INTERNAL AUDITING AND FRAUD: HOW TO MANAGE FRAUD INFORMATION

One of the important links between internal auditing and occupational fraud is how the information is handled. This information falls into two categories—information that somebody decides to give to the organisation (e.g., whistleblowers, management, or the audit department) and information corroborated by investigation—that each raise unique questions of how to be processed and communicated. Discover an effective procedure, based on internal auditing skills, compliance program knowledge, and organisational experiences, for managing fraud information in the internal audit department.

PIERO MATRICIANI, CFE, CIA, CCSA
Audit Manager
Ferrovie dello Stato Italiano
Italy

Piero Matriciani leads the compliance auditing function and fraud investigation activities for the FSI Group. He is a member of the committee concerned with adequacy and observance of the compliance program for crime prevention, due to Italian law on corruption and other crimes against public institutions, public faith, and investors. Matriciani was previously employed as a tax and compliance inspector in public institutions management.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, re-published, modified, reproduced, distributed, copied, or sold without the prior consent of the author.
<table>
<thead>
<tr>
<th>Presentation Overview</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
<td></td>
</tr>
<tr>
<td>2. Just a few words about internal auditing and fraud</td>
<td></td>
</tr>
<tr>
<td>prevention</td>
<td></td>
</tr>
<tr>
<td>3. Handling of information on frauds by the Internal</td>
<td></td>
</tr>
<tr>
<td>Audit Department</td>
<td></td>
</tr>
<tr>
<td>• Acquisition of information on fraud</td>
<td></td>
</tr>
<tr>
<td>• Management of information relating to fraud</td>
<td></td>
</tr>
<tr>
<td>• Management of the database of information on fraud</td>
<td></td>
</tr>
<tr>
<td>• Dissemination of the Audit Final Report</td>
<td></td>
</tr>
<tr>
<td>• Management of the database of fraud schemes</td>
<td></td>
</tr>
<tr>
<td>4. About Internal Audit Department’s investigations</td>
<td></td>
</tr>
</tbody>
</table>

**Introduction**

It might not always be easy to identify the elements that link the internal auditing activity with frauds and sometimes misunderstandings can arise on this subject. The main goal of this paper is to portray the points of contact—and the operational boundaries—existing between internal auditing activities and frauds.

They are about: 1) fraud prevention, 2) handling of information on frauds, and 3) investigations carried out by the Internal Audit Department.

The discussion will be mainly focused on point 2). The relationship between internal auditing and frauds surely exists and it is specifically codified by the International Standards for the Professional Practice of Internal Auditing (SPPIA 1210.A2 -1).

“Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have
The expertise of a person whose primary responsibility is detecting and investigating fraud.”

In Ferrovie dello Stato Group (hereinafter “FS Group”) we use this definition of fraud: “Deceptive behaviour, carried out to obtain an unfair profit (for oneself or for others) to the detriment of others.”

A fraud has three essential elements: the perpetrator (as the author of the fraudulent behaviour), the deception (the behaviour or means through which someone misleads) and the victim, as the organization that suffers an undue damage or loss, or the society (broadly intended).

The internal auditing activity deals only with a particular kind of fraud—*occupational fraud*, which can be defined as “Fraud committed by someone who has an ongoing relationship with the company, fiduciary or—in any case—a qualified one”.

Internal auditing has to deal with occupational frauds—committed within the organization or having had support by employees—and this paper explains what internal auditing has to do (and is expected to), and how it has to be done (and is expected to).

**A Few Words About Internal Auditing and Fraud Prevention**

In general, how does the internal audit department contribute to preventing irregularities (including frauds) in running business activities? By assessing the internal control system in each of its components that are listed in the COSO Report:

- Control Environment
- Risk Assessment
- Control Activities
By checking the internal control system, both in its architecture (design of controls) and in its functioning (the concrete effectiveness of controls), the internal auditors learn if the controls in place are adequate (and effective) to prevent misconducts.

Through this kind of assessment, the top management of a company expects an internal audit department to:

- Assess and report internal control deficiencies.
- Assess and report key business risks.
- Provide control improvement recommendations.

With the general context clarified, we will shortly see how the internal auditing activity is able to prevent frauds specifically.

As everybody knows, frauds have three elements that can coexist: opportunity (as we all know, *opportunity makes the thief*), rationalization (the way oneself sees a fraudulent behaviour as a non-fraudulent behaviour), and pressure (the motivation or the incentive linked to the potential outcome of the fraud). The prevention of fraud requires action on each one of those elements.

Reducing the *opportunity* means tightening hard controls (such as the segregation of duties and functions, inspections, limits on proxies) and the main aim of the audit function is to evaluate controls, obviously including hard controls.

Regarding *rationalization*, what we can do? A fraud auditor and a fraud examiner would answer, “Improve the tone at the top.”
It’s hard to find a motivation for misconduct if there is a very strong, widespread perception of fraud intolerance and if penalties related to some kinds of frauds are very harsh and very well known (as well as the code of conduct).

An internal auditor (maybe more than a forensic auditor) would answer: improving many components of the internal control system, first of all control environment. That means spreading ethical values and a proper business culture, also giving workers a good example through management behaviour; training employees and doing an employee-background analysis when hiring.

Second, an internal auditor would answer: improving the related aspects of the control activities, such as the frequency of controls, which can lead to penalties and the depth of investigations usually performed.

Third, an internal auditor would answer: improving the related aspects of information and communication, including the fact of giving resonance to penalties and dismissals for fraud, or ad hoc campaigns.

With regard to pressure, it has to be considered that this factor changes with human needs.

As Maslow explained, when basic needs are satisfied, space arises for increasingly sophisticated needs that can be extremely diverse in the different hierarchical levels of an organization.

Thus, the incentive to commit fraud will be extremely different from one to another. For instance, a not-upright CEO can commit fraud without bringing home a penny. His relationship with the company is so strong that he could be motivated to commit fraud without expectation of a private
gain, simply for personal prestige. A not-upright doorman, with all the due respect, would never commit the same type of fraud.

Given the considerations above, it is impossible to set rules on how internal audit can act directly and relevantly on this issues.

Furthermore, internal auditing can help organizations in preventing fraud through performing fraud risk assessment (hereinafter FRA).

It’s like a bridge between who knows where the risks of fraud are, but has no power to prevent them, and who doesn’t know where the risk of fraud are, but has the power to prevent them, appropriately tuning the internal control system.

Regarding fraud risk assessment, it is useful to fix some general rules.
1. Risks of fraud must be considered as standalone risks. This because there is always a kind of reluctance to talk about fraud risks (sometimes it can lead to a dead end).
2. Risks are not red flags.
3. Risks are not lacks of control.
4. If these two different things are confused, there is a high likelihood of ending up in a loop with no way out; the chain of control will never have adequate results.
5. You always need a list of probable frauds, like a checklist, related to each business sector of interest.
6. Once fraud risk assessment is ended, it is necessary to assess the existing controls (preventive and subsequent) by checking each component of the COSO Report.
Handling Information About Fraud
As mentioned at the beginning, internal auditing has to deal with occupational frauds committed within the organization or having internal relief. At this point, it’s necessary to have a look at how internal auditing has to work and—more specifically—how it has to handle information and reports on frauds.

The handling of information on frauds, in compliance with SPPIA, should be reasonably structured on the following headings:

- Acquisition of information on fraud
- Management of information relating to fraud
- Management of the database of information on fraud
- Dissemination of the audit final report
- Management of the database of fraud schemes

The FS Group is currently going to emit an ad-hoc corporate policy concerning how to manage occupational fraud’s information, based on such elements.

Information on frauds can consist in reports coming directly from the reporter (blows) or found while performing audit activities in the Group.

In the first case, the Central Audit Department (CAD) of the parent company can receive reports on fraud either by someone within the company or by a third party. In the second case internal auditors (those belonging to each Internal Audit Department of the group), while performing their engagements, find information or elements generating suspicions of fraud (*information incidentally acquired*).

In any case, whatever is the source of reports, they have to be forwarded to the CAD to be managed centrally. The
reports will be classified as *confidential* and stored in electronic or paper archives.

After the receipt of those reports or the information incidentally acquired, the CAD has to deliver an opinion on their merits to avoid an unnecessary waste of time and resources. In case of direct reports, a preliminary assessment of reasonableness of the allegations set out is needed. Auditors have to evaluate two key elements:
- The credibility of the information
- The reliability of the informer

To assess the *credibility of the information* it is necessary to identify each element (data, value, parameter, reference, etc.) that may be subsequently compared with the corresponding elements identified from trusted sources. Given that, it’s always possible to resort to a specialized support by the appropriate company departments. In this phase the CAD can usefully consult the database of reports on fraud or the database of fraud schemes (which will be described later on).

At the same time, when the policy includes a list of red flags, auditors can check it and try to find any of them in the reported circumstance.

To assess the *reliability of the informer* it’s necessary to define his or her “profile”. Such activity can be run with different operating ways, depending on whether the report is anonymous or not.

In case of reports on fraud coming from a known informer, auditors will collect all the useful information (through the allowed channels) to reconstruct the profile of the informer and, if deemed appropriate by the audit team, try to enter in direct contact with the whistleblower.
The type of information collected includes:

- Personal details (name, age, sex, date and place of birth, residence, address, profession etc.)
- Existence of a qualified relationship, previous or actual, with the group
- Existence of family links with people whose employer is the group
- Existence of previous reports on fraud coming from the same informer
- Number of previous reports coming from the same informer that have been confirmed by investigations

When reports on fraud come from an employee of the group, auditors can ask for support from the Administration and HR Departments to acquire useful data when building the informer’s profile.

When reports of fraud are anonymous, auditors must try to define a hypothetical profile of the informer by analysing the writing style, editing, and terms used in the allegation. By assessing the credibility of the information and the reliability of the informer, the internal audit team is able to deliver an opinion on the report, such as “manifestly groundless” or “not manifestly groundless”.

When the allegation is considered manifestly groundless, no investigations have to be done and the report is directly stored in the database of reports on fraud.

In the second case, in accordance with SPPIA, the Chief Audit Executive (CAE) has to bring the report of fraud to the attention of the audit committee, together with a proposal for further investigations.

- Information on frauds must be stored in a specific database, together with a report summary sheet.
- These sheets shall include the following elements:
INTERNAL AUDITING AND FRAUD: HOW TO MANAGE FRAUD INFORMATION

- The date in which the CAD received the report
- The protocol number assigned by the corporate system
- The company/ies mentioned in the report
- The business process that is involved in the fraudulent hypothesis
- The type of possible fraud
- The opinion on report (manifestly groundless or not manifestly groundless)
- The eventual decision taken by the audit committee on the advisability of further investigations

Once received the assignment to carry out an investigation, the CAD must perform it in accordance with the provisions contained in the audit process manual of the group. The investigation must also be done in compliance with laws, regulations, and the international SPPIA.

The main features and limitations on the investigations carried out by internal auditors will be discussed later in this paper; in this context it suffices to say that the auditing activities are governed by several SPPIA and some Italian laws that restrict the range of action.

When the investigations confirm the fraudulent hypothesis (reports confirmed by investigations), the CAD—before submitting the final report to the intended recipients—must share its contents with the Legal and Compliance Department.

In compliance with the SPPIA, such sharing supports auditors in identifying the modes of communication of all the information pertaining to the detected violations of law (and those that might be regulatory offenses and generate corporate liability), to ensure that its contents do not lend themselves to harmful misunderstanding for the company.
The Practice Advisory n° 2400-1 (Legal Considerations in Communicating Results) states that: “Internal auditors should exercise caution when including results and issuing opinions in audit communications and workpapers regarding law and regulatory violations and other legal issues. Established policies and procedures regarding the handling of these matters and a close working relationship with other appropriate areas (legal counsel, compliance, etc.) is strongly encouraged.

“Internal auditors are required to gather evidence, make analytical judgments, report their results, and ensure corrective action is taken. Internal auditors’ requirement for documenting engagement records may conflict with legal counsel’s desire not to leave discoverable evidence that could harm a defense. […] These policies should include role definition and methods of communication.

“The internal auditor and corporate counsel should also foster an ethical and preventive perspective throughout the organization by sensitizing and educating management about the established policies.

“Internal auditors should consider the following [other recommendations included in the last part of the Practice Advisory], especially in connection with engagements that may give rise to disclosing or communicating results to parties outside the organization.”

Then, the Audit Final Report has to be sent to those who have the power to take appropriate measures. In this regard, the SPPIA n° 2440 (Disseminating Results) states that: “The Chief Audit Executive must communicate results to the appropriate parties. It means that the CAE is responsible for reviewing and approving the final
engagement communication before issuance and for deciding to whom and how it will be disseminated.”

Moreover, the SPPIA n° 2440-A1 and 2440-A2 say that: “The CAE is responsible for communicating the final results to parties who can ensure that the results are given due consideration. If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization the chief audit executive must:

- Assess the potential risk to the organization.
- Consult with senior management and/or legal counsel as appropriate.
- Control dissemination by restricting the use of the results.”

If the audit final report (for any particular reason and only for those profiles that relate to the company) should be transmitted outside the FS Group (as in the case of communications required by law), the CAE must first contact the CEO, because it is responsible for taking the appropriate decisions.

After completing the investigation, the results have to be evaluated with the aim either to define a new fraud scheme or to attribute it to a fraud scheme already surveyed. The database of fraud schemes is an electronic archive (accessible by authorized personnel only) in which the fraud schemes identified by the CAD at the end of each audit activity are stored.

Detecting a fraud scheme means identifying the architecture of fraudulent behaviour investigated and (if possible) identifying the corresponding fraud indicators (red flags).
A fraud scheme also represents a functional tool, useful to facilitate the evaluation of reports on fraud. Furthermore, it represents a helpful tool to identify fraudulent practices because the patterns of fraud repeat themselves over time, in the manner and sometimes in the individual who commits it (e.g., due to the role they cover within the organization).

The task of defining each fraud scheme is assigned to the audit team that conducted the investigation and its contents must be viewed and approved by the CAE.

**About the Internal Audit Department’s Investigations**

**Peculiarities in Comparison with Normal Audit Activities**

When dealing with occupational frauds, internal auditors have to behave in a specific way. There are some relevant features that are peculiar in respect to traditional audit activity.

**OCCUPATIONAL FRAUD INVESTIGATIONS DON’T ALLOW YOU TO DRAW GENERAL CONCLUSIONS**

The object of the investigation cannot be considered as a representative sample that will lead to general conclusions on the internal control system: it’s only a specific suspicious fact.

If the audit team employs samples while investigating, they have to be considered as non-representative sets of data.

In general, this type of data is collected because it is marked by a high degree of dangerousness (called a *targeted sample*), by a high concentration of red flags, and it is not representative of the general internal control system. Such data can be, for
instance, all the contracts concluded by the company in a certain year, or all the financial transactions in a specific period of time.

**OCCUPATIONAL FRAUD INVESTIGATIONS ARE CONDUCTED WITH A VERTICAL APPROACH**
In traditional audit activities we usually use a horizontal approach that looks at each phase of a process, considering many items in each phase. In fraud investigations the scope of observation is restricted to each specific fact or event, and it has to be examined from cradle to grave.

**OCCUPATIONAL FRAUD INVESTIGATIONS LOOK AT CONTINUOUS POINTS OF CONTROL**
Traditional audit activities are performed focusing on a particular process and assessing the critical issues of its development. So, the results might consist in the identification of a set of discrete points of control that can be adequate or inadequate. Differently, a fraud audit detects continuous points of control because it is very important to examine an item in each step of its progress and evaluate its consistency and its coherence with the previous one.

**FRAUD INVESTIGATIONS DO NOT INVOLVE MANAGEMENT AGREEMENT ON RESULTS**
Traditional audit activities end up sharing the results of the internal assessment with the appropriate management in order to agree to its contents. In the case of fraud audits, sharing the contents of the audit final report could be dangerous or meaningless.
The Conflict Between Employer’s Interest and Workers’ Right

The internal audit department has also to comply with laws and regulations while performing its engagement. In this respect, in the Italian legal system, there is a tough balancing act between two competing claims: on the one hand, the right of the employer to exercise control over its employees to safeguard company assets but on the other hand, the right of the worker to not be offended in his dignity, freedom, and privacy.

The Italian laws on workers’ protection are very strong and restrictive, but similar principles are in force (in a lighter manner) also in the other European countries. While investigating, the practical consequences of those rules are that an internal auditor cannot use remote controls on workers.

VIDEO SURVEILLANCE IS LIMITED IN SPACE AND TIME

It is limited in space because it can be installed only if needed by organizational, productive, or safety reasons and by prior agreement with the company trade union representatives. It shall be indicated by a visible sign, but cannot be installed in reserved locations or places not pertaining to work.

Video surveillance is also limited in time: recorded images must be stored for a limited period of time; integrated systems must adopt specific security measures to be audited by the Authority for Personal Data protection and any intelligence system must be compulsorily signalled to the that Authority.
The Authority for Data Protection, in its “Guidelines for email and internet”, stated that corporate custom emails have the nature of private correspondence, so its secrecy is inviolable.

Therefore, the Authority softened its position by adding that if the company has defined a policy (pointing out the legitimate controls it intends to exercise) and if this policy is clear, properly publicized, and regularly updated, some controls on the corporate email of the employees are possible.

The same Authority decided to apply those rules to the faculty of the employer to control the Web pages visited by its workers.

Furthermore—within these limits—possible controls rarely can be deep enough to let auditors understand something, or to provide strong evidence of something.

Use of security guards is possible only with the purpose of safeguarding company assets.

Frisks of workers (also called *searches on worker’s body*, or *personal perquisitions*) are forbidden, except from cases where they are essential to the safeguard of corporate assets.

In such cases, frisks are possible only if they are carried out at the exit of the workplace, preserving the dignity and privacy of the employee, and using automatic methods referred to the community or groups of workers.

* An extreme example is the national mint, where coins are produced and controls on workers are clearly very important.

Anyway, frisks modalities must be agreed with the trade union representatives.
– In addition to these rules, frisks cannot be done anonymously.
– The law provides that names and specific tasks of supervision personnel that must be communicated to workers if they are concerned about their rights.