Over the recent years, several companies have been fined for compliance breaches, in France and around the world.

It is a growing concern for company directors and shareholders, as sanctions and repercussions are becoming increasingly severe.

How can the risk of sanctions be averted? How can companies safeguard their reputation? What control procedures can be implemented to do so? Who should be appointed as Chief Compliance Officer? Clients are increasingly asking these questions.

While the US (Foreign Corrupt Practices Act), and the UK (Bribery Act) are ahead in terms of regulatory compliance, other countries are also preparing to enforce compliance rules, including France with the Sapin II legislation.

Compliance is a complex, multi-faceted issue and all aspects need to be considered. From April to June 2016 KPMG’s Risk Consulting team surveyed over 150 listed and unlisted industrial companies to obtain an overview of regulatory compliance in France.

We would be happy to have the opportunity to discuss these issues further with you. We wish you a pleasant reading.

Sylviane Hautin
Partner
Risk Consulting
### Contents

<table>
<thead>
<tr>
<th>Part</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Scope of compliance</td>
<td>5</td>
</tr>
<tr>
<td>Origins of compliance</td>
<td>7</td>
</tr>
<tr>
<td>Stakeholders</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Chief Compliance Officer’s Profile</td>
<td>11</td>
</tr>
<tr>
<td>Chief Compliance Officer’s Role</td>
<td>13</td>
</tr>
<tr>
<td>3</td>
<td>16</td>
</tr>
<tr>
<td>Chief Compliance Officer’s Tools</td>
<td>17</td>
</tr>
<tr>
<td>Interaction with risk management</td>
<td>19</td>
</tr>
<tr>
<td>Improvements in compliance</td>
<td>21</td>
</tr>
<tr>
<td>Conclusion</td>
<td>23</td>
</tr>
</tbody>
</table>
If compliance is defined broadly as meeting regulatory and legal requirements, its scope is far-reaching. It can encompass all aspects of business, including legal affairs, human resources, business processes, accounting, tax and the environment.

Clearly, the compliance function cannot be made responsible for all the regulatory requirements incumbent upon groups in their business operations.

In order to delimit the reasonable scope that could be entrusted to the compliance function, we asked our survey respondents what they included in their definition of compliance.

Our survey found that over half of our respondents included the following areas in their compliance scope: anticorruption, conflicts of interest, ethics, fraud, antitrust law, and information security. These involve both external constraints on groups, and “soft law” commitments made spontaneously, for instance as part of a charter of ethics or anticorruption procedure.

That being said, it would not be sufficient to limit the compliance scope to these areas. Although they can form the groundwork on which a compliance programme is built, these areas do not reflect the full extent of a compliance programme.
Companies that consider themselves relatively mature in terms of compliance issues, have extended the responsibility of the compliance function to specific matters. This reflects their experience with incidents, constraints and even sanctions already endured due to their size and international presence, or regulatory requirements specific to their business.

Most often, extending the scope of responsibility entails drawing up a non-compliance risk map to highlight the sensitive issues to be addressed by the compliance function.

This appears to be the most effective means of assisting groups in extending the scope of the compliance function beyond its primary areas of intervention. The main purpose of the compliance function being to reduce groups’ non-compliance risk by implementing appropriate measures.

**Key points**

- There is no single compliance scope or standard applicable to all companies.
- However, compliance systematically addresses anti-corruption, conflicts of interest, ethics, fraud, antitrust law, and information security.
- Drawing up a non-compliance risk map is best practice, making it easier for companies to focus on priority compliance matters.

**Origins of compliance**

Examining why companies decide to appoint a Chief Compliance Officer (CCO), has provided useful information on the main drivers for setting up the compliance function.

51% of those surveyed cited the increasingly complex and restrictive plethora of regulatory obligations as the main reason.

High-profile media coverage of increasing incidences of non-compliance, with severe financial repercussions, have also prompted companies to set up compliance processes and measures.

However, we found that in over 20% of cases, our respondents do not approach compliance from the regulatory angle alone. They see it as an integral part of a broader approach to risk management encompassing foresight, prevention and management.

To a lesser extent, some companies stated that they had set up a compliance programme to meet the requirements of their main clients and/or partners. It is likely that such requirements will increase in coming years, particularly for companies operating in the United States. Indeed, the growing number of compliance measures taken by various economic players, some to a very advanced degree, naturally incite them to demand the same level of compliance from their partners.

This virtuous cycle is perfectly in tune with developments in other areas of risk management. For instance, a parallel could be made with internal controls. The 2013 COSO IC Framework encourages groups to inquire about the control measures implemented by their subcontractors.

**Main drivers for setting up the compliance function**

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Main Drivers</th>
</tr>
</thead>
<tbody>
<tr>
<td>51%</td>
<td>Regulatory obligations</td>
</tr>
<tr>
<td>22%</td>
<td>Risk management</td>
</tr>
<tr>
<td>15%</td>
<td>Already in place in the group</td>
</tr>
<tr>
<td>11%</td>
<td>Required by clients and/or partners</td>
</tr>
</tbody>
</table>

**Why the compliance function is set up?**

- **“Regulatory pressure.”**
- **“We were heavily fined recently.”**
- **“A proactive approach to improving compliance risk management.”**
- **“Pressure from our international clients.”**

---

**Sapin II (French law): an opportunity to define or review the compliance scope**

1. **Integrated approach to risk**
   - Draw up a risk map, defining non-compliance risks.
   - Set up and oversee the arrangement for non-compliance risk management.

2. **Compliance measures**
   - Adopt a code of conduct describing behaviour to be avoided.
   - Set up an internal whistleblowing mechanism.

3. **Reinforce transparency**
   - Set up internal and external accounting control procedures.

4. **SAPIN II ACT:**
   - Set up a compliance programme.

5. **Training plan**
   - Train the company’s senior managers and employees that are most exposed to risk.

6. **Sanctions**
   - Set up a discipline policy.

7. **Internal Control**
   - Establish an internal evaluation and control system for implemented measures.
Two observations emerge:

• Compliance is a necessity for all companies, and many have already implemented measures to varying degrees.
• Setting up a “preventive” compliance programme costs much less than incurring sanctions.

To conclude, compliance should reflect the maxim “better safe than sorry”. Best practice is for companies to be prepared, by conducting an analysis of risk.

Key points

• All companies, regardless of size or industry, are concerned by compliance.
• One in five survey respondents had been sanctioned for non-compliance, leading the respondent to set up a compliance programme at a much lower cost than the sanctions incurred.
• The ability to demonstrate that preventive measures are in place can minimize sanctions in the event of an investigation.

Did you know?

From 2010 to 2016, several French companies were sanctioned:

For bribery/corruption: Almost fifty European companies were heavily sanctioned. Fines totalled nearly €4 billion.

10% of the companies were French, accounting for €1.5 billion in fines.

For antitrust: The European Commission levied over forty fines on European companies. Fines totalled nearly €16 billion.

43% of the companies were French, representing over €1 billion in fines. No industry was spared.

For export controls, sanctions and embargos: over 60 European companies were fined, particularly by the Office of Foreign Assets Control (OFAC), with fines totalling €3 billion.

40% of the total fines applied to three French companies, which together incurred €1.1 billion in fines. The main industries affected were banking, energy, and transport.
Chief Compliance Officer, hereinafter referred to as CCOs, are responsible for enforcing company compliance with the laws, regulations and internal policies assigned to them. They play a key role in defining, setting up, monitoring and controlling company compliance systems for all areas of business. They can also provide guidance if non-compliance is suspected.

Chief Compliance Officer: Profile and Role

### Chief Compliance Officer’s Profile

When asked for human qualities were most important in a Chief Compliance Officer, most participants mentioned being a good communicator and educator. Beyond the merely "technical" aspects of their job, CCOs must provide guidance and educate directors, employees, and all other stakeholders regarding compliance issues, risks, and solutions.

One in two respondents felt that academic credentials alone were not enough for CCOs. The skills required for the job are learned through experience, grappling with real-world challenges. Accordingly, only 40% of those surveyed cited knowledge of law or compliance as essential requirements for a CCO.

A corresponding percentage cited risk management skills as necessary, since CCOs are in charge of managing compliance risk.

### Who is responsible for compliance?

- 64% Chief Compliance Officer
- 14% Chief Legal Officer
- 11% Company Secretary
- 11% Other

### CCO educational background

- Technical / Engineering: 46%
- Finance: 27%
- Legal: 10%
- Business: 8%

### Technical knowledge required of a CCO

- Expertise in compliance and law: 40%
- Knowledge of group operations: 27%
- Risk management: 21%
- Communication: 10%

Although most companies stated having specifically appointed a Chief Compliance Officer, others entrust the responsibility to the Chief Legal Officer or Company Secretary. The compliance function is almost always at head office level, reporting to Executive Management in 68% of cases, illustrating the importance assigned to it.
Survey responses also reveal that CCOs or their counterpart:

- Have over 15 years of professional experience in 81% of cases. Of these, 60% have at least five years of experience in compliance. This degree of experience appears necessary in order to firmly grasp the issues and be able to manage them with insight throughout the group.
- Are from very diverse backgrounds, although a clear majority studied law (46%) or finance (27%).

"CCOs need to be discreet, diplomatic and good educators – three essential qualities."
Chief Compliance Officer
Automobile industry

Key points

- Most of our panel use the title «Chief Compliance Officer» for the person responsible for compliance.
- Over 50% of CCOs have over five years of experience in compliance.
- Legal knowledge combined with communication and skills as an educator are essential qualities for this position.

Chief Compliance Officer’s Role

Compared with other corporate functions, for many companies, compliance is a recent, even very recent, addition. We have therefore endeavoured to determine how it is positioned in relation to other departments and functions with clearly-defined scopes of responsibility.

Our survey revealed that the CCO works and interacts with many corporate departments. Those most commonly mentioned were:

- the legal department, which works closely with the CCO particularly on antitrust and anticorruption matters;
- human resources, which participates, for instance, in matters concerning the code of ethics; and
- sales and finance, both of which are crucial to an effective compliance programme.

Departments that work with regulatory compliance

On the other hand, the departments mentioned least were procurement and communication:

- The low number of responses indicating collaboration with procurement is surprising since, like sales, it interacts extensively with external third parties. It is therefore highly exposed to non-compliance risk such as ethical breaches and corruption. Most CCOs who stated that they interact regularly with procurement were from companies that had been fined in the past.
- The finding that the communication department has limited interaction with compliance confirms another observation for France: 70% of survey respondents stated that they had no formally-defined communication plan for their compliance programme. This is in stark contrast with the United States, where public relations are closely tied to compliance. Companies will have to make rapid progress on this point.

On the other hand, the departments mentioned least were procurement and communication:

- The low number of responses indicating collaboration with procurement is surprising since, like sales, it interacts extensively with external third parties. It is therefore highly exposed to non-compliance risk such as ethical breaches and corruption. Most CCOs who stated that they interact regularly with procurement were from companies that had been fined in the past.
- The finding that the communication department has limited interaction with compliance confirms another observation for France: 70% of survey respondents stated that they had no formally-defined communication plan for their compliance programme. This is in stark contrast with the United States, where public relations are closely tied to compliance. Companies will have to make rapid progress on this point.
Although the position of CCOs can be measured by their interaction with other corporate departments, another interesting indicator is their involvement in the “life” of the company.

Most companies surveyed have also set up a company audit committee, whether to meet legal requirements or to encourage more effective corporate governance. For 59% of them, the CCO participates in the audit committee, illustrating the keen interest of directors and their perception of compliance-related issues.

Other interesting findings:

- One in two CCOs is a member of the Executive Committee or otherwise reports to Executive Management if not a member. This also shows that management considers compliance a key concern;
- Regarding operational governance, 76% of respondents are actively involved in an operational governance committee at their company, and 41% participate in at least two committees such as ethics, compliance, risk, and to a lesser extent, strategy.

Finally, it is noteworthy that 44% of respondents indicated that they participate in a Compliance Committee. Most of these were companies that reported highly mature compliance arrangements. Since this committee is specifically devoted to compliance, when steered by Executive Management with all the resources it requires, it truly makes compliance programmes more effective.

Key points

- CCOs increasingly participate in operational committees and mainly work with the legal department, human resources, finance and sales.
- The CCO reports to Executive Management.
- Unlike the United States, in France compliance has few dealings with procurement and communication. More interaction between these functions should be encouraged in coming years.

“The Chief Compliance Officer participates in all governance committees (e.g. the Board of Directors and associated committees) as well as committees geared towards operations (e.g. risk, legal, HR, technical).”

Chief Compliance Officer
Pharmacy industry.
Compliance programme: tools, risk management vectors, and improvements

A compliance programme encompasses the processes, tools, and players working to prevent, detect, and handle compliance breaches in the entity.

Compliance programmes are mainly built on codes and procedures for employees and sometimes partners. But they also feature measures to create a culture of compliance, namely training, awareness-raising and guidance coupled with risk management and control components such as reporting, whistleblowing, self-assessments and audits.

3.

Chief Compliance Officer’s Tools

When asked about the main compliance tools they used, 84% of CCOs mentioned the code of ethics or conduct being used to disseminate compliance requirements internally and externally.

Some 78% stated that they had defined internal compliance procedures.

However only 57% reported that a training plan was in place, and 30%, a communication plan, despite the fact that the latter is an important building block of a compliance programme. It serves as a basis for conveying key messages and makes it easier for employees and stakeholders to take ownership of compliance.

Some 51% of companies have formed a network of compliance officers to help employees apply the compliance programme at work. Since this can be a costly solution for companies, another possibility is to develop synergies with other risk management vectors such as internal control or the legal department. In this way CCOs can leverage existing networks to launch, promote and track the compliance within their company.

A whistleblowing procedure was also in place in 70% of companies surveyed. Employees or third parties can thus report breaches of principles or rules. Interestingly, a study by KPMG US found that 53% of non-compliance cases were reported in this way.

Some 51% of companies have formed a network of compliance officers to help employees apply the compliance programme at work. Since this can be a costly solution for companies, another possibility is to develop synergies with other risk management vectors such as internal control or the legal department. In this way CCOs can leverage existing networks to launch, promote and track the compliance within their company.

Our survey found that the main communication resources used by CCOs were:

- in-house training seminars and conventions facilitated by the CCO;
- information and documents given to new hires;
- manuals, charters, and codes; and
- newsletters to regularly convey information.

To summarize, appropriate communication is one of the keys to a successful compliance programme. It raises awareness and educates employees regarding best practices to adopt.

If an incident should occur, a communication plan is also evidence that the group had procedures in place to prevent non-compliance.

A whistleblowing procedure was also in place in 70% of companies surveyed. Employees or third parties can thus report breaches of principles or rules. Interestingly, a study by KPMG US found that 53% of non-compliance cases were reported in this way.

Some 51% of companies have formed a network of compliance officers to help employees apply the compliance programme at work. Since this can be a costly solution for companies, another possibility is to develop synergies with other risk management vectors such as internal control or the legal department. In this way CCOs can leverage existing networks to launch, promote and track the compliance within their company.
Key points

• The code of ethics and whistleblowing procedures are primary compliance tools.
• However, additional measures in terms of communication and training is needed for a compliance programme to be understood, followed, and effective throughout the entity.

Interaction with risk management

The first finding of our survey was that there is fairly extensive interaction with the functions shown in the bar graph below. In two out of three companies, compliance worked regularly with one or more. However, that figure still shows considerable room for improvement before a truly integrated approach is achieved between compliance and risk management.

Of the three functions, internal audit is mentioned most often. Generally, it is the oldest risk management vector within companies. It can provide CCOs with useful support given its independence, cross-departmental vision, and knowledge of the group’s history.

Internal audit is very important for post-incident investigations. However, it is most effective if its input is sought to assess the compliance function’s risk management arrangements, or to train employees and raise staff awareness, before any incident occurs.

Risk management vectors with which the Chief Compliance Officer regularly works

The risk management function was also cited by 65% of respondents as an important support for compliance. However, some companies still do not assign it the importance it deserves.

Understanding compliance issues and risks is one of the first steps in defining a relevant compliance program. Accordingly, several companies have mapped their non-compliance risks to assess and prioritize them.

A risk map is not merely an effective tool for communicating with top management and the audit committee. It is also a valuable steering tool for CCOs to help them build a roadmap and set priorities.

This risk-based approach can also be productive for more mature companies, helping them streamline efforts while maintaining the same level of assurance.

Finally, under the Sapin II Act, non-compliance risk maps will become an integral part of companies’ compliance programs.

Of these three risk management vectors, CCOs call on internal control the least, even though their respective scopes are very similar. In fact, compliance with current laws and regulations is one of the three objectives of internal control under the COSO Integrated Framework. Synergies of principles, tools, and resources naturally follow, strengthening systems to prevent or handle cases of non-compliance.
To illustrate, the internal control network could provide an excellent source of support for the compliance function at all stages of the compliance programme. Similarly, internal control self-assessment could be adapted to help steer compliance measures.

Key points

- Internal audit is the risk management vector with which the CCO works most closely.
- Risk management and internal control are also valuable sources of assistance in setting up the compliance function and applying its roadmap. Members of these networks can provide support and feedback.

“‘For us, internal audit, internal control, risk management and the legal department all play a key role in integrating regulatory compliance in the company, defining each function’s scope, and capitalising on the methodologies used.’”

Chief Compliance Officer - Pharmacy industry

Improvements in compliance

One of the major challenges for CCOs is to raise awareness of the risks the company runs in the event of non-compliance, and the potential for a damaged reputation or financial, legal, and operational repercussions.

We asked CCOs about topics they are currently working on, particularly which areas they thought likely to be reinforced in the near future.

Third-party relationships topped CCOs’ list of priorities (with 48% mentioning the supply chain and 32%, customers). This reflects our findings discussed earlier, that these areas appear to be under-represented in the compliance scope. It also reflects concerns expressed by French and international regulators in their reports on companies’ third-party relationships, particularly the Know Your Customer (KYC) principle addressed in the Sapin II Act.

Current compliance issues our survey panel is facing

“We asked CCOs about topics they are currently working on, particularly which areas they thought likely to be reinforced in the near future.”

Areas requiring more stringent regulatory compliance in the future

“Third-party relationships topped CCOs’ list of priorities (with 48% mentioning the supply chain and 32%, customers). This reflects our findings discussed earlier, that these areas appear to be under-represented in the compliance scope. It also reflects concerns expressed by French and international regulators in their reports on companies’ third-party relationships, particularly the Know Your Customer (KYC) principle addressed in the Sapin II Act.”

Improvements in compliance

One of the major challenges for CCOs is to raise awareness of the risks the company runs in the event of non-compliance, and the potential for a damaged reputation or financial, legal, and operational repercussions.

We asked CCOs about topics they are currently working on, particularly which areas they thought likely to be reinforced in the near future.

Third-party relationships topped CCOs’ list of priorities (with 48% mentioning the supply chain and 32%, customers). This reflects our findings discussed earlier, that these areas appear to be under-represented in the compliance scope. It also reflects concerns expressed by French and international regulators in their reports on companies’ third-party relationships, particularly the Know Your Customer (KYC) principle addressed in the Sapin II Act.

Current compliance issues our survey panel is facing

“Complying with regulations for healthcare products and coping with inspections by healthcare authorities.”

Chief Compliance Officer - Pharmacy industry

“Using indicators to track regulatory compliance in recently-acquired companies.”

Compliance Officer - Aviation industry

“How can compliance procedures be integrated into companies acquired in emerging countries?”

Compliance Officer - Energy industry

“How anti-money laundering and financing of terrorism (AMLFT) is still our chief concern.”

Compliance Officer - Services industry

“Controlling risks relating to international trade and cybersecurity.”

Compliance Officer - Transportation industry

“Complying with regulations for healthcare products and coping with inspections by healthcare authorities.”

Chief Compliance Officer - Pharmacy industry
The second issue mentioned was data protection and storage. Extensive work is required to inventory and classify the types of data within a company (e.g. client-related, technical, legal, personal) and rank it by sensitivity.

Finally, against a fluctuating economic backdrop with increasing numbers of transactions, Chief Compliance Officers must also be able to take on an “advisory” role for top management at their company, and provide support for internal and external growth strategy.

Survey participants stated that their compliance arrangements for joint ventures and mergers and acquisitions need to be reinforced. In both of these instances, CCOs strive to reassure management that their company will be able to handle any new compliance risks arising from the new consolidation scope.

**Conclusion**

It goes without saying that French companies have not put compliance programmes on hold, waiting for hefty fines or stiffer legislation at home or abroad before taking action. Some 38% of survey respondents rated their compliance program as “mature”. However, that figure was 70% in the KPMG US survey.

Our study also found that, due to the subjects and areas handled, compliance can only be properly addressed within companies if it reports to Executive Management and interacts with the various business and support departments. The interaction and ties should be reinforced to bring the needed answers to companies.

In France, Chief Compliance Officers are becoming increasingly prevalent. However, several companies mentioned that they found it difficult to define the CCO’s scope of action, duties and responsibilities, and the tools and resources that should be provided to help CCOs work effectively and control compliance issues and risk.

To provide groups with a consistent, uniform risk management approach that meets its purpose, in our opinion compliance must be integrated to an even greater degree, cooperating with other functions such as risk management, internal control, and internal audit. Very often potential synergies have not been fully leveraged, and could provide companies greater effectiveness and reassurance without additional resources.

We have received many questions on upcoming legal changes in France pertaining to compliance. This shows that many companies still have room for improvement in order to set up the right structure, dimension and resources for their compliance function for it to be a suitable, reliable function for risk management. The upcoming promulgation of France’s Sapin II Act will move companies to meet their new obligations rapidly. In our opinion, this is a golden opportunity to study compliance in greater depth and include other areas over and above those targeted by the law, namely corruption and influence peddling.

**Key points**

- In France, third-party relationships and data protection and storage are the two major areas where compliance can be improved.
- The compliance function is increasingly called upon when drafting customer contracts, and for mergers & acquisitions, and joint ventures.
- The second issue mentioned was data protection and storage. Extensive work is required to inventory and classify the types of data within a company (e.g. client-related, technical, legal, personal) and rank it by sensitivity.

We invite you to contact us in order to discuss your specific requirements.
Contacts

Sylviane Hautin
Partner Risk Consulting
Head of IARCS
/Internal Audit Risk and Compliance Services
Tel: +33 (0)1 55 68 69 68
E-mail: shautin@kpmg.fr

Julien Auvray
Director Risk Consulting
Tel: +33 (0)1 55 68 75 07
E-mail: jauvray@kpmg.fr

Pierre-Yves Le Naourès
Senior Manager Risk Consulting
Tel: +33 (0)1 55 68 74 89
E-mail: pienaoures@kpmg.fr

Jérémy Villessange
Senior Manager Risk Consulting
Tel: +33 (0)1 55 68 29 12
E-mail: jvillessange@kpmg.fr

Stéphanie Dominguez
Manager Risk Consulting
Tel: +33 (0) 1 55 68 23 76
E-mail: stephaniedominguez@kpmg.fr