

December 11, 2019

FRENCH ANTI-CORRUPTION LAW

How to Assess Risk Under Sapin II

By [Bryan Sillaman](#) and [Nicolas Tollet](#), [Hughes Hubbard](#)

In today's increasingly complex anti-corruption enforcement environment, regulators are consistent in indicating that risk assessments are fundamental components of strong compliance programs. The practical exercise of conducting a risk assessment can, however, present challenges and raise questions. These difficulties stem in part from differing regulator views on the details of the risk assessment process, and the resources that conducting effective risk assessments require.

In this article, we examine the different approaches taken by two important jurisdictions – the United States and France – and attempt to offer four practical suggestions for companies balancing increasingly challenging internal and external expectations when developing and implementing their anti-corruption compliance programs.

See the Anti-Corruption Report's three-part guide to risk assessments: "[Types of Assessments](#)" (Jun. 26, 2019); "[Techniques and Building a Team](#)" (Aug. 7, 2019); and "[Where to Look for Risk and Risk Ranking](#)" (Sep. 4, 2019).

American Expectations for Risk Assessments

Authorities in the United States have long considered the effectiveness of a company's compliance program as a factor to be considered in determining whether to bring charges and negotiating plea or other agreements with companies believed to have engaged in wrongdoing.

In defining the elements necessary for an effective compliance program, the DOJ and SEC's [Resource Guide](#) indicates that assessing risk is "fundamental to developing a strong compliance program." It specifies that there is no one-size-fits-all way in which companies should assess and mitigate their compliance risk, and it is largely for companies to determine on their own where such risks are more pronounced.

In April 2019, the DOJ updated its guidance with respect to the [Evaluation of Corporate Compliance Programs](#) (ECCP). According to the ECCP, the DOJ considers the starting point for a prosecutor's evaluation of whether a company has a well-designed compliance program to be an understanding of the company's business and how the company itself assesses its compliance risk.

The ECCP explains that prosecutors will assess three key process points for a risk assessment. First, what is the compliance process that has been developed and deployed throughout the company, including the methodology used and the type of information and metrics that the company has collected and evaluated in order to perform its risk assessment? Second, how has the company allocated resources, and are they spending a proportionate amount of time and resources assessing areas of greatest risk, such as high-risk third-party relationships? Finally, is the risk assessment subject to periodic update, and are the company's policies and procedures accordingly updated in light of lessons learned? Beyond these points, however, the ECCP, like the Resource Guide, leaves the decisions of how precisely to structure and execute a risk assessment in the hands of the company for which it is being performed.

See [“A Close Look at the New ECCP’s Commentary on Compliance”](#) (May 29, 2019).

Risk Mapping Under Sapin II

The French enforcement authorities take a different – and more structured – approach to risk assessments.

In late 2016, France passed what has become known as “Sapin II” – the Law on Transparency, the Fight against Corruption and Modernization of Economic Life. Sapin II requires companies of a certain size to develop and implement compliance programs designed to prevent corrupt activities. It contains eight mandatory pillars that are directly derived from international anti-corruption best practices that have been applied by companies

around the world for years, in particular those that have been placed under monitorship following a settlement with the U.S. DOJ/SEC.

AFA Controls of Compliance Programs

A French agency – the *Agence française anticorruption* (AFA) – was formed to oversee companies' compliance with Sapin II, which include periodic “controls” (examinations) by the AFA to determine if a company has adopted and implemented the requisite elements of an effective compliance program required by Sapin II. Unlike in other jurisdictions, these controls can be (and are) initiated by the AFA even in the absence of evidence that corrupt acts have occurred.

Risk Mapping Is Required

Article 17, II, 3° of Sapin II requires companies to perform a risk mapping (a *cartographie des risques*). According to the law, the risk mapping must “take the form of regularly updated documentation designed to identify, analyze and prioritize the company's risks of exposure to external solicitations for the purpose of corruption, taking into account in particular the sectors of activity and geographical areas in which the company carries out its activity.”

When compared to other international anti-corruption standards and guidance, the description of what constitutes a risk mapping appears similar to the description of a risk assessment as envisioned by the U.S. enforcement authorities' guidance documents. Referring to the process as a *cartographie des risques* (i.e. risk mapping), however, appears to have led to questions and potential confusion, within the business community in France, given that “risk mapping” is

terminology typically used by corporate risk management functions to refer to a specific risk management exercise involving certain specific methodologies and the evaluation of general risks that a company faces.

AFA Guidance on Risk Mapping

Sapin II also required the AFA to publish recommendations and guidelines to assist companies in preventing and detecting acts of corruption and complying with Sapin II's requirements.^[1] According to the AFA's guidelines on risk mappings – which are nearly five pages long and were released in December 2017 – risk mapping is an extensive exercise designed to achieve two objectives. First, it should identify, assess, prioritize and manage corruption risks in order to ensure an effective anti-corruption compliance program adapted to the company's business model. Second, the risk mapping should inform the company's governing body and ensure the necessary visibility for the implementation of proportionate prevention and detection measures to address the issues identified by the mapping.

According to the AFA, an adequate risk mapping must contain three main features. It must be

1. *comprehensive*, in that it covers all managerial, operational and support processes of the company;
2. *formalized*, in that it must be in a structured, written document; and
3. *adaptable over time* taking into account the need to reassess risks periodically and in accordance with the evolution of the business.

The AFA guidance indicates that the risk mapping should seek to identify a comprehensive list of potential corruption risks, and then quantify their probability (frequency) and the impact (severity) of such risks, along with factors that could increase their occurrence (aggravating factors).

The AFA's guidelines include a specific methodology based on six steps:

1. clarification of roles and responsibilities of the individuals that will be conducting the risk mapping;
2. identification and classification of a comprehensive list of potential risks;
3. assessment of the potential exposure to corruption risks (*i.e.*, the “gross” risk);
4. assessment of the level of risk mitigation measures in place;
5. assessment of the residual “net” risk; and
6. formalization and periodic updating of the risk mapping.

The AFA guidelines contain sample tables that companies can consider replicating in terms of assessing various preventative measures that exist to mitigate potential risks. The guidelines also recommend that companies describe in an appendix to their risk mapping the precise methodologies that they have employed in arriving at their calculated *gross* and *net* risks.

AFA Controls in Practice

The weight to be accorded to the AFA's guidelines with respect to conducting such an exhaustive risk mapping was addressed in the first decision of the AFA Sanctions Commission in July 2019. The case brought before the Commission related to failures allegedly committed by a company in implementing its anti-corruption compliance program in conformity with Sapin II.^[2]

One of the primary faults identified by the AFA in this case was “not to have a mapping of the risks of corruption and influence peddling in accordance with Article 17” of Sapin II. Arguments made during the public hearing indicated that the company had conducted a risk mapping identifying 17 risks and 42 risk scenarios over 44 countries, which resulted in the development of 183 specific action plans to address such risk points. Notwithstanding these efforts, the AFA considered that the methodology did not appropriately reflect the full scope of risks that existed within a group of that size,^[3] and experts for the AFA argued that the risk mapping must combine two elements – breadth and depth – which they believed were not met in that case.^[4]

The Sanctions Commission sided with the company, however, and concluded that the efforts that they had taken in the period between the AFA’s control and the Sanctions Commission’s review complied with Sapin II’s requirements. Among other things, the Commission noted that there is no legal obligation for a company to follow the AFA’s recommended methodology so long as it demonstrates the relevance, quality and efficiency of the methodology used.

See “[How AFA Compliance Program Controls Are Changing the French Anti-Corruption Compliance Landscape](#)” (Apr. 3, 2019).

Criticisms of the AFA’s Approach to Risk Assessments

In terms of form, the AFA guidelines differ considerably from those issued by U.S. regulators, and are not without some level of controversy.

For one, the idea that companies can realistically identify a full, comprehensive universe of potential risks seems unlikely, given the creative ways in which fraudsters and those intent on circumventing otherwise robust controls have succeeded.

Second, the guidelines use risk management nomenclature and principles that may not be consistent with (and could in fact be counterproductive to) the “risk-based” way in which anti-corruption compliance has developed internationally over the last decade. They tend to focus significant attention on developing *quantitative* metrics (*gross* and *net* risk) for topics that in many ways are subjective. That is, the level of perceived risk of a particular activity will be ranked differently by individuals in different positions and levels of responsibility. Spending an excessive amount of time trying to identify and artificially quantify risks that may be quite low in terms of probability of occurrence has the risk of devoting otherwise valuable compliance resources to an exhaustive exercise that in the end does little to reduce the likelihood of corrupt conduct occurring within an organization.

Third, the requirement to assess the corruption and influence-peddling risks throughout all the operations and divisions of very large multinationals is certainly beneficial to preventing corruption, but only to the extent companies realize the importance of the exercise and devote sufficient anti-corruption compliance resources to its performance.

Finally, based on our analysis of initial AFA control reports on a number of French multinationals, the AFA expects the risk assessment to be independent/objective, in-depth and based upon anti-corruption

compliance expertise. What this means in practical terms is that companies may find themselves devoting substantial resources to the exercise, particularly if they do not have a fully functioning and independent compliance department.

Four Tips for AFA Compliance Risk Assessments

In addition to the overarching goal of compliance programs in preventing and detecting corruption, a sufficiently robust compliance program can also serve the very real purpose of eliminating or mitigating the legal, financial and reputational consequences of a regulatory investigation or prosecution for corruption. While the DOJ and SEC's "pragmatic" approach may appear to contrast with the AFA's more "Cartesian" approach, the differences in expectations may not be significant in practice. Based on the published guidelines, as well as the first AFA controls assessment, companies should consider the following when undertaking a risk assessment.

1) A One-Size-Fits-All Approach Will Not Work

American and French authorities agree in the general view that a risk mapping or assessment, like a compliance program overall, must be built to suit the particular company and adaptable over time. A one-size-fits-all approach is not going to be considered effective. Consequently, the identification of risks inherent to a company's activities requires knowledge of the organization as well as a detailed understanding of the processes implemented within the organization that can mitigate the company's risk of compliance failures.

2) Build an Independent and Knowledgeable Team

Our experience in advising companies performing risk assessments and presenting them to regulatory agencies is that to meet AFA expectations, a risk assessment should be conducted with some degree of independence. For this reason, the AFA will assess the independence of the compliance department, as well as who conducted the risk assessment. Self-assessments by operational personnel responsible for overseeing certain risk areas are therefore unlikely, on their own, to be perceived as a best-practice approach. To better ensure independence, some companies may choose to externalize the exercise, in particular since the AFA seems to assess whether the resources devoted to the exercise are consistent with the size and risk profile of the particular company. For smaller companies or those with budgetary constraints, having the exercise performed by a cross-sectional group of individuals from different departments (*i.e.*, compliance, audit, operations) may offer a degree of additional independence.

Additionally, those performing the risk assessment must be sufficiently attuned to anti-corruption risks so that they can develop a risk-based roadmap that will allow for resources to be appropriately focused on areas of heightened risk. Without knowledgeable, independent risk assessors, there is a risk that the risk assessment itself will be considered flawed by the regulators, which could negatively impact the view of the compliance program as a whole. A company might implement a compliance program that is not relevant to its corruption risks and may hinder its operations without good reasons. Such a misguided exercise will not prevent or detect corruption, will not provide credit for its

compliance program, and will ultimately have resulted in a loss of money, time and energy.

Thus, companies should consider who is responsible for conducting the risk mapping/assessment and whether such parties have sufficient:

1. independence;
2. anti-corruption expertise;
3. knowledge of the organization's activities and controls; and
4. resources to fully conduct the exercise in a broad and thorough manner.

Given the high expectations for this exercise, a partnering of internal and external resources may be appropriate in order to allow companies to benefit from the independence/objectivity and expertise that external advisors can provide, while also having internal individuals fully engaged in the process to efficiently identify controls and areas of risk that may not be immediately obvious to an external advisor.

3) Identify Possible Vehicles for Bribes

Companies may wish to approach the risk mapping/assessment by identifying areas of risk that are vehicles for bribes rather than trying to identify each individual risk that they could face in their operations. There are a multitude of scenarios where a particular bribe can be paid, such as to obtain a construction permit on a particular project or for a particular good to clear customs. Rather than looking at each scenario in which a corrupt payment could be made, assessing controls over specific *vehicles* through which they may be made is likely more manageable.

Typical vehicles for corruption include:

1. [third-party intermediaries](#);
2. [gifts](#) and [hospitality](#);
3. sponsorships and [charitable activities](#);
4. rebates and [discounts](#); and
5. [joint-venture](#) relationships.

Companies may wish to compile a list of these relationships and types of activities in various locations to better focus their risk assessment efforts. To the extent that third-party due diligence or approvals for gifts and hospitality are not centralized, companies may consider assessing payment or spend data to identify the frequency of certain of these risk areas in their operations in different locations. Once such vehicles are identified and their frequency determined, the company can better assess the severity of the risk profile and focus their efforts accordingly.

4) Develop Risk Assessment Metrics

So long as the AFA does not change its guidance, a company potentially subject to an AFA control should create scores for gross and net risks. Precisely how companies choose to develop such scores – whether on a numeric or more qualitative basis (*i.e.*, severe, moderate, low), will depend on the preferences and, perhaps, existing audit practices of particular companies.

What is critical from the perspective of the AFA, however, is to demonstrate that companies have taken a clear and, as noted above, independent view of the likelihood and potential impact of corrupt practices in various areas of their operations and assessed how the risk of such practices is mitigated, or not, through existing controls. Only once such

assessment has been performed can a company then focus the resources and attention necessary to further mitigating such risks.

See the Anti-Corruption Report's four-part series on measuring compliance: "[Getting Started](#)" (Aug. 2, 2017); "[Seven Areas of Compliance to Measure](#)" (Aug. 16, 2017); "[How to Measure Quality](#)" (Sep. 6, 2017); and "[Gathering and Analyzing Data](#)" (Sep. 20, 2017).

Bryan Sillaman is managing partner of the Paris office of Hughes Hubbard & Reed and a member of the firm's anti-corruption and internal investigations practice group. He is licensed to practice in New York, Washington, D.C., and Paris. He previously served as an attorney in the Division of Enforcement of the SEC, where he conducted several FCPA investigations.

Nicolas Tollet is a partner in Hughes Hubbard's Paris office, where he conducts internal investigations, counsels on compliance matters and participates in monitorships. He is licensed to practice in New York, Paris and before the U.S. Supreme Court and formerly served as vice president compliance of Technip.

^[1] *Avis relatif aux recommandations de l'Agence française anticorruption destinées à aider les personnes morales de droit public et de droit privé à prévenir et à détecter les faits de corruption, de trafic d'influence, de concussion, de prise illégale d'intérêt, de détournement de fonds publics et de favoritisme. Avis 22 décembre 2017, NOR : CPAZ1735744V : JO, 22 déc.*

^[2] For detailed comments on the first hearing, see M.A. Nicolas and N. Tollet, "Première audience de la Commission des sanctions de l'AFA", *International Review of Compliance and Business Ethics*, August 2019, p. 50, or see M.A. Nicolas and N. Tollet, "France: Anti-Corruption Agency's Sanctions Committee holds blockbuster hearing", *FCPA Blog*, July 8, 2019.

^[3] « Au soutien de sa position, l'Agence a indiqué que la méthodologie utilisée n'offrirait pas, faute notamment d'une documentation appropriée, de garantie quant aux diligences effectuées et ne permettrait pas, en tout état de cause, de refléter l'exhaustivité des risques existant « aux bornes du groupe ». *Id.*

^[4] « Du point de vue méthodologique en particulier, l'expert cartographie de l'AFA a expliqué qu'un tel exercice devait reposer sur la combinaison de deux paramètres, à savoir (i) le « périmètre » et (ii) la « profondeur ». », *Id.*