Discussion Paper

JFSA's Approaches to Compliance Risk Management

October 2018

金融庁
Financial Services Agency

Table of Contents

I. Introduction

In June 2018, the Japan Financial Services Agency released "JFSA's supervisory approaches –replacing checklists with engagement," which explains key principles for supervision. As specified in this paper, the ultimate goal of financial regulation and supervision is to enhance national welfare by enabling sustainable growth of the economy and national wealth –through attaining both financial stability and effective intermediation, both consumer protection and better services, and both market integrity and vigour. It was also made clear that JFSA will issue theme-specific discussion papers aiming to facilitate dialogues between financial institutions and JFSA.

"JFSA's Approach to Compliance Risk Management" is one of the discussion papers which focuses on areas that were previously referred to as systems for compliance and user protection.

There are various types of risks that financial institutions should manage. There are cases where compliance risk and other risks are related, i.e., when different risks emerge from a common root cause, or when problems related to compliance risk are indications that other risks may materialize. Therefore, the concept of this document is considered appropriate for risks that are normally classified into other categories when it relates to compliance risk.

JFSA called for public comments before finalizing this discussion paper, and will continue to engage in discussions with a wide range of stakeholders, including financial institutions and users in order to enable continuous improvement.

As stated in "JFSA's supervisory approaches –replacing checklists with engagement," the Inspection Manual will be repealed after the end of FY2018 (April 1, 2019 or later)[1].

The Inspection Manual contained checklists on compliance and customer protection systems, based on which financial institutions had accumulated business practices. Thus, the repeal of the Inspection Manual is not intended to deny established practices but to support financial institutions' initiatives to improve them.

[1]The Inspection Manual was repealed on 18th December, 2019.

JFSA will hold dialogues with financial institutions in order to analyse actual conditions of compliance risk management, and provide feedback or publish collected examples of efforts, practices and common issues.

This discussion paper is intended to facilitate dialogues between financial institutions and JFSA towards better practices. The JFSA will not superficially apply each item to financial institutions or use them as checklists. In addition, when holding dialogues using this document, JFSA will fully consider the size and characteristics of each financial institution. In particular, JFSA will not require small financial institutions to engage in unnecessarily complex discussions.

II. The need to enhance compliance risk management

1. Previous practices

Financial Institutions saw 1) excessively detailed and strict internal rules, superficial compliance checks against laws and regulations, and shallow prevention measures, causing 'compliance fatigue,' 2) backward-looking and ad-hoc, one-by-one responses to problems which have already materialised, with limited root-cause analysis, and 3) problems addressed mainly by compliance divisions, but not considered as an entire management issue with limited leadership by management and/or ownership by front divisions.

JFSA's intention was to focus on important risks and to conduct root-cause analysis that leads to actual improvement. However, JFSA's nit-picking onsite monitoring on minor flaws and focus on ex-post partial verification of individual cases may have contributed to the above practices at financial institutions and impeded effective and efficient internal control.

2. Rapid changes in business circumstances and expansion of financial institutions' cross-border activities

The rapid change in business circumstances, such as innovation and globalisation, may breed new forms of financial products, services and transactions, which could bring new types of risks. In response, financial institutions are now required to review their risk management practices. Moreover, financial institutions that are expanding cross-border activities need to take into account culture and market practices of each countries and regions when building their risk management systems.

3. Misconducts that had serious impacts on financial institution's business

Financial institutions have been making efforts to build and develop appropriate internal control systems. Nevertheless, misconducts have happened, which had serious impact on financial institutions' business and damaged trust. These misconducts may not have been in immediate conflict with existing laws and regulations, but did not meet social expectations.

In many of these misconducts, problems at the core of business, such as management's attitude, business model and strategy, and corporate culture, are considered an important cause.

III. Management Framework at Financial Institutions

The following points will be important for financial institutions to enhance their compliance risk management.

1. Management and governance

[Issues]

Compliance risk is an integral part of business and is likely to be embedded in the business model and strategy itself. Compliance risk management is indeed the foundation of management. However, the management of financial institutions did not necessarily recognize this. In monitoring financial institutions, JFSA observed following issues.

1) The management tended to understand compliance risk management as a process of building internal control systems based on checklists provided in the Inspection Manual. The management did not regard compliance risk management to be closely related to their business model and strategy, and did not recognize it as an important issue that requires leadership of the management.

2) Financial institutions had a tendency to take superficial measures, such as introducing additional internal procedures, to prevent the recurrence of misconducts. They were weak at preventing different forms of misconducts with a common cause by tracing back to the root, e.g., management's attitude, business model and strategy, and corporate culture.

3) Business functions were likely to view compliance risk management as a role of compliance functions and did not recognize the need to manage risk on their own.

[Compliance risk management as the basis of business]

(1) Management’s attitude and leadership

In order to solve the above mentioned issues, it is extremely important for the management of financial institutions to take the initiative, recognising that compliance risk management is truly the core of management.

The management of financial institutions must understand that compliance risk is inherent in business models and strategies, and many serious incidents are inextricably linked to them.

For example, the management’s excessively short-term income-oriented message may exert unreasonable profit pressure on the executives and employees of the business division. As a result, they may make inappropriate judgments or take unfavourable behaviours that could lead to misconducts

Another example may be that the internal control system may not be keeping up with the expansion of the business function.

Thus, it is important for the management to fully envisage what risks can arise from the financial institution’s business model and strategy. In addition, when developing business models and strategies, it is necessary to consider a wide range of risks, including compliance risks. In doing so, it is important to take into account not only abstract qualitative facts but also specific and quantitative facts.

This management’s attitude ("tone at the top") has a significant impact on corporate culture that underlies effective compliance risk management.

(2) Internal control

Even if the management is accurately aware of compliance risk and making decisions accordingly, it is impossible to appropriately manage compliance risk firm-wide, unless this awareness is penetrated by all executives and employees.

Firstly, middle managers give daily instructions to employees and are responsible for primary performance reviews. Therefore, middle managers are required to concretely understand the “tone at the top” in relation to their functions, and to disseminate them through their own attitudes (“tone in the middle”) in their daily operations.

Secondly, human resource management and remuneration policies generally work as an incentive for executives and employees, and have major impact on their behaviour[2]. Therefore, it is closely related to compliance risk management. For this reason, it is important to design and manage human resources and remuneration consistently with the management's attitude and the ideal corporate culture.

Thirdly, many financial institutions have in place whistleblowing systems that allow employees to directly report misconducts to internal and external expert contact points. In reality, however, there are cases where the whistleblowing system was not utilized and problems were not recognized for a long time, and cases where misconducts were uncovered through whistleblowing to the media. In these incidents, it is likely that employees did not feel that their voices will be properly and safely handled. The attitudes of the top management and middle management play an important role in encouraging employees to speak up.

(3) Corporate culture

The values, philosophies, and codes of conduct shared by executives and employees, i.e., corporate culture, can have a major impact on their behaviour and decision-making. Corporate culture is the foundation of compliance risk management, and underlies attitudes of the top management and middle management and internal control systems relevant to compliance risk management.

A sound and open corporate culture can mitigate compliance risks, while an income-first or authoritarian corporate culture can trigger compliance-related issues.

It is important for the management to clarify and foster the ideal corporate culture in relation with business strategies[3].

(4) Corporate governance system that enables feedback from the outside

It is not always easy for the management to reflect on their attitudes and objectively view the status of the internal control system or corporate culture. Sometimes, common sense within the firm may diverge from common sense of the society. In addition, to manage

[2]If the management sends excessively short-term income-oriented messages and emphasizes sales results, while at the same time builds human resource management and remuneration policies that disregard compliance, employees may form inappropriate motives that some misconducts will not be questioned as long as sales results are improved.

[3]Cultural issues often materialize when business performance deteriorates. However, in some cases, cultural issues did exist from the past, but were hidden behind strong business performances.

compliance risk, it is important to sensibly and timely obtain necessary information, such as rapid changes in the business environment surrounding financial institutions.

Therefore, it is important to establish a governance structure which allows to properly control management's decisions, with the initiatives of the board of directors including outside directors and the audit committee.

There are some cases in which the top management or the middle management themselves are engaged in misconducts. Control by outside directors is particularly important in preventing and correcting misconducts by the management

[Risk management framework[4]]

(1) Risk ownership by the business function

The business function is the source of risk arising from income-generating business activities and is generally primarily responsible for risk management. Therefore, it is important for the executives and employees of the business divisions to have ownership in compliance risk management.

(2) Control by the compliance function

The compliance function's role is to independently control and support risk management by the business function. It is also responsible for comprehensively managing risk on a firm-wide basis. The compliance function is therefore required to understand both the operation of the business function and potential risks, in addition to having expertise in risk management.

For the compliance function to fully perform these important responsibilities, the management should take the initiative to grant authority to executives and employees of the compliance division, ensure their independence, and to secure sufficient human resources.

[4]The roles of the business function, compliance function, and internal audit function are often understood as the "three lines of defence." This concept helps financial institutions build an optimal internal control system by allocating necessary roles to each function. However, "three lines of defence" is merely one means of risk management, and the objective is not to clearly distinguish the lines. It is important for each financial institution to develop a system that enables suitable risk management.

(3) Assurance by the internal audit function

The internal audit function is expected to review the functioning of compliance risk management independently from both the business and compliance function, point out to the management to correct any deficiencies in the framework of compliance risk management, or provide advice or recommendations to the management for improvement.

It was often the case that the role of internal audit function was limited due to lack of understanding and support from the management. Risk assessment by the internal audit division tended to be inadequate, and reviews tended to check whether the operations in the firm were in line with the internal rules. .

In order to improve the quality of internal audits, it is necessary to conduct risk assessments based on business models for selecting audit items, and conduct audits from the perspective of disciplining the management.

In addition, when the internal audit function conducts investigation on compliance issues, it is important that the management takes the initiative to trace back to the structural problem behind the issue and formulate effective measures to prevent recurrence. For example, if the management's excessively income-oriented attitude is the major cause of the compliance issue, it is unlikely that a fundamental solution will be reached if that cause is not tackled. If the cause is the compliance function not being able to keep up with the rapid growth of the business function, merely adding the rules may even deteriorate compliance risk management.

In order to reach such root-causes, it is important for the management to play a central role in fostering a corporate culture that allows executives and employees to analyse the issue from multifaceted perspectives, through discussions with the executives and employees from multiple divisions, including the business, compliance, and internal audit.

For the internal audit function to work effectively, it is important to secure sufficient human resources that enables to control the management team. In addition, it is also important to appropriately cooperate with outside directors and the audit committee and implement appropriate audits.

(4) Group companies and overseas offices management

Often, compliance issues occur across multiple firms within a financial group. While the form of group governance is diverse, it is important for the management team that

oversees the entire financial group to build and manage the group's compliance risk management system, accurately identify the risks associated with the business strategy, and establish a system that enables appropriate response when risks materialize.

Especially for financial institutions with overseas offices, compliance risk must be managed in accordance with differences in countries and regions. While laws, regulations, and policies of financial authorities may differ across countries and regions, risks are borne by the entire group. Therefore, it is important that the head quarter implements effective controls with the initiative of the management.

[Human resources and IT]

(1) Securing human resources for compliance risk management

The scope of expertise necessary for compliance risk management has been expanding. On the other hand, in order to effectively manage compliance risk, it is also important for the members of the compliance function to have a deep understanding and experience of the business, as well as the ability to recognize important management issues.

Rotating human resources between the compliance or internal audit function management division and the business function is considered to be useful for the purpose of assigning human resources who have a good understanding of the business function’s operations to the control function, and for enhancing their authority. In addition, it may be beneficial in supplying human resources with knowledge of compliance risk management to the business function.

(2) Utilization of IT

Financial institutions are expected to make use of IT for effective and efficient compliance risk management. The management must have good understanding of IT and strategically allocate budgets and personnel to it.

2. Development of a risk-based approach

[Issues]

In general, financial institutions took rules-based approaches, strictly but superficially observing laws, regulations and checklists of the Inspection Manual. JFSA has observed following tendencies through monitoring.

1) Due to lack of risk-based approach, some financial institutions established a management system that imposed excessive burdens on the firm. As a result, those

financial institutions could not allocate sufficient resources to important management issues.

2) There was a tendency to concentrate on ex post responses to problems that have occurred. The perspective of considering how to prevent potential risks was weak.

3) Financial institutions that did not have a forward looking perspective tended to leave out risks that arise from new areas where laws and regulations were not sufficiently developed.

(1) Risk-based approach

In order to solve the above mentioned issues, it is necessary to consider risk management, taking into consideration cost-effectiveness and the purpose behind the law, while focusing on prevention of the occurrence of significant business risks that could seriously affect user protection and market integrity, thereby impair the trust in the financial institution itself.

To establish an effective risk management framework, it is necessary for the management to take the lead in implementing the risk-based processes. The implementation can be broadly categorized into the following processes.

1) Risk identification and assessment

Collect a wide range of information, comprehensively and concretely identify and assess compliance risks, and determine whether there are any significant risks or areas that requires development of management systems.

2) Risk mitigation and control

Formulate and implement specific action plans to mitigate and control identified risks.

The actual implementation of these processes may vary depending on the scale and characteristics of the financial institutions. Thus, it is important for each financial institution to continue to make efforts to improve the process so that an appropriate management system can be established.

It is also important to revise or abolish any unnecessary internal rules found through the risk-based approach and establish a more efficient system.

(2) Identification and understanding of a wide range of risks

In risk identification, it is important to accurately find out risks that are significant for the financial institution. The starting point is to identify applicable laws to the financial

institution's businesses, and find any services that may breach those laws. Next, the management is required to analyse risks from a fundamental perspective, i.e., whether the service would adversely affect the society and the economy, or whether they would violate the protection of users. In the absence of such analysis, significant risks may be overlooked. The following are examples of such situations.

1) When a business area where the financial institution does not recognize any issues and does not manage risks, turns out to adversely affect many customers or receive major social criticism (see Box).

2) When the financial institution is engaged in new financial products and new trading methods that arise in the rapidly changing financial and economic environment, which are yet to be covered by the regulatory framework.

In order to identify exposure to these risks, it is necessary to identify services or operations that could affect user protection and the fairness and market integrity, leading to a significant impairment in trust. It is important to prevent future misconducts from occurring, by accurately grasping various changes in the environment and detecting potential issues, rather than only focusing on ex post responses to risks that already materialised.

<Box> Conduct Risk

Conduct risk has recently begun to attract global attention. While a common understanding is yet be formed, it is a useful concept that allows financial institutions to be aware of potential risks that are not captured or understood within their current risk management framework. Such risks may not be regulated by laws and regulations, but they often lead to (1) behaviours that are against social norms, (2) conducts that violate business and market practices, and (3) services that lack users' perspectives. As a result of these misconducts, corporate value may be significantly impaired.

For this reason, the concept of conduct risk is sometimes understood with an emphasis on risk that deviation from social norms may affect the protection of users and market integrity, thereby causing damage to the creditworthiness and financial losses on financial institutions[5].

[5]This document uses relatively new concepts. However, JFSA does intend to require financial institutions to use similar concepts or to develop new internal rules. It is important for each financial

Conduct risks can materialize when behaviours of financial institution's executives and employees: (1) adversely affect the protection of users; (2) adversely affect the fairness and transparency of the market; and (3) leads to social criticism regardless of actual damage.

Financial institutions have always been expected to actively contribute to user protection and market integrity due to their public nature and social role. It is possible to understand that conduct risk may be a relatively new word but simply refers to risks that arise when financial institutions are unable to meet social expectations.

IV. JFSA's Supervisory Approach

1. Procedures for Monitoring

JFSA will generally take the following procedure for monitoring compliance risks.

(1) Wide-ranging intelligence gathering

Interviews and discussions with the management, outside directors, executives and employees of financial institutions enable JFSA to timely understand business trends and any issues in internal control, and form the basis of intelligence gathering. Documents submitted by financial institutions (public information, minutes of board meetings, and other information requested by JFSA) are also an important source of intelligence.

However, it is necessary for JFSA to gather and analyse information from a wider source. For example, it is important to follow 1) news and interview requests from media, 2) consultations and complaints received by JFSA, 3) misconduct events at non-financial firms, 4) domestic and foreign legislative movements, 5) discussions at overseas financial authorities, and 6) changes in economic and social environments.

In addition, it is necessary to collect information that may not seem directly related to compliance risk of financial institutions, and analyse whether it could have impact on compliance risk in the future.

(2) Setting monitoring issues

In monitoring financial institutions, it is necessary for JFSA to set monitoring issues by analysing the risks of each financial institution that may affect user protection, fairness and transparency of the market, the firm itself and the wider financial system, from

institution to enhance its existing risk management framework in an optimal manner.

information gathered from a wide range of sources. In this process, it is important to analyse both the risks that have already materialized and the risks that could arise in the future.

Risks of individual financial institutions should be analysed based on their business models and strategies, business operations, and the organizational framework. Based on the analysis, JFSA will discuss with each financial institution to share JFSA's views and obtain mutual understanding of the risks.

When there is a possibility that compliance risks are increasing or that the internal management system may not be responding to risks, JFSA will have to collect and analyse information on business models and business trends, and hold dialogues with the managers of relevant departments and outside directors. This is likely to happen when the financial institution is rapidly expanding its business.

When analysing risks, it is also important to pay attention to complaints received at JFSA, especially, if 1) there are multiple similar complaints about a particular financial institution, 2) similar complaints are received over a long period, and if 3) there is a trend in the content of the complaints. It is important for JFSA to link individual information, including information that were obtained in the past, and find out whether there are any trends to be noted. For analysing huge amount of information, JFSA will make use of IT.

(3) Strategy development and monitoring

Grasp actual conditions and set perspectives for monitoring

JFSA will first grasp actual conditions of the risks at the financial institution, and set monitoring perspectives. This process is particularly important when dealing with new types of risks.

When assessing the actual conditions of financial institutions, JFSA will have to fully understand the businesses and operations relevant to the risks to be monitored. In addition to interviews with the executives and employees of financial institutions, interviews with various experts including lawyers, auditors, and consultants will also be beneficial for assessment.

In building a monitoring perspective, depending on the nature of the risks, it may be useful for JFSA to study the issues by setting up a working group, or to share and deepen JFSA's understanding through discussions with the industry associations.

Monitoring policy formulation

JFSA will set monitoring policies, i.e. which financial institution to monitor, the scope, and specific methods for monitoring.

JFSA will select financial institutions that are considered high risk or likely to become high risk in the future. JFSA will give priority to on-site inspections of financial institutions that are regarded as relatively high risk. For example, financial institutions with a long on-site inspection interval may be regarded as high risk, since there could be issues that JFSA haven't identified.

When deciding the scope of monitoring, JFSA will select areas that are high risk or likely to become high risk, taking into account JFSA's recourse constraints.

Review of the monitoring policy

In some cases, it may not be possible for JFSA to clearly identify the specific issue from the information gathered, even if it is highly likely that compliance risk is emerging.

In these cases, JFSA will still set up perspectives before conducting monitoring based on available information (including the financial institution's risk awareness). However, new information obtained through monitoring may alter JFSA's understanding of the issue, and JFSA will change monitoring policies accordingly. Thus, the monitoring processes would not be clearly segregated. It is important for JFSA to constantly review the process while eliminating assumptions.

Monitoring

In policy formulation, it is necessary to analyse available information and set certain perspectives. However, monitoring itself should be conducted without prejudice. Discussions with financial institutions should be based on facts, and JFSA should make efforts to reach mutual understanding regarding the monitoring results.

In some cases, JFSA will exercise legal authority to conduct on-site inspections. Especially in cases where there is a high possibility that the financial institution is violating the law or where JFSA needs to verify whether the financial institution is fulfilling minimum standards, it is likely for JFSA to conduct on-site inspection, in order to swiftly and accurately grasp the situation and take necessary corrective measures.

JFSA may also conduct horizontal reviews of multiple financial institutions. Horizontal reviews are useful in analysing the reasons behind the differences among financial institutions, verifying problems that pertain to similar types of financial institutions and

the industry as a whole, and supporting their overall improvement. In horizontal reviews, financial institutions that have taken advanced initiatives or those that have distinct features may be included in the scope.

(4) Communication

In order to conduct effective monitoring, JFSA will share JFSA's understanding of issues throughout the monitoring process by publishing reports and holding dialogues with industry associations. .

JFSA will provide feedback of important findings (including the lessons learned from problems and advanced initiatives) as a result of monitoring to the financial institution. In addition, JFSA will share these findings by publishing reports and holding dialogues with industry associations. In addition, the results of monitoring on specific issues and relevant supervisory viewpoints will be made public as necessary.

When an issue that may require consideration of legal revisions are found, JFSA will share information and hold discussions with relevant ministries and industry associations.

(5) Developments necessary for JFSA

JFSA has to develop its ability to conduct effective monitoring. JFSA will build a system to detect the rapidly expanding and changing business of financial institutions, and to collect relevant information and analyse risks. For analysing huge amount of information, JFSA will make use of IT. It is also important to develop human resources with the ability to 1) analyse wide range of information, such as business of the financial institutions, management, risk management, IT, and domestic and overseas legal and regulative issues, 2) identify potential risks and issues faced by financial institutions, 3) judge the seriousness and potential implications of those issues, and 4) communicate sufficiently with the management of financial institutions.

At the same time, it is important for JFSA to maintain a high level of knowledge of each financial institution and the industry, and accumulate experience concerning compliance risk management, and to build the organization and culture that enables JFSA to make full use of such knowledge and experience. For example, JFSA will compile case studies on important domestic and overseas issues, and use them in training staff members. JFSA will also appropriately accumulate various information obtained in the monitoring process, and develop a system that effectively utilizes such information for future monitoring.

2. Key points

While JFSA will conduct dialogues with financial institutions based on their business models and strategies, business models and strategies themselves are left to the discretion of financial institutions. Thus JFSA will respect financial institutions' judgements.

Nevertheless, if the management is not adequately managing compliance risk, misconducts could happen that may have a material impact on their business and seriously damage its trust.

The purpose of dialogues and discussions between JFSA and the financial institution's management is to prevent those misconducts by sharing issues that JFSA realised through wide-ranging information gathering.

When monitoring, JFSA staff shall observe proper procedures based on legal requirements, and shall exercise their authority in light of the perspectives set forth in the Supervisory Guidelines. When taking administrative actions, JFSA will objectively confirm the fact that serious illegal problems have arisen in user protection or market integrity, and that the major causes of such problems are deficiencies in the internal control system and governance of the financial institution[6].

In addition, JFSA will not place excessive burdens on financial institutions during monitoring. In addition to giving necessary consideration to financial institutions during on-site inspections, JFSA will review the contents and frequency of submissions from financial institutions based on their usage in monitoring.

[6] "Administrative Action in the Financial Sector" (https://www.fsa.go.jp/en/refer/guide/action.html)