
***Ethics and organization:
The Fraud Risk Management
practice in Istat***

Rome, August 2017

1. Foreword	2
2. The fraud risk management system in Istat	2
3. The architecture: roles and actors involved	3
4. The fraud risk management process and its phases	4
4.1 Phase 1: risk identification	4
4.2 Phase 2: risk assessment	5
4.3 Phase 3: treatment action monitoring and its integration with the performance system	7
5. Supporting tools: <i>RiskinIstat</i>	8

Authors: Angela Leonetti, Alessandra Lucchese, Fabrizio Rotundi, Marco Tozzi

1. Foreword

The Act no. 190/2012 introduced a new approach to manage fraud risks in Italy by moving from a vision based entirely on repression to a vision based on involving the public bodies in order to prevent corruption through their own participation and responsibility. In Italy, every public entity is currently expected to implement an anti-corruption strategy through designing, setting up and developing a fraud risk management system while respecting the directions and recommendations given by law and the Italian Anti-corruption Authority (A.N.A.C.). This new overall vision of an organizational risk management system is affected by international expertise and standards that are best known and most widely used in public sectors, such as ISO 31000:2009 – Risk Management Principles and Guidelines and in particular ISO 37001:2015 – Anti-Bribery Management Systems.

The Italian Anti-corruption Authority yearly releases strategic Guidelines (named *National Anti-corruption Plan*) to prevent fraud in the public sector; from such lines every public entity is expected to draft on a yearly basis its own Anti-corruption Plan.

The term “corruption”, used in this paper, is to be understood in a broad sense, including bribery, asset misappropriation and financial fraud situations, to state an intentionally fraudulent behavior aimed at causing an unfair advantage or disadvantage with regard to a particular entity.

2. The fraud risk management system in Istat

Since 2009 Istat has been implementing its own Risk management system, of which a key feature is specialization, that is, the possibility to structure the a risk register according to the nature of risk. The risk identification and analysis phases currently include, on the one hand, clustering organizational risks as corporate and operational ones, on the other hand, building registers for specific risks (fraud, safety at work, etc). In Istat Fraud risk management is therefore integrated in the Risk management system, but according to the Italian anti-corruption law the responsibility for the process of fraud risk identification and analysis is kept separate from the organizational one.

In Istat a specific function for risk management has been established; according to this organizational choice, the process owners identify and assess both organizational and fraud risks they are responsible for (bottom-up phase), while the risk manager is expected to validate, weight and determine the treatment priorities (top-down phase). Italian law provides for a senior manager

appointed by the governing body to ensure proper implementation of the corruption risk management processes, and describes his duties in detail.

Establishing one Risk Management function only allows to coordinate organizational risk management with the corruption risk one, given that mis-organization is a key factor in facilitating fraud behaviors to such an extent that most actions to prevent corruption risks are traceable to overall organizational improvement initiatives.

3. The architecture: roles and actors involved

In Istat, the actors involved in the fraud risk management system implementation are as follows:

- a) The *Governing Body*, that is expected to determine the strategic goals to prevent corruption and promote transparency and integrity, as well as to appoint the Head of Anti-corruption Management and to adopt the Anti-corruption Plan;
- b) The *Head of Anti-corruption Management & Transparency*, whose main duties are:
 - to draft a proposal of Anti-corruption Plan to be submitted to the Governing Body's approval;
 - to set out proper procedures to select and train the staff to be involved in the corruption risk management process;
 - to coordinate treatment action implementation and evaluating of its effectiveness;
 - to monitor the Plan overall implementation;
- c) The *Senior Managers*, who have to set out and implement the treatment actions (against fraud) which are responsible for, as well as appoint the contact persons and other staff involved in activities to prevent corruption within the Division/Department they are in charge of;
- d) The *Risk Management Function*, which methodologically supports all structures during any phases of the risk management process and cooperates with the Head of Anti-corruption Management in defining criteria for establishing treatment priorities;
- e) The *Contact Persons for Anti-corruption Management*, who support:
 - the Risk Management Function during the fraud risk identification process;
 - the Head of Anti-corruption Management in monitoring the risk mitigation actions by promptly notifying any needs for changing the Anti-corruption Plan;
- f) The *Performance Assessment Independent Body*, which evaluates the consistency of the Anti-corruption Plan with the goals established within both strategic and operational planning

through checking if the performance measurement and evaluation process has taken into account the achievement of specific anti-corruption objectives;

- g) *All Istat personnel*, who are expected to know the contents of the Anti-corruption Plan and to cooperate in implementing the related treatment actions.

4. The fraud risk management process and its phases

The risk management model adopted by Istat entails the same framework to manage both organizational and fraud risks, although these latter have a different evaluation target, that is, the scheme of fraud. The process therefore involves the following phases:

1. Risk identification;
2. Risk assessment, in terms of analysis and weighting;
3. Risk treatment.

In order to strengthen the corruption risk governance, Istat has set up an integrated Risk Policy whose implementation in charge of the actors involved is monitored by the Risk Manager.

4.1 Phase 1: risk identification

Identification of those risks that can threaten Istat's integrity, together with the analysis of those factors that can encourage corruptive conducts, is preparatory to setting out of the most effective treatment in order either to prevent a risk occurrence or to mitigate its impact. Istat's risk management model therefore aims at locating the elements characterizing a scheme that is common to any kind of fraud:

- *behaviors*, i.e., practical actions through which fraud is made real;
- *causes*, i.e., factors that can generate a risk, either alone or together with other factors;
- *enablers*, i.e., those factors encouraging behaviors and then allowing for detection of the most effective treatment to mitigate the likelihood of risk occurrence as well as the consequences of a risk event.

In Istat, risk identification is carried out by the offices in charge of the related processes, according to methodological directions given by the *Risk Management Function* and under the coordination of the Head of Anti-corruption Management.

The information thus obtained helps to set up the *Fraud Risk Register*, which is also made of the following further items:

- *Risk area*: cluster of activities that are linked to each other and more subjected to corruption risk;
- *Risk event*: any actual occurrence coming from the uncertainty related to proper pursuing the public interest, and then the Istat's mission;
- **effect/consequence** from a risk event;
- **existing controls**: structured and formalized activities aimed at reducing the likelihood and/or impact of a risk event;
- *mitigation measures*: treatment actions aiming to either prevent specific risk events or reduce their effects/consequences.

All these elements must be added to the above-mentioned information on *behaviors, causes* and *enablers*.

Here follows a *template* used to identify fraud risks.

Table 1: Example of typical features in a risk occurrence

<i>Risk Area</i>	<i>Fraud Risk</i>	<i>Enabler</i>	<i>Cause</i>	<i>Effect</i>	<i>Behaviour</i>	<i>Controls</i>	<i>Treatment</i>
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	<ul style="list-style-type: none"> ● Outlining of a control procedure to identify possible improper accesses; ● Report from the whistleblower system
				Loss of reputation	2) Early dissemination of data from press releases with a high degree of confidentiality	Code of Conduct and sanctions	

4.2 Phase 2: risk assessment

The second process phase is about assessing the behaviors linked to risk events and consists of the following sub-phases:

- a) *Risk analysis*: the *Risk Management Function* checks out the consistency between the information obtained from the offices and the methodology adopted.

b) *Risk measurement*: this sub-phase takes into consideration the value of “inherent” risk, that is, the extent of a risk before any treatment action is undertaken. Risk assessment is carried out using the *Control & Risk Self-Assessment (C&RSA)* method, which involves the same actors who identified risk events. Then the level of existing control reliability is checked; matching this latter with the value of inherent risks results in a level of *residual risk*, that is, the extent of risk remaining after its treatment.

Table 2: Risk analysis - Example

<i>Risk Area</i>	<i>Fraud Risk</i>	<i>Enablers</i>	<i>Cause (category)</i>	<i>Behaviour</i>	<i>Likelihood</i>	<i>Impact</i>	<i>Inherent Risk</i>	<i>Control effectiveness</i>	<i>Residual Risk</i>
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

c) *Risk weighting*: this sub-phase aims at identifying, through using specific parameters, the most recurring risks that also affect Istat’s strategic goals and/or the main organizational activities and structures. During the weighting phase priority risks and treatment actions are selected according to criteria set by the Head of Anti-corruption Management (i.e., cross-cuttingness or recurrence of risks; the value of inherent risk; sustainability of the treatment proposals). With reference to priority treatment actions, the offices in charge are expected to plan in detail while including the following information:

- treatment progress, that is, the level of implementation for any treatment action, from start to full accomplishment;
- outline of performance indicators and related targets;
- final output, that is, the result expected at a set time, aimed to reduce a risk;
- timetable for implementation;
- people in charge of – and actors involved in – cross-cutting treatment actions.

Here follow some examples of treatment action planning.

Table 3: Treatment action planning – example

General actions	State of implementation	Implementation phases and timetable	Implementation indicators	Accountabilities
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

Table 4: Treatment action planning – example

Specific actions	State of implementation	Implementation phases and timetable	Implementation indicators	Accountabilities
Outlining of a control procedure to identify possible improper accesses	To be formalized	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

4.3 Phase 3: treatment action monitoring and its integration with the performance system

The fraud risk treatment actions are designed with the participation of the managers in charge of the activities/processes related to the risks registered. The monitoring phase entails periodically asking such managers for information about the treatment action implementation/progress, the outputs achieved and the state of risk events. All priority treatment actions whose implementation is assigned to senior managers in charge of generating outputs are subject to monitoring; in case of cross-cutting actions the monitoring also mentions the coordination office.

Treatment actions contribute to the performance assessment for the senior managers in charge of risk preventing actions and for other staff involved.

5. Supporting tools: RiskinIstat

To build up, update and monitor the risk registers, Istat offices use a specific application named “RiskinIstat”, a tool supporting risk management through the setup of initiatives specifically planned. All process phases are *web-based*: every office can access according to its level of clearance (either read-only or full access) in order to ensure the traceability of the operations carried out, data security and the highest transparency of information. The application can generate a timely and straight-through reporting which allows authorized senior managers to entry and view, in a prompt and intuitive way, all needed information to manage the risks related to their offices, thus ensuring a regular update of the risk registers, the level of goal accomplishment and the different phases of the Risk Management process. The application allows for planning treatment actions related to priority risks; in this respect, detailed planning based on the so-called “Feasibility plans” is carried out, which locates actors, phases, lead-times as well as indicators for the outputs accomplished. Comparing these latter with related costs incurred allows to assess the effectiveness of treatment actions for “inherent” risks, as well as make appropriate amendments if needed, in order to reduce the overall level of “residual risk” as much as possible.