SETTING UP AN ANTI-FRAUD CONTROL PLAN

How mature is your organisation in mitigating fraud risk? Learn how to develop a fraud risk governance framework, based on the three lines of defence model, and to make sure that this framework is functioning as intended by putting in place an anti-fraud control plan.

PATRICK RISCH, CFE, CIA, CCSA
Head of Fraud Prevention & Detection
BNP Paribas Fortis
Belgium

Patrick Risch has more than 20 years of experience in the financial services sector, mainly focused on internal auditing and fraud risk management. In his current position, he heads the Fraud Prevention & Detection department within BNP Paribas Fortis and is responsible for setting up and implementing a framework for fraud prevention (policy setting, raising awareness, giving advice, reporting on fraud risk exposure) and fraud detection. Risch is also a President of the Belgian Chapter of the Association of Certified Fraud Examiners.

“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.
### SETTING UP AN ANTI-FRAUD CONTROL PLAN

<table>
<thead>
<tr>
<th>Introduction</th>
<th>NOTES</th>
</tr>
</thead>
</table>

#### Purpose of the Presentation

In the elaboration of an anti-fraud policy, obviously attention is paid to the definition of *fraud* and the dos and don'ts for employees. But this is also the ideal opportunity to reflect and decide on the allocation of the responsibility for fraud prevention, fraud detection, and fraud case management. By allocating these responsibilities in accordance with the “three lines of defense” model, you ensure that the various operational risks are approached consistently throughout the organization, and that the successive steps in the control environment of this model can function fully. An important point is that at regular intervals, time is taken to determine whether the responsibilities are taken up adequately by the different first line of defense entities. An anti-fraud control plan allows you to do this in a structured and formalized way.

**BNP Paribas Fortis**

BNP Paribas Fortis is the first bank in Belgium, offering a comprehensive package of financial services to private and professional clients, wealthy individuals, corporate clients, public entities, and financial institutions through a multi-channel network.

In Belgium, more than 17,000 staff members service 3.6 million retail customers and 35,000 corporate clients.

BNP Paribas Fortis has been part of the BNP Paribas Group since 2009.
<table>
<thead>
<tr>
<th>Fraud Risk Framework</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The Need to Manage Fraud Risk</strong></td>
<td></td>
</tr>
<tr>
<td>Fraud is often a difficult issue to talk about. In fact, it is typically one of those topics that you try to hide by just not talking about it.</td>
<td></td>
</tr>
</tbody>
</table>

And actually, there is some truth in it: if you don’t talk about fraud, you won’t look for fraud, and you will have less fraud in your accounting books. Unless a third party—a customer or a supplier—has been harmed, you might never find out. The fraudulent loans are booked along with the bad loans, and simply increase our bad debt ratio. When travel expenses increase, we will just ask for a bigger budget next year.

This leads us to the 5 percent loss for a typical organisation, which is nice to quote, but remains a statistic and, even though it is based on real incidents, it’s too easily put aside as a theoretical approach. When you go and look at the real victims, things become more threatening.

At the end, this is why it is so important to talk about fraud: to know the real cost of it, and to be able to take appropriate action.

It is only by demonstrating the real cost of fraud that you can convince the target-oriented business managers of what’s in it for them: how many loans do they have to sell in order to win back the losses of one fraudulent loan? This means that by protecting themselves against fraudsters, in fact they are working on their business targets indeed.
Why Do People Commit Fraud?

The question of why people commit wrongful acts is as old as the old scriptures. And if we are honest with ourselves, most of us will have to admit that we can imagine a situation in which we would commit such an act. It is a folk wisdom that everyone has his price, although the height of this price may differ.

Folk wisdoms often are caricatured and simplified representations of reality; nevertheless, let us go a bit further that way.

*Bad to the bone* is one of them, and *too good for this world* is somehow the opposite.

Translated to the reality of an average population, this means that you will find some people who are always looking for an opportunity, without any consideration for others, rules, ethics, and so on. *Some people are dishonest all of the time.*

Conversely, you have people that will obey to the rules up to the point where it becomes absurd. The red traffic light in the desert that remains red for half a day, the typical whistleblowers. *Some people are honest all of the time.*

These two groups of people are extremes of a whole continuum, where *most people are honest some of the time and some people are honest most of the time.*

Most people let their behaviour largely depend on what is happening around them: what are the others doing, are there controls in place, how does the “authority” react, how badly do I need the money …

---

1 Quotes from Tommie Singleton, Ph.D., University of Alabama
Both extremes probably understand each other and probably have big difficulty understanding the large category in between, because people in this category can so easily be influenced.

Unfortunately, we cannot exclusively hire “good people”: not only is it difficult to distinguish them, there are probably too few of them to give every employer a chance. However, when we look at this given from a perspective of fighting fraud, it can lead us to a few useful considerations:

- We have to avoid hiring “bad people.” This might seem obvious, but the importance hereof increases when we take into account the impact they can have on our large situational category. This means that thorough pre-employment screenings are important. Calling a previous employer is not a luxury. It is obvious that we will not succeed in avoiding all miscasts—after all, they are masters in deception—but it is clear that every villain we keep outside is a gain for our organisation.

- Even though “good people” seem to flourish in risk and control departments, we should not isolate them in that environment. When they are spread throughout the organisation, they can influence the situational people around them.

- And finally, the situational people need, above all, a well-developed control environment, with an organisational culture that is imbued by the need for integrity and with an example-setting management style.

To set up this healthy control environment, it is important to bear in mind the three drivers that bring someone to commit a fraud, and these are of course the elements of our well-known fraud triangle:
<table>
<thead>
<tr>
<th>SETTING UP AN ANTI-FRAUD CONTROL PLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Opportunity: a sound internal control system helps to reduce the risk of errors, and subsequently the risk of fraud.</td>
</tr>
<tr>
<td>• Pressure: balanced target setting helps to reduce the risk of unwanted activities focused on achieving impossible targets.</td>
</tr>
<tr>
<td>• Rationalisation: an organisational culture that cherishes integrity, compliance, and team spirit increases the threshold to colour outside the lines.</td>
</tr>
</tbody>
</table>

**NOTES**

- Opportunity: a sound internal control system helps to reduce the risk of errors, and subsequently the risk of fraud.
- Pressure: balanced target setting helps to reduce the risk of unwanted activities focused on achieving impossible targets.
- Rationalisation: an organisational culture that cherishes integrity, compliance, and team spirit increases the threshold to colour outside the lines.

**Steps in Fraud Risk Management**

We’ve just learned that most probably in every organisation we will have people who are tempted to defraud us at a given moment in their career. Whether we like it or not, this makes it necessary to manage the operational risk called “fraud”. Of course, any comparison is lame, but I like to compare the management of this fraud risk with healthcare.

The first step is prevention. From all perspectives, this is the best approach: in general, it is the cheapest way, for you as well as for society, and you don’t get actually sick.

However, you have to be aware that most of it you have to do yourself: don’t smoke, don’t drink too much, have some exercise … in a few words, a healthy lifestyle. Healthcare professionals can help you do this (e.g., during a regular check-up), but it remains your responsibility.

When you get ill anyhow, you are glad that you can ask a specialist to look after you, and to take care of you. Even though he will do what he can to help you, this will cost you more, it will take a lot of your valuable time and most probably some scars will remain.
Afterwards, a physiotherapist helps you to revalidate and to take up your life. Or, in case things don’t turn out well, an autopsy can show what went wrong, and this knowledge can help others to avoid getting in the same painful situation.

Likewise, in fraud risk management, prevention is the best, and the cheapest way. But, here as well, management has to take up their responsibility to ensure that the entity remains healthy. Of course, fraud professionals can be of a great help, but it remains the responsibility of the management to take action: assessing the risk, putting controls in place, … making sure the organisation is well armed against fraud risk.

When an alleged fraud incident takes place, a professional inquiry will have to reveal what actually happened, to determine the losses, responsibilities, and to decide upon guilt and innocence. This inquiry will most probably have to be carried out within a very strict regulatory or legal framework.

Once the fraud scheme has been unravelled, the appropriate accounting corrections have to be booked, disciplinary actions might be appropriate and, because we do not want this to reoccur, enhancements to the system of internal control might be necessary.

**Fraud Risk Management: Putting It into Practice**

In any organisation of considerable size, and in particular in a highly regulated sector such as financial services, you can find formal policies on almost everything, from “gifts and entertainment” to “personal transactions”. So, why take the effort to write down yet another policy?
The consequences of a fraud incident can be enormous, financially and with respect to the reputation of the organisation. Besides this, we’ve explained before that the majority of the people can and will be influenced by the environment. A formal statement by the highest governing bodies in the organisation to this respect has an impact, provided—of course—that these nice words are not contradicted by the behaviour of the top.

In fact, there is only one thing worse than not having a clear anti-fraud statement by the highest authority in the organisation … and that is having a beautiful statement overruled by any person with authority. When it comes to adopting bad habits, most people learn very quickly.

On the risk of fraud, there are no winners, and no flowers at the finish line. This means that, even though everyone is usually very interested in the juicy details of individual cases, often managers are reluctant to take up responsibility to take action … and so nothing happens.

Therefore, besides stating a zero tolerance principle (even though this is very important indeed), an anti-fraud policy should in particular determine an appropriate governance and clearly define the roles and responsibilities in the fraud risk management process. In general, two contradictory opinions steer the discussion on who owns fraud risk and subsequently bears the final responsibility on the management of this risk.

• On the one hand, the internal control theory places this responsibility, as any other responsibility, with management at the different levels of the organisation and with all staff members. The rationale behind this is that setting up a dedicated
department will only lull regular business management to sleep, leaving them in their comfort zone with the knowledge that fraud risk is being taken care of.

- On the other hand, specialists might claim that fraud is a very specific risk, and that you cannot expect your average manager or employee to fully understand the risk well enough to investigate fraud suspicion, to assess the risk, and to work out the necessary preventive and detective controls.

Because of these specificities, depending on the organisation, the responsibility for managing fraud risk can be at different locations and levels or can be, within one organisation, allocated to different entities: the auditing department, compliance, safety, human resources... Sometimes this is a well-thought-out decision (e.g., for practical reasons), and sometimes this is “because it has always been that way”.

THREE LINES OF DEFENCE
With respect to risk governance within organisations, the three lines of defence model has been increasingly applied over recent years. In brief, it can be explained as follows:

- As a first line of defence, the organisation’s operational management has ownership, responsibility, and accountability for assessing, controlling, and mitigating risks.
- As a second line of defence, the risk management function (and also other supporting functions like compliance, quality) facilitates and monitors the implementation of effective risk management practices by operational

---

2 Source: [www.eciia.eu](http://www.eciia.eu)
management and assists the risk owners in reporting adequate risk-related information up and down the organisation.

- As a third line of defence, the internal auditing function will, through a risk-based approach, provide assurance to the organisation’s board and senior management, on how effective the organisation assesses and manages its risks, including the manner in which the first and second lines of defence operate.

FRAUD AND THE THREE LINES OF DEFENCE
To ensure a proper management of fraud risk, and to maintain coherence with other risk management processes, alignment of the different components of fraud risk, as explained before, with the three lines of defence framework is recommended.

FIRST LINE OF DEFENCE
The management of the operational entities are most familiar with the processes and their weaknesses, the products and their risks, and customers and staff members and their particularities.

And when it comes to fraud, the products, customers, and staff that are almost always involved in one way or the other. Also, they are usually the first who can react to an incident and they manage the budgets that have to be addressed to implement mitigating measures.

So it is obvious that they have to feel concerned and implicated. And this only can be done by giving them also the responsibility to do so.
The following table shows an overview of the different focus areas related to fraud risk management, fitting with the overall first line of defence approach.

<table>
<thead>
<tr>
<th>Prevention and Early Detection</th>
<th>Case Management</th>
<th>Repair and Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Install a culture of fraud risk awareness</td>
<td>• Ensure that a fraud alert line is installed and known to everyone in the organisation</td>
<td>• Make the necessary accounting entries and register losses</td>
</tr>
<tr>
<td>• Provide fraud awareness training to staff</td>
<td>• Set up a process for the management of fraud cases</td>
<td>• Reimburse customers</td>
</tr>
<tr>
<td>• Include fraud risk in the overall risk assessment process</td>
<td>• Investigate all fraud cases in a professional and objective way</td>
<td>• Take disciplinary action towards the perpetrator</td>
</tr>
<tr>
<td>• Incorporate fraud preventive and detective controls in the operating procedures: segregate duties, monitor adherence to policies and procedures, etc.</td>
<td></td>
<td>• Take legal action against the fraudsters</td>
</tr>
</tbody>
</table>

Taking into account this wide area of responsibilities, it is a good practice to have, within different operational entities of the organisation, a person formally designated by the management team as a Mr or Ms Anti-Fraud. The main purpose of this function is to keep the story of fraud alive in the entity: to coordinate and prioritise all fraud-mitigating activities in the organisation, to maintain contact with counterparts in other entities and if necessary within other organisations, and to ensure that a proper consequence management is put in place.

In particular the issue on where to allocate the operational responsibility for investigating
internal and external fraud cases is subject for discussion.

From a governance perspective, it is a strictly first line of defence activity, subject to policy and oversight by the second line, and periodic control by the third line.

Nevertheless, it is obvious that, regardless of whether the fraud incident is internal or external, the inquiry has to be carried out independently and objectively, taking into account the following considerations:

* Investigating a fraud case, in particular an internal fraud case, requires specific skills and competences.
* In an internal fraud, the fraudster or an accomplice might try to destroy or falsify evidence, or management might try to cover up its responsibility in not discovering the fraud earlier.
* External fraud cases are often facilitated by a non-respect of procedures. Subsequently, staff members or managers could be tempted to conceal their mistakes, thus hindering the learning process that should follow any incident.
* Confidentiality is required until the incident has been fully investigated and a conclusion has been reached. This is in particular the case in internal fraud cases.

Again, different approaches are possible, with the most obvious leading to a distinction between internal and external fraud:
SETTING UP AN ANTI-FRAUD CONTROL PLAN

* External fraud is often a part of the business-as-usual processes, and the risks are usually well known to the operational management. Subsequently, the investigation of these incidents, and the ex-post analysis, can be treated adequately in the operational department itself or in a closely related permanent control department.

* Taking into account the specificities and the need for confidentiality, internal fraud incidents will probably be investigated in a dedicated competence centre (eventually jointly with other entities), or even by third-party investigators.

NOTES

SECOND LINE OF DEFENCE
It is the responsibility of the second line to ensure an adequate and consistent approach to fraud risk throughout the organisation, to maintain oversight, and to report on fraud risk and on the state of the organisation’s defence system against fraud risk.

<table>
<thead>
<tr>
<th>Prevention and Early Detection</th>
<th>Case Management</th>
<th>Repair and Remediation</th>
</tr>
</thead>
</table>
| • Oversight on fraud risk management activities within the organisation  
  • Guidance, advice, and recommendations to line management  
  • Fraud risk assessment methodology and oversight on roll out  
  • Knowledge centre on fraud risk | • Report on fraud risk exposure | • Post mortem analysis and recommendations to line management  
  • Monitoring evolution of fraud-risk exposure |

©2014

2014 ACFE European Fraud Conference
## Setting up an Anti-Fraud Control Plan

In the first place, this will be done by setting the policy and communicating and enforcing it throughout the organisation. Besides that, there will be regular contacts with business management, to guide them and assist them in setting up the framework.

To summarise, the purpose is not to take over any responsibility from line management with respect to fraud risk, but to support management in setting up an adequate fraud prevention and protection framework.

Depending on the size of the organisation and of the fraud risk exposure, this second line against fraud risk can be a part of the risk or compliance department, or it can be a dedicated entity. However, in either case visibility in the organisation is important.

### Third Line of Defence

The role of the internal audit department is to give assurance that fraud risk is managed adequately:

- First and second lines are functioning properly.
- A fraud prevention framework is in place.
- Any specific incident is investigated in a professional and independent way.

In this view, internal audit should avoid starting up its own inquiry, apart from ensuring that the first line has dealt with the issue adequately.

Given the extensive powers and authority usually given to a fraud investigator, taking into
account the strict regulatory framework and the possible reputational impact of an inadequate case management process, it is not a luxury to make sure that this process is functioning as intended.

<table>
<thead>
<tr>
<th>Prevention and Early Detection</th>
<th>Case Management</th>
<th>Repair and Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide assurance to the organisation’s board and senior management that fraud risk is managed in an effective way by the organisation.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It is obvious that, when a fraud incident has—or could have had—serious financial or reputational consequences, the second and even the third line of defence will want to have their say at a certain moment. Nevertheless, they should restrain from intervening actively in the first line of defence processes; indeed, by doing so they would compromise their independent view on the fraud-mitigating activities.

They should approach the incidents from their own perspective (i.e., to maintain oversight over the risk control activities and to give assurance to the highest governing bodies of the organisation).

The IIA’s International Standards for the Professional Practice of Internal Auditing refer to fraud in the following paragraphs:
### Anti-Fraud Control Plan

Once roles and responsibilities regarding fraud risk management are fully and clearly established, controls can be put in place to give assurance that all mitigating activities are covered and that the system is functioning as intended.

The second line of defence will put controls in place verifying that the first line of defence control activities actually take place according to the standards, and that the governance of fraud risk management in the organisation as a whole is implemented as intended.

The following tables show an overview of how these controls could be worked out for some of the responsibilities of the first and the second line.
## Setting Up an Anti-Fraud Control Plan

### First Line of Defence

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Control</th>
<th>Periodicity</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install a culture of fraud awareness</td>
<td>Fraud risk is a mandatory topic on the agenda of the management team meetings</td>
<td>Annually</td>
<td>Review minutes of the meetings</td>
</tr>
<tr>
<td>Provide fraud awareness training to staff</td>
<td>Every newcomer in the organisation has received a basic anti-fraud training.</td>
<td>Quarterly</td>
<td>Compare list of newcomers with attendees to training</td>
</tr>
<tr>
<td></td>
<td>Every staff member receives periodical refresher training.</td>
<td>Annually</td>
<td>Compare attendance list with payroll</td>
</tr>
<tr>
<td></td>
<td>Every new people manager receives a dedicated training on professional ethics and fraud.</td>
<td>Quarterly</td>
<td>Compare list of new people managers with attendance list</td>
</tr>
<tr>
<td>Improve internal control</td>
<td>Each internal fraud incident is reviewed by a multidisciplinary working group.</td>
<td>Annually</td>
<td>Compare list of incidents (extract case management tool) with minutes working group meetings</td>
</tr>
<tr>
<td></td>
<td>External fraud incidents above a threshold (individually or cumulative according to fraud type) is reviewed by a multidisciplinary working group.</td>
<td>Annually</td>
<td>Compare list of incidents (extract case management tool) with minutes working group meetings</td>
</tr>
</tbody>
</table>

### Second Line of Defence

<table>
<thead>
<tr>
<th>Responsibility</th>
<th>Control</th>
<th>Periodicity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversight on fraud risk management activities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install a culture of fraud awareness</td>
<td>A fraud risk manager, with sufficient authority, has been appointed formally in the first line of defence.</td>
<td>Annually</td>
</tr>
<tr>
<td>Provide fraud awareness training to staff</td>
<td>An adequate common body of knowledge has been defined for staff members and managers.</td>
<td>Annually</td>
</tr>
<tr>
<td></td>
<td>Training material and trainings include CBOK</td>
<td>Annually</td>
</tr>
<tr>
<td>Include fraud risk in the overall risk assessment process</td>
<td>The methodology for fraud risk assessment is implemented in the annual risk assessment exercise. In the assessment, the different types of fraud (asset misappropriation, corruption, fraudulent statements) are evaluated.</td>
<td>Annually</td>
</tr>
<tr>
<td>Fraud risk assessment methodology and oversight on roll out</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Conclusion

Fraud risk is too important to ignore. Not only can the losses be significant, but the reputation risk is very important as well, in particular for a financial institution. This brings forward the need for a dedicated framework in order to mitigate this risk throughout the lines of defence of the organisation.

In this perspective, an entity in the second line of defence for which fraud risk management is the core business is a good practice. Without taking over any responsibility, this entity can give guidance to the organisation’s management with respect to fraud risk, and monitor the organisation’s exposure and mitigation activities.

A dedicated control plan monitors respect for the policy by all the stakeholders in the organisation.

The combination of these elements forms a complete and proactive approach to mitigate fraud risk and ensure that management at all levels of the organisation is fully aware of the risks. Of course, this does not guarantee a fraud-free organisation. However, it prevents giving fraudsters unnoticed and unrestrained access to your assets.