88%**	**73%**
Would you report to the authority an episode of corruption?	**56%**	**70%**

Source: Global Corruption Barometer
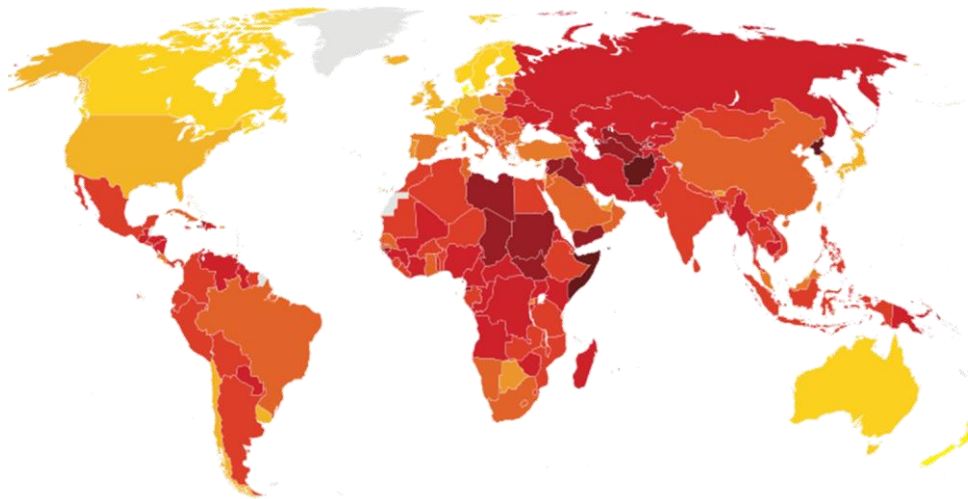
Corruption Perception Index

TRANSPARENCY INTERNATIONAL
the global coalition against corruption

SCORE

Highly Corrupt — Very Clean

0-9 10-19 20-29 30-39 40-49 50-59 60-69 70-79 80-89 90-100   No data
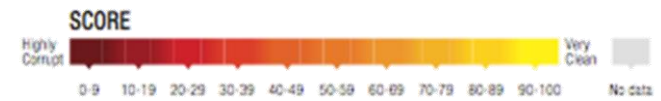
Regulatory framework

Government

Act n. 190/2012
Provisions for the prevention and repression of corruption and lawlessness in public administration

Authority

National anti-corruption plan (PNA)

| Trasparenzcy Act n. 33/2013 | Ineligibility Act n. 235/2012 | Attributes preventing sb from getting appointed & incompatibility Act n. 39/2013 | Code of conduct Act n. 62/2013 |

Three-year prevention of corruption plan (PTPC)

Public Administrations

PNA GOALS:

1. **Reduce opportunities** for corruption

2. **Increase the ability** to detect corruption cases
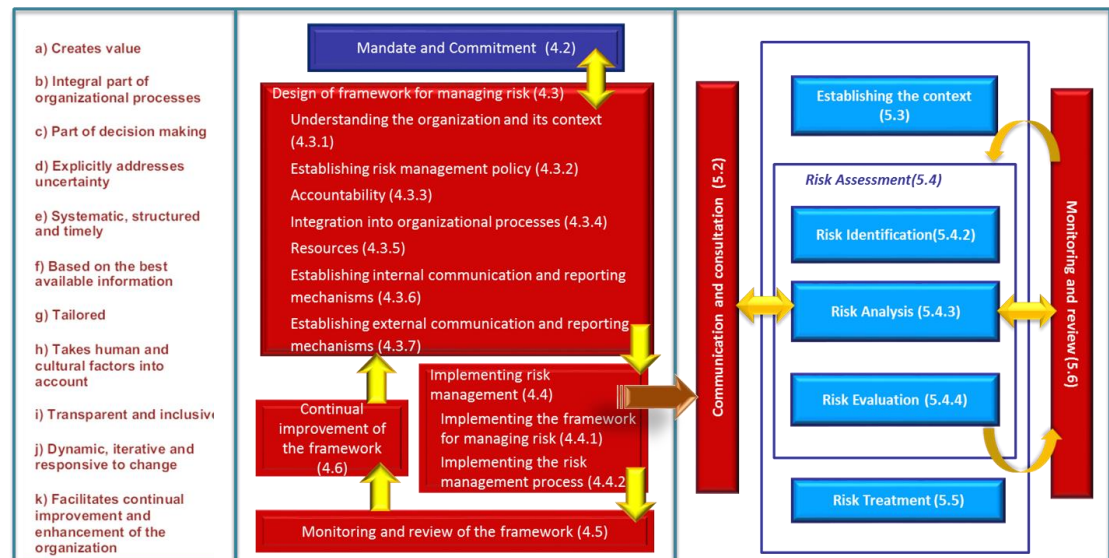
3. **Create an adverse** context for corruption

PTPC GOALS:

1. **Identify activities,** sectors and business areas **mostly exposed to corruption**

2. **Identify** the activities, mechanisms and **tools** for **preventing** the identified **risk of corruption**

3. **Verify** how PTPC **is implemented**

4. **Implement and update** PTPC

Fraud Risk Management in Istat

❑ **ISTAT has build its Fraud Risk Management System** relying on the **experience gained in the Organizational RM** making some **adjustments** due to the characteristics of corruption risks: internal and external context, actors, object, standards, techniques

❑ ISTAT's model goes **beyond the logic of fulfillment** and aims to build a structured system designed to identify, analyze, evaluate and treat potential illegal behaviors

❑ Risk management leads to **reduce the likelihood** that a critical event will occur through a **planned and cyclical identification**, evaluation and treatment of **behaviors** potentially risky and detrimental to the integrity (**ISO31000:2009**)

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 inclusive

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)

❑ To manage the risk of corruption, the **same computerized system** adopted for the organizational risk management is used so to build progressively an unique Risk catalog

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, under the coordination of the Responsible for the Anti-corruption System (the Risk Manager);

3) **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;

4) **the Contact points network,** **supporting the highest level of decision making** to define the Risk Management policy, is **coordinated by the Risk Manager** and composed by managers operating in the most risky areas;

5) **the Chief Statisticians and Governing body define the strategies** based on the information coming from the RM System;

6) **The Internal Control** is responsible for **reporting to the Governance** on the **adequacy of the RM process** and the **compliance of the mitigating actions**.
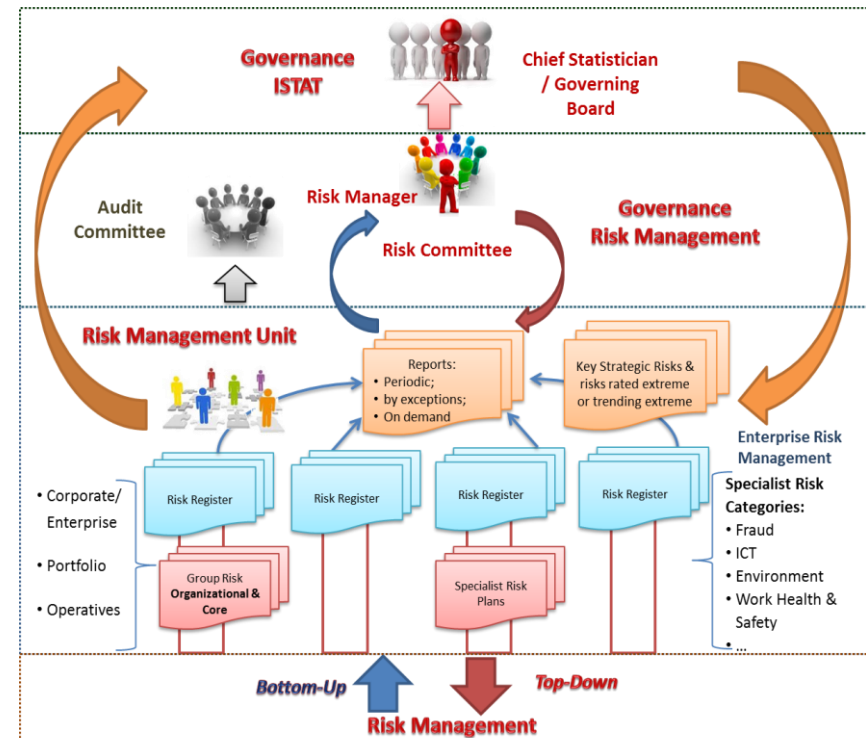
Istat

Risk management Process in ISTAT

The process is **composed by 6 steps**:

1. *Establish the process*
2. *Identify the risks*
3. *Rate the inherent risk*
4. *Identify and rate mitigating controls*
5. *Calculate residual risk*
6. *Develop action plan*

| 1. Establish the process | 2. identify the risks | 3. Rate the inherent risk | 4. Identify and rate mitigating controls | 5. Calculate residual risk | 6. Develop action plan |

Global Compact Model
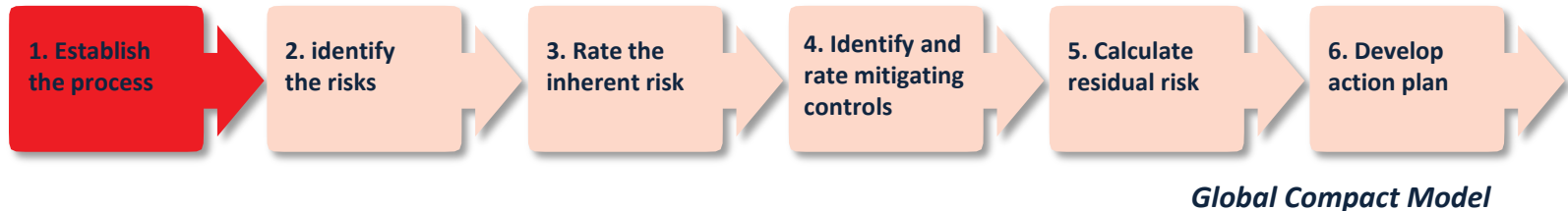
➢ **The first step of the Risk Management process "Establishing the process" is based on the definition of the Risk Tolerance,** involving either the **Board of Directors** or those charged with governance (such as the Audit Committee).

➢ **If risk tolerance is not explicitly determined** up front, there is the potential that **management will rationalize existing levels of corruption risks as acceptable**, thereby undermining the purpose and value of the anti-corruption risk assessment.

The CORRUPTION SCHEME

FRAUD SCHEME: Set of **factors that qualify an existing event of corruption**, composed by (at least): Author(s), Risk, Behavior and Cause.

1. **RISK**: **Occurrence or change of a particular set of circumstances** (organizational, social or environmental) that may obstacle the achievement of a public or private entity (from ISO 31000:2010).
   DESCRIPTION: Type of **criminal offense or criminal category** where a conduct of corruption is included
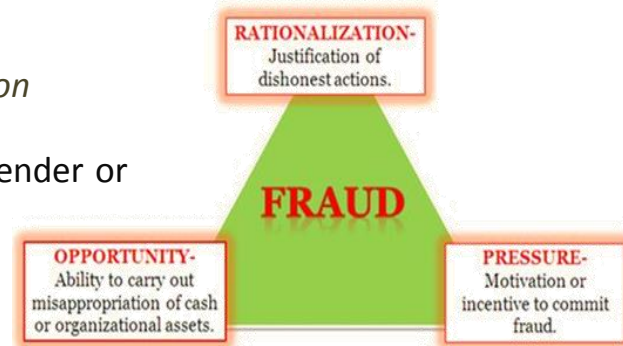
2. **BEHAVIOUR:** Action by which an **act or omission is committed** by one or more persons, in any agreement between them, with the intention to realize an act of corruption in a "broad" sense.

3. **CAUSE**: **Voluntary or forced push**, related to personal sphere, organization or environment, to act a corrupt behavior, including:

   • *Financial pressures: needs, «modus vivendi», incentive programmes, greed, self-centeredness;*

   • *Perceived opportunity by potential offenders because of their technical skills, knowledge of control weaknesses; motivation; limited consequences;*

   • *Rationalization (wish) in carrying out the fraud, self-justification*

4. **EFFECT:** Any **situation of unfair advantage** in favor of the offender or unfair loss against third parties, organizations or communities

5. **ENABLING FACTOR:** **organizational, social, environmental circumstance which may favor** committing a **fraud**

RATIONALIZATION-
Justification of dishonest actions.

FRAUD

OPPORTUNITY-
Ability to carry out misappropriation of cash or organizational assets.

PRESSURE-
Motivation or incentive to commit fraud.

The triangle of fraud, D. Cressey

Istat

Examples from the Istat's Risk Register

1. Establish the process	2. identify the risks	3. Rate the inherent risk	4. Identify and rate mitigating controls	5. Calculate residual risk	6. Develop action plan

Extract from Fraud Risk catalog ISTAT – Risk Identification

Risk Area	Fraud Risk	Enabler	Cause	Effect	Behaviour	Controls	Treatment
Statistical products & services	**Unauthorised disclosure of statistical data and/or information (sensitive data included)**	**Lack of security systems**	**Economic Pressures (internal / external)**	**Litigation, class actions**	**1) Use of disaggregated data for personal purposes**	**Internal procedure**	**Outlining of a control procedure to identify possible improper accesses**
				Loss of reputation	**2) Early dissemination of data from press releases with a high degree of confidentiality**	**Code of Conduct and sanctions**	**Report from the whistleblower system**

Inherent and *Residual* Risk

Risk:

Combination of the likelihood of an event and its effects
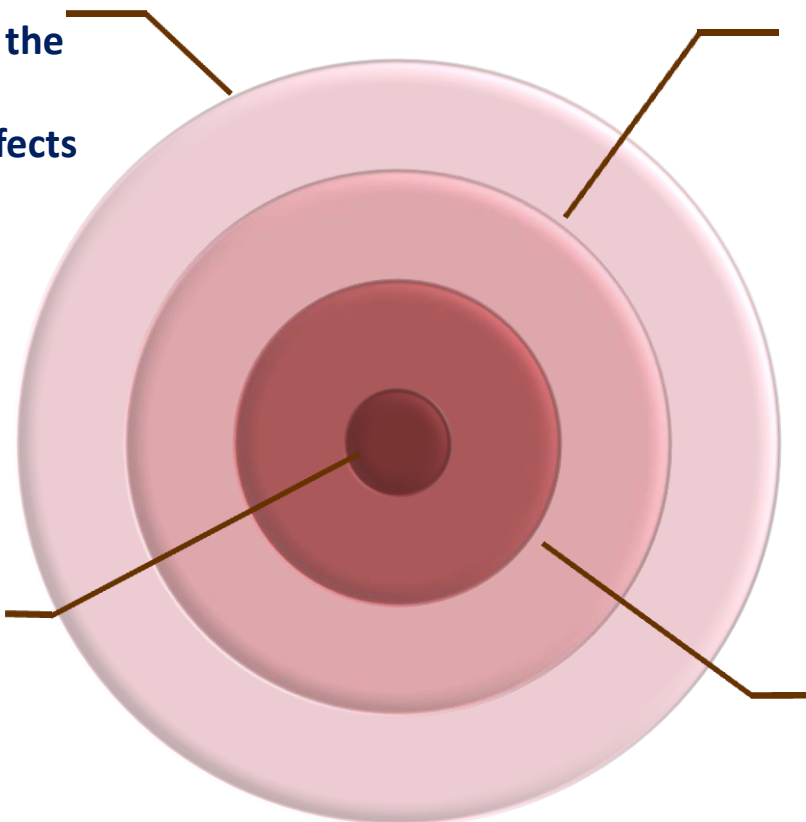
Inherent Risk:

Risk without any intervention

Residual risk:

Risk remaining after the treatment, possibly containing risks not identified

Risk treatment:

Selection and implementation of interventions on risk: transfer, rejection, probability and impact reduction, mitigation, elimination

Istat

Risk Assessment: Likelihood & Impact Rating

| 1. Establish the process | 2. Identify the risks | 3. rate the inherent risk | 4. Identify and rate mitigating controls | 5. Calculate residual risk | 6. Develop action plan |

Probability Scoring Matrix

three-point scoring matrix for identified Corruption Schemes	score
Little probability of corruption activity	1
Some probability of corruption activity	2
High probability of corruption activity	3

five-point scoring matrix for identified Corruption Schemes	score
Minimal probability of corruption activity	1
Little probability of corruption activity	2
Some probability of corruption activity	3
Considerable probability of corruption activity	4
Very high probability of corruption activity	5

Potential Impact Scoring Matrix

sample three-point potential impact scoring matrix for identified Corruption schemes	
categorization of corruption scheme potential impact	score
Insignificant impact	1
Moderate impact	2
High impact	3

sample three-point potential impact scoring matrix for identified Corruption schemes	score
Insignificant Impact	1
Minor Impact	2
Moderate Impact	3
Major Impact	4
Catastrophic Impact	5

Risk Assessment: Identify and rate mitigating controls

| 1. Establish the process | 2. Identify the risks | 3. rate the inherent risk | 4. Identify and rate mitigating controls | 5. Calculate residual risk | 6. Develop action plan |

Scoring Matrix for Control Rating

sample of 3-point scale scoring matrix for control rating		
Qualitative Categorization	**numerical Categorization**	**Control risk rating**
Good/Effective	3	Low
Fair/Partially Effective	2	Medium
Poor/Ineffective	1	High

sample of 5-point scale scoring matrix for control rating		
Qualitative Categorization	**numerical Categorization**	**Control risk rating**
Excellent/Very Effective	5	Very Low
Good/Effective	4	Low
Fair/Neutral/Partially Effective	3	Medium
Poor/Somewhat Effective	2	High
Very Poor/Ineffective	1	Very High

Risk Assessment: Calculate residual risk

| 1. Establish the process | 2. Identify the risks | 3. Rate the inherent risk | 4. Identify and rate mitigating controls | 5. Calculate residual risk | 6. Develop action plan |
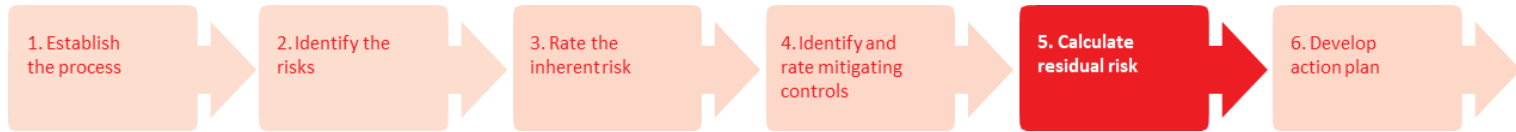
Qualitative Scale for Determining Residual Risk

If inherent risk is	And Control risk rating is (Low=Effective; Medium=Partially Effective; High=Ineffective)	then residual risk is Normally
High	High	High
High	Medium	Either High or Medium
High	Low	Either Medium or Low
Medium	Low	Low
Medium	Medium	Either Medium or Low
Medium	High	Medium
Low	High, Medium or Low	Low

Istat

Risk Assessment: Calculate residual risk

| 1. Establish the process | 2. Identify the risks | 3. Rate the inherent risk | 4. Identify and rate mitigating controls | 5. Calculate residual risk | 6. Develop action plan |
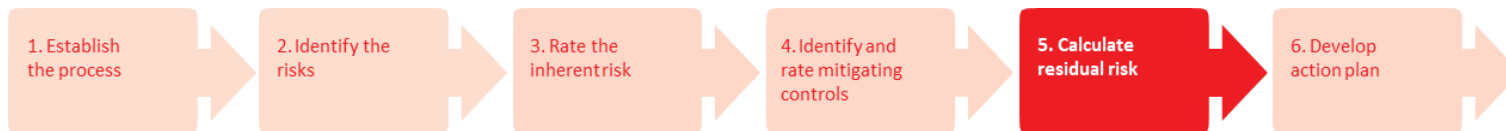
Extract from Fraud Risk catalog ISTAT – Residual Risk Assessment

Risk Area	Fraud Risk	Enablers	Cause (cathegory)	Behaviour	Likelihood	Impact	Inherent Risk	Control effectiveness	Residual Risk
Statistical products & services	Unauthorised disclosure of statistical data and / or information (sensitive data included)	Lack of security systems	Pressures (internal / external)	1) Use of disaggregated data for personal purposes	Medium	High	High	Medium	Medium
				2) Early dissemination of data from press releases with a high degree of confidentiality	Medium	High	High	Medium	Medium

From a Bottom-up to Top-Down perspective: «Corporate» risks

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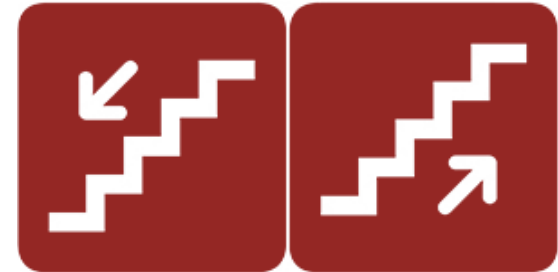
❑ Operational risks are identified by accountable managers and then **gathered in strategic categories** (*corporate risks*), in order to be assessed, treated and monitored.

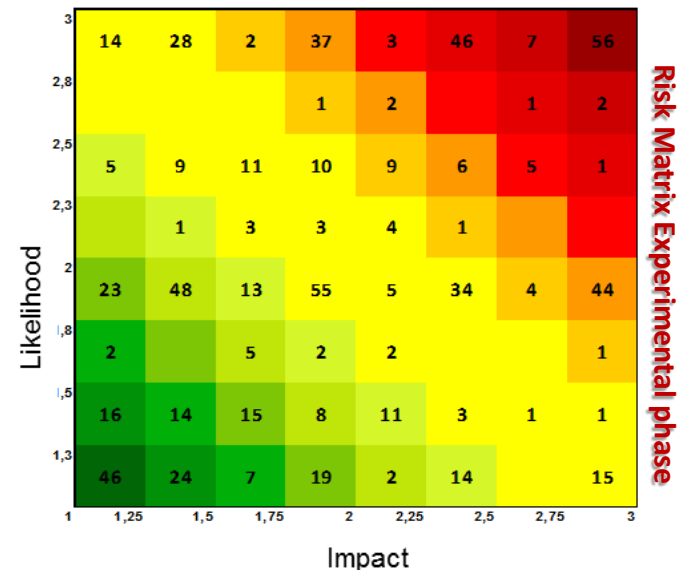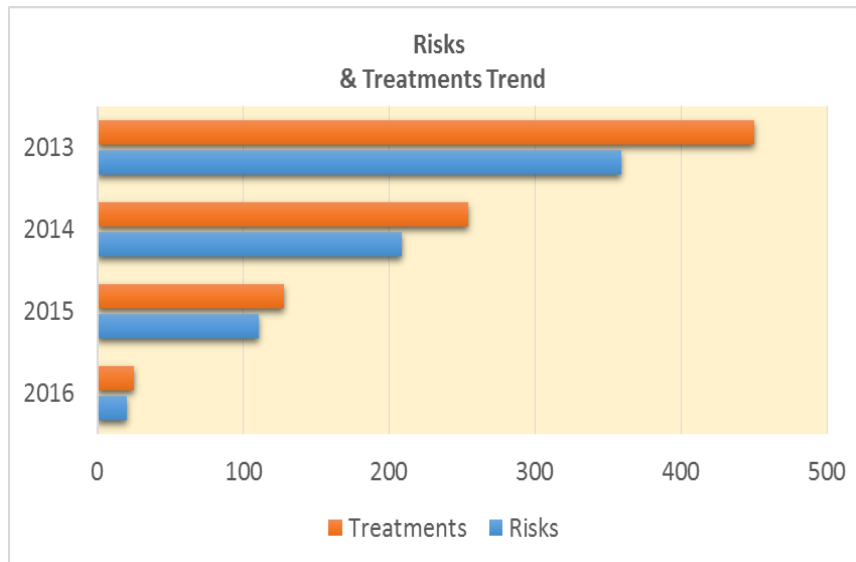Corporate risk selection also takes into account the **following criteria:**

➢ **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 means of proper output and performance indicators

Istat

Results from the Top-Down approach

The **ISTAT's three-year anti-corruption plan** shows that, according to the **Top-Down perspective**, risks have been dramatically decreased: from 359 events of the experimental phase to the **58 potential happenings were classified as risks in 2016** (20 "Corporate"), while **the associated behaviors** are 109, (20 related to "Corporate" risks).

The **Inherent risks are assessed by the same personnel** who identified them with the **C&RSA method** to measure **likelihood** and **impact and allocated along the Risk Matrix**

Risks & Treatments Trend

Year	Risks (blue)	Treatments (orange)
2013	~360	~450
2014	~210	~255
2015	~110	~130
2016	~20	~25

■ Treatments ■ Risks

Risk Matrix Experimental phase — Likelihood (y-axis) vs Impact (x-axis)

Likelihood \ Impact	1,25	1,5	1,75	2	2,25	2,5	2,75	3
3	14	28	2	37	3	46	7	56
2,8			1	2			1	2
2,5	5	9	11	10	9	6	5	1
2,3		1	3	3	4	1		
2	23	48	13	55	5	34	4	44
1,8	2		5	2	2			1
1,5	16	14	15	8	11	3	1	1
1,3	46	24	7	19	2	14		15

Risk treatments have been reduced too, from 450 (2013) to **118** (2016); about 29% (32) are associated with **"Corporate" risks, monitored by appropriate performance indicators.**

Risk treatment process

| 1. Establish the process | 2. Identify the risks | 3. Rate the inherent risk | 4. Identify and rate mitigating controls | 5. Calculate residual risk | 6. Develop action plan |

Planning contains programming scheme helpful to reduce likelihood of risk occurrences, according to risk areas, showing:

Feasibility Plan

| Specific actions	State of implementation	Implementation phases and timetable	Implementation indicators	Accountabilities
Outlining of a control procedure to identify possible improper accesses	On Going	**I Phase:** Procedure Formalization (October 201X); **II Phase:** Procedure Dissemination (November 201X) **III Phase:** Six-monthly monitoring through a specific application	Information from managers in charge and other staff involved	All the senior managers involved
Reports from the whistleblower system	To be implemented	**I Phase:** Outlining of the whistleblower system requirements (October 201X); **II Phase:** Information system test (January 201X) **III Phase:** Adoption of whistleblowing regulation	No. of reports followed up / No. of reports received	Head of HR

Risk Treatment

Proposer Responsible Controller		
Risk		
Process		
Phase		
Behaviour		
Enabling Factors		
Time of Validity		
Objectives		
Indicators and control procedure		
Procedure	....	
Format		
Phases	**Unit**	**Timesheet**
1.	....	...
2.	....	....

Istat

The three lines of defense (3LOD - ECIIA)

**Internal control system** is structured on **3 different levels**:

1. the **first line**, *(Risk owners)* by *operational management* who have the responsibility to identify analyze and mitigate risks (***Key Performance Indicators***);

2. the **second line**, *(Risk Manager)* that is the role of the compliance function, with the task of facilitating and monitoring the implementation of effective "risk management" by managers; this level oversees the process of risk assessment and control, ensuring its consistency with business goals (***Key Risk Indicators***);

3. The **third line (in progress)** will be played by Audit, which, with a "risk based" approach, will provide an adequate assurance on the effectiveness whereby the organization evaluates and controls compliance and adequacy of the other lines (***Key Performance & Key Risk Indicators***).
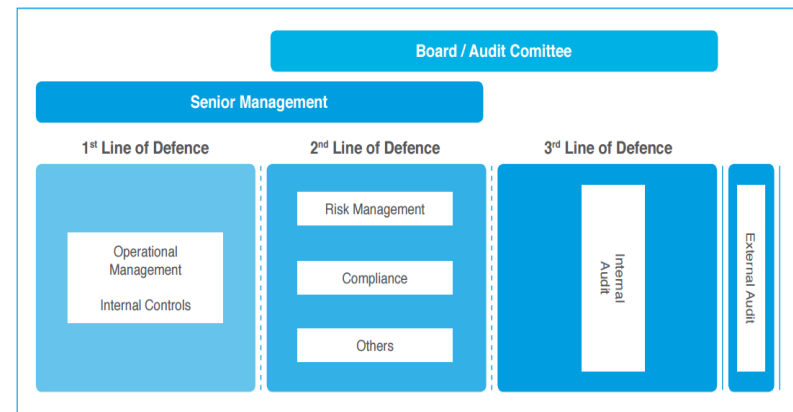
The information supporting system - RiskInIstat

The tool **RiskInISTAT:**

➢ **manages risks via web** with to let Management edit and view the necessary information, **in an intuitive and immediate way**, depending on organizational hierarchy;

➢ provides the possibility to **update the catalogs** and show how much the objectives has been realizing at **different stages of the ERM process**;

➢ allows for **planning treatment actions** related to **priority risks** through the detailed planning based on the so-called **"Feasibility plans",** which **locates** *actors, phases, lead-times as well as indicators for the outputs* accomplished, and **compares costs** incurred to *assess the effectiveness of treatments.*

CATALOG UPDATE	CATALOG VALIDATION	MONITORING ACTIONS
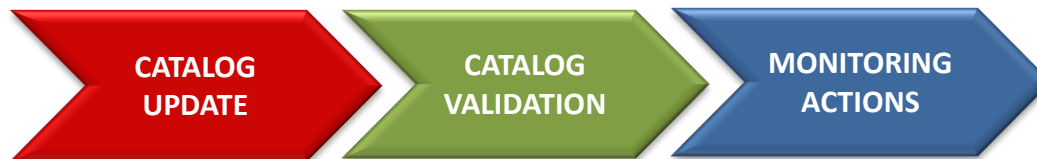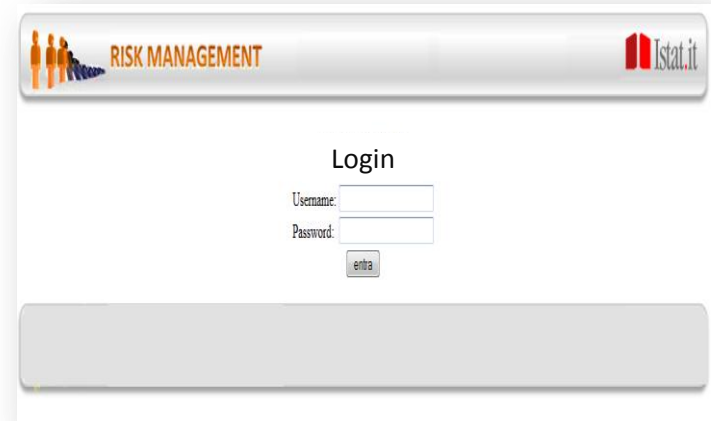
The tool complies with the Risk Management process's phases.

The implementation of Fraud Risk Management in ISTAT has been continuously followed by internal and external training and the dissemination via a specific website

Thanks for your attention !!!

Fabrizio ROTUNDI

rotundi@istat.it

fabrizio.rotundi@gmail.com