5

Internal Controls and Risk Culture in Banks

Doriana Cucinelli

5.1 Internal Controls and Culture Evolution

In the last 30 years, regulators and academics have focused their attention on different topics related to the corporate culture of banking.

During the late 1990s, control culture was considered the most important aspect of enterprise culture in financial institutions and a fundamental driver of the effectiveness of the internal control system (BIS 1998). In the next phase, attention shifted from control culture to compliance culture. BIS (2005) defined compliance risk and issued guidelines on the compliance risk function, a new component of the internal control system. In BIS (2005), the Basel Committee also made recommendations on the responsibilities of Boards of Directors (BoD) and Senior Management in defining ethical and integrity values and behavioral models for staff. It also made recommendations on the relationship between compliance function and the other control functions,

D. Cucinelli (✉)
Università Degli Studi Di Milano-Bicocca, Milan, Italy
e-mail: doriana.cucinelli@unimib.it

A. Carretta et al., *Risk Culture in Banking*, Palgrave Macmillan Studies in Banking and Financial Institutions,
DOI 10.1007/978-3-319-57592-6_5

such as the Internal Audit function. It emphasized that compliance should be part of the culture of any organization. Compliance should start at the top and is most effective if corporate culture emphasizes standards of honesty and integrity. The compliance function should be independent and the Internal Audit should monitor it regularly.

During the financial crisis, authorities and institutions realized that risk is a key component of a bank's business. In this third and current phase, one of the most important goals is to identify the main risks and draft risk mitigation plans. It has become widely recognized that "risk culture" can be defined as "*the values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with common purpose, in particular the employees of an organization*" (Institute of Risk management 2012). Risk culture and Risk management are closely related, and risk culture is a critical element of risk management efforts.

In a fundamentally altered landscape, the Financial Stability Board (FSB 2014) issued Guidance on Supervisory Interaction with Financial Institutions on Risk Culture. This identifies elements underpinning a good risk culture in financial institutions and aims to assist supervisors in assessing the strength and effectiveness of the culture of financial institutions in risk management.

The BoD and senior risk management play an important role in the dissemination of risk culture. Because the rest of the institution will emulate top managers' behavior, it is critical that senior management demonstrates adherence to sound risk management and high standards of integrity.

In order to investigate and develop their risk culture, banks often focus on tangible aspects such as Risk Appetite Statement, Mission Statement, the proxy system, and the approval limits. These, however, do not capture the complex behaviors and skills that make up the risk culture of a bank, and which are often the most difficult to change. It is, in fact, necessary to go beyond the "tools" of risk culture, and it is crucial that banks learn new methods of doing this. Risk management skills are the key to successful risk management.

Culture is the most important determinant of behavior, and the financial crisis has highlighted the great importance of a sound risk culture as an element of the internal control system. But even when an

internal control system is in place and compliant with regulations, there is no guarantee that it is applied and followed by the whole organization. It can be the case that the fundamental principles of control are not "embedded" in the enterprise culture. The Board of Directors may define a good internal control system, but if they fail to disseminate the culture of risk, bank employees may not adopt the ideals of the organization.

This chapter describes the evolution of banking culture, from the culture of control, to the culture of compliance, up to the culture of risk prevailing today. It describes the relationships between the different "lines of defense" existing in a bank and the role of the BoD and top management in disseminating risk culture over all levels.

This chapter is structured as follows. Section 5.1.1 describes internal enterprise control and its components, focusing on the environment and the key factors that influence it. Section 5.1.2 describes the concept of culture of control. Section 5.1.3 analyzes the culture of compliance. Part 2 examines the relationship between the internal control system and risk management in the banking organization. Sections 5.2.1, 5.2.2, and 5.2.3 focus on the three different lines of defense. Part 3 provides conclusions.

5.1.1 Internal Controls and Enterprise Risk Management: The Key Role of Control Environment

Regulators have always considered culture as a fundamental element of the internal control system (ICS). In the early 1990s, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a document on the internal control framework providing principles-based guidance for designing and implementing an effective internal control system to meet management need to control their enterprise and ensure that organizational goals related to operations, reporting, and compliance are achieved (COSO 1992). Today, the Internal Control—Integrated Framework has been replaced by a new document published in 2013. These new guidelines help organizations

in implementing and designing an internal control system in the light of the many changes in business and operating environments brought about by the financial crisis. COSO represents the key elements of the Internal Control System in a "cube"[1] showing the five key areas as monitoring, information and communication, control activities, risk assessment, and control environment.

At the beginning of the 2000s, there was a growing awareness of the importance of sound risk management. In 2001, COSO and PriceWaterhouseCoopers started developing a framework for improved enterprise risk management (COSO 2004). In those years, events highlighted the increasing importance of risk management and the need to implement a strong framework to effectively identify, assess, and manage risk.

In addition to defining the Internal Control System, COSO also defines Enterprise Risk Management. The 2004 definition was "*a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.*"

The eight ERM components define a sound internal controls system and specify all phases of risk management (Table 5.1). They are the same as the phases in the Internal Control System cube, but Risk Assessment is expanded into four different phases: objective setting, event information, risk assessment, and risk response. These phases are closely linked to the identification, assessment, and management of risks (Fig. 5.1). With this specification, COSO highlights that ERM is integrated with the internal controls system.

As in the Internal Control System, COSO inserts the objectives and business structure into the lateral and top sides of the cube.

The environment where companies work is uncertain for various reasons: the financial crisis, globalization, technology, the threat of terrorism, regulation, and changing markets. This uncertainty generates risk. In order to manage this risk correctly, and take the only risk that is in line with its risk appetite, a company needs to define the ERM. When

Table 5.1 The eight ERM components

Components	Description
Control environment	The internal environment is the basis of the organization approach. At this level, the organization defines its tone and specifies the level of risk that wants accept. Key elements include the BoD, the risk appetite, the risk management philosophy, etc.
Objective setting	The goals of the organization must be aligned with the risk appetite defined. Risks can derive from both external and internal sources, so it is crucial that the enterprise risk management defines a precise process of risk management, from risk identification, to risk assessment, and risk response
Event identification	The identification of internal or external events and assessment of which events would be positive or negative for the entity as a whole
Risk assessment	The organization defines the probability of occurrence of a negative event and the impact. This is the first phase in defining risk management
Risk response	Management identifies the best response aligning it with the risk tolerance and appetite of the organization
Control activities	Crucial to ensure the effectiveness of risk response. Policies and procedures are designed for maximum efficiency by management
Information and communication	Information is communicated rapidly among the organization. Fast and complete information ensures efficiency
Monitoring	Completes the cycle. If necessary, the risk management team can step in and realign the activity to company risk tolerance and appetite.

Source COSO (2004)

ERM is clearly defined, a company can operate knowing the level of the risk it can take on, and avoid risk outside its risk appetite. In this

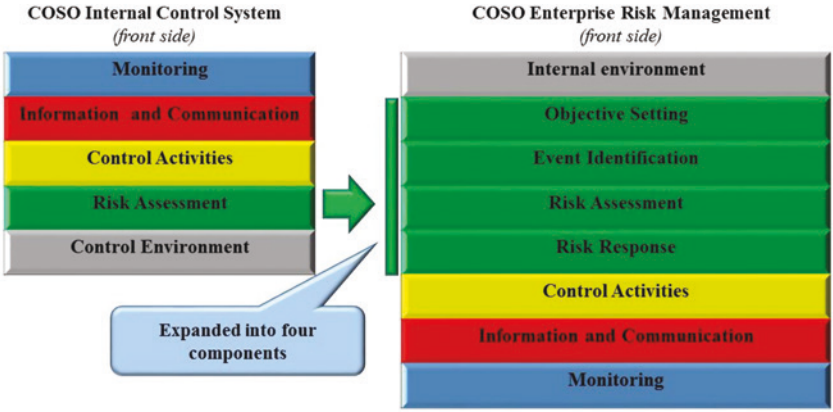

Fig. 5.1 Internal control system vs Enterprise risk management. *Source* Author's elaboration on COSO Internal Control System and COSO Enterprise Risk management

scenario, a company can create maximum value for its stakeholders, who know that risk is managed correctly.

Many of the notorious financial failures leading to the 2008 financial crisis, including governance failures, and Enron and WorldCom, were, at least in part, the result of weak control environments. The control environment, in fact, underpins the seven components of ERM and is the key element of a sound internal control system. It is the first element of ERM shown in the "cube," and could be described as the basis of the internal control system where it operates and furthers the strategic objectives of the organization. The vision and strategy communicated by senior management can be seen as the "glue" which holds the organization together, and moves all employees in the same direction.

Top management determines the control environment, with the help of the management team. The aim is to define the risk culture of the organization and to increase the employees' risk sensitivity. They create the basis of the ERM and define the goals and the scope.

There are seven key factors that influence the internal control environment:

1. Communication and enforcement of integrity and ethical values;
2. Commitment to competence;

3. Participation by those charged with governance;
4. Management philosophy and operating style;
5. Organizational structure;
6. Assignment of authority and responsibility;
7. Human resource policies and practices.

1. Communication and enforcement of integrity and ethical values: in this key factor, the most important element is the "tone at the top." We can define this concept as the Board of Directors and Management team behavior. If they demonstrate integrity, honesty, and ethics, these values spread among the entire organization, and employees are more likely to follow the same behavior. However, for employees to be honest and upright, the "tone at the top" must be credible, and the code of ethical conduct must be followed in particular by top management.
2. Commitment to competence: each employee should be assigned to his job according to his or her competences. Without the right skills, the employee cannot obtain good results. For this reason, the definition of competences necessary for a role is a crucial goal for the management team. They need to identify the right employee for the right tasks.
3. Participation by those charged with governance: The Board of Directors plays an important role in the internal control system. Usually, the BoD defines the strategy of the company and controls accountability, but it is fundamental that the internal committee are independent of the BoD. The audit committee and the internal control committee (inside the BoD) especially need to be independent.
4. Management philosophy and operating style: the Board of Directors will include individuals who are different in terms of philosophy and operating style, but overall the philosophy and operating style of the BoD should be in line with the control environment and should be pervasive. Compliance with financial report standards is crucial for sound management practices. Where there is manipulation of profits because they are not applied, and where a management team shows

an aggressive attitude, these are signs of weaknesses in the management philosophy and operating style.

5. Organizational structure: in order to achieve its objectives, the company should define how activities are planned, executed, controlled, and monitored in detail. An organizational chart showing truthfully roles and responsibilities of employees and company's goals is necessary for an efficient organizational structure.
6. Assignment of authority and responsibility: ERM can work efficiently only where employees know what their responsibilities are and who they answer to. Clear job descriptions showing responsibilities of each role are a good tool to strengthen the ERM system.
7. Human Resource policies and practices: in order to clarify the company–employee business relationship, the company should clearly define guidelines for HR management, covering recruitment, promotion, remuneration, and training. In absence of such guidelines, the company is exposed to the risk of hiring people who lack the necessary skills and qualifications.

For the internal control system, the internal control environment is like the chassis of a car, which defines the form and position of the different sections. When the chassis is damaged, driving the car is more difficult and risky; there can be instability and loss of control over gears etc. Just as a chassis is the fundamental component of a car, the internal control environment is the basis of the internal control system, and only if the internal control environment is properly defined can the other components function properly and the bank achieve its objectives.

5.1.2 Internal Control System in the Banking Sector: The Culture of Control

The Basel Committee has dealt with the internal control system on the basis of COSO since 1998. In the "Framework for Internal Control System in Banking Organizations," the Committee defines the principles for a sound internal control system. These principles are intended to be for general application and use by supervisory authorities for

monitoring how banks structure their internal control system. As a result of this regulatory intervention, the concept of "control culture" has become widespread.

The Basel Committee (1998, p. 8) defines the internal control system as "*a process effected by the board of directors, senior management and all levels of personnel. It is not solely a procedure or policy that is performed at a certain point in time, but rather it is continually operating at all levels within the bank. The board of directors and senior management are responsible for establishing the appropriate culture to facilitate an effective internal control process and for monitoring its effectiveness on an ongoing basis; however, each individual within an organization must participate in the process.*

The main objectives of the internal control process can be categorized as follows:

1. *Efficiency and effectiveness of activities (performance objectives);*
2. *Reliability, completeness and timeliness of financial and management information (information objectives); and*
3. *Compliance with applicable laws and regulations (compliance objectives).*"

Among the group of principles outlined by the Basel Committee,[2] those regarding management oversight and the control culture highlight the importance of BoD and senior management responsibilities. The BoD is required to approve and periodically review business strategies and bank policies. In addition, it is responsible for the definition of an adequate and effective internal control system. After this, senior management take on the task of implementing the strategies and policies, and is also responsible for the development of processes referring to the identification, measurement, and monitoring of risks that arise. (BIS 1998). Furthermore, BoD and senior management are responsible for promoting high ethical and integrity standards among all the levels of the organization.

In order to achieve internal control goals constructing the enterprise culture should give priority to cultivating teamwork spirit, so as to spur employees to self-improvement, and create, maintain, and advocate an

agreeable atmosphere for teamwork spirit. Information and communication become sound tools of control culture. Finally, the BIS (1998) underlines that having a strong internal control culture does not ensure that goals are reached, but in its absence, there are more opportunities for errors or improprieties to go undetected.

Despite the regulatory interventions following the Basel Committee guidance in many countries, there have been numerous cases of internal control failure in recent years (for an example, see Box 5.1). There are several reasons for the failure of the internal control system, which include taking decisions without adequate information, human error, deliberate circumvention, management overriding controls, and above all the prevalence of form over substance in implementing control measures. It is not enough to set up a risk or supervisory committee to meet once or twice a year. Only where formal control measures become real and are thoroughly integrated into the organization can financial intermediaries achieve the aim of having a strong internal control system.

Box 5.1. An example of the failure of the internal control system: the case of UBS

UBS, *the Swiss bank hit by an alleged rogue trading incident, admitted that its internal controls had failed and that it was looking at whether to "claw back" bonuses from some individuals as a result of the incident.*

While the overall ***bank was able to report a SFr1bn (£711 m) profit for the third quarter,*** *the investment bank posted a pre-tax loss of SFr650 m. After the unauthorized trading loss, a drop in revenues because of the Eurozone crisis and a weaker Swiss franc.*

Analysts focused on the compensation ratio—the amount of money set aside to pay staff relative to income—which reached 94% inside the investment bank. Management defended this high level by saying it included deferral of bonuses from previous years.

In total, the bank set aside SFr775 m for "variable compensation" in the third quarter, compared with SFr867 m in the second quarter, and said SFr467 m was related to prior years' bonus deals.

Finance director Tom Naratil admitted that some staff may have to pay back a portion of their bonuses. "We do have a harmful act clause. As we review individuals' accountability for the incident we'll be reviewing if the harmful act clause applies," he said.

A number of resignations have taken place since suspected rogue trader ***Kweku Adoboli was arrested and charged with four counts of fraud and false accounting.*** *He is yet to enter a plea to the charges and*

is due in court next month. Among those to leave are the chief executive Oswald Grübel, as well as the two co-heads of equities—Francois Gouws and Yassine Bouhara—as well as handful of others who are facing "disciplinary action".

Naratil also indicated that the bank was keen to pay bonuses, despite the loss in the investment bank. "We are in a competitive market, particularly for talent," he said.

In a filing to the Securities and Exchange Commission in the US, made at the same time as it published third-quarter results, ***UBS said its internal controls were "not effective".*** *It is required to make a statement about internal controls under the Sarbanes-Oxley Act, brought in a decade ago after the Enron scandal. The bank highlighted two control deficiencies:*

• the control requiring confirmation with counterparties of trades within the investment banking equities business

• the controls for relationships between different trading desks within the investment bank's equities and fixed income, currencies and commodities businesses to ensure that internal transactions are valid and accurately recorded in UBS's books and records.

"Investigations are ongoing, and management may become aware of facts relating to the investment bank that cause it to broaden the scope of the findings described above and to take additional remedial measures," the bank said.

The bank, which employs 6000 people in the UK, is now expected to announce plans to scale back its investment banking arm—putting more UK jobs at risk—at a presentation in New York on 17 November. Its German rival, Deutsche Bank, also admitted on Tuesday that it was cutting 10% of its investment banking staff even as it reported a better than expected third-quarter pre-tax profit.

"During the third quarter, the operating environment was more difficult than at any time since the end of 2008, driven by a deteriorating macro-economic outlook, and significant financial market turbulence," said Josef Ackermann, the Deutsche Bank chief executive who has also been involved in the talks to try to solve the Eurozone debt crisis.

Deutsche's third-quarter pre-tax profit of €942 m (£820 m) included €329 m. from the corporate and investment bank which had reported €1.3bn a year earlier.

Deutsche Bank has written down its exposure to Greek government bonds to 46% of their face value—although the European Banking Authority is asking banks to assess their capital on the basis of a 60% loss. Finance director Stefan Krause said it would be able to meet the capital requirements set out by the EU.

Source Article published in "The Guardian" by Jill Treanor, 25 October 2011[3]

5.1.3 Culture of Compliance

Customer interest in the reliability of financial institutions has been growing rapidly since before the beginning of the financial crisis. The financial and banking systems thus started a process of defining ethical values with the aim of setting up organizational defenses in the internal control system, with the specific purpose of making a preventive analysis of all possible consequences, legal, reputational, and operational.

The compliance function responds to these requirements. Basel Committee (2005) defines the "*compliance risk*" as "*the risk of legal or regulatory sanctions, material financial loss, or loss to reputation a bank may suffer as a result of its failures to comply with laws regulations, rules, related self-regulatory organization, standards, and codes of conduct applicable to its banking activities.*" The compliance function checks that the organization respects rules, regulations, and laws at all levels, both internal (self-regulation) and external (from authorities). In order to obtain the best results, compliance should be part of the culture of the organization; not just the responsibility of specialist compliance staff. All employees should work in line with compliance standards, but a bank will be able to manage better its compliance risk if it has inside the organization an effective compliance function.

In order to help banks and financial intermediaries to set up an effective compliance program, the Basel Committee issued guidelines in 2005. The document highlights the principles regarding the Board of Director and senior management responsibilities and the characteristics of the compliance function. It includes an in-depth analysis of the independence and the relationship between compliance function and the other control functions, such as the Internal Audit.

Like the control culture, compliance also needs to start at the top. It will be most effective in a corporate governance culture where top managers and BoD emphasize standards of honesty and integrity. It should be seen not as an obstacle in the organization, but as an integrated part of the business activities. Only when compliance becomes an integral part of the corporate culture at all levels can compliance risk be managed correctly.

A compliance function, to be effective, should be independent from the other functions of the organization. The Basel Committee (2005) states that to be independent, it should follow four criteria: first, "*the compliance function should have a formal status within the bank; second, there should be a group compliance officer or head of compliance with overall responsibility for co-ordinating the management of the bank's compliance risk; third, compliance function staff, and in particular, the head of compliance, should not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have; fourth, compliance function staff should have access to the information and personnel necessary to carry out their responsibilities.*"

So the concept of a culture of compliance has been present for more than a decade. Its importance and the importance of compliance risk management for establishing an effective internal control system and sound risk management is often acknowledged by regulators. However, continuing compliance and ethics scandals show that it is still dramatically lacking in many organizations (See Box 5.2). The problem does not always lie in the compliance function itself, but sometimes in an individual employee. A high profile bank should, however, be capable of ensuring the ethics of its own compliance staff at all organizational levels. If serious damage can be done by just one "bad apple," there are clearly problems with the culture of compliance in such cases.

Box 5.2. Cases of failures of culture of compliance

This insert shows several examples of failure of culture of compliance during the last decade. In all cases, banks or financial intermediaries failed in their compliance programs and were fined for breaking the law, mainly money laundering legislation.

In December 2016, ***Intesa San Paolo Bank*** *was fined $2.35 million by the US Authority. It was found guilty of bypassing the laundering controls from 2002 to 2006 and using opaque practices in about 2700 clearing transactions in US dollars with Iranian clients.*

At the end of 2016, ***Department of Financial Services fined the Agricultural Bank of China*** *$215 million for violation of money laundering laws and masking potentially suspicious financial transitions. The bank was also required to install an independent monitor in order to reinforce its* ***internal control system and compliance function.***

In summer 2016, the NY Department of Financial Services also fined the Commercial Bank of Taiwan $189 million for violation of ***New York money laundering state laws.***

In 2015, ***MoneyGram's chief compliance officer*** *was fined for $1 million for failure to adequately address significant money laundering activity.*

Two of Sweden's banks were tried in 2015 for violation of money laundering laws. ***Noredea bank was alleged not to have detected attempts to launder money and finance terrorism*** *and was fined SKr 50 million. Nordea had already been fined in 2013* ***for a previous problem of compliance with money laundering*** *regulations, and was told to* ***improve its compliance programs and repair the major deficiencies in current compliance practices.*** *In the same way, regulators fined Handelsbanken SKr 35 million for failing to conduct risk assessments of their clients. This failure could lead to a high risk and clients could exploit this failure for purposes of money laundering.*

Another example of compliance program failure was JPMorgan Chase which in 2014 ***was fined for violation of the Secrecy Act,*** *linked to the failure of the report of the multi/billion dollar fraud of the Mardoff Ponzi scheme. In January 2013, the OCC had already warned three affiliates of JPMorgan Chase to* ***improve their compliance programs and improve weaknesses***.

In December 2012, ***HSBC was accused of conducting transactions*** *on behalf of customers in Cuba, Iran, Libya, Sudan and Burma. It was fined $1.3 billion as part of a deferred prosecution agreement, and paid $665 million in civil penalties for helping to launder $880 million in drugs proceeds through the U.S. financial system.*

In 2012, ING was also fined $619 million for moving $2 billion on behalf of Cuban and Iranian entities. It was charged with violating the International Emergency Economic Powers Act and the Trading with the Enemy Act and the New York state laws.

Source examples of news published online[4]

To prevent such scandals, and protect the company from the possible penalties for noncompliance with the rules, it is important that banks build a foundation for a culture of compliance. It is important that all employees and the organization as a whole operate in line with compliance principles, in order to prevent the risk of operating illegally and incurring in the risk of a sanction. Table 5.2 outlines the main steps for having an effective culture of compliance throughout the organization.

Effective implementation of a compliance program is expensive and lengthy, but the cost of noncompliance is likely to be higher. Opting to be noncompliant, which is a matter of conscious choice, may lead

Table 5.2 The main steps of a culture of compliance

Steps	Definitions
Start with leadership	Board of Directors and Senior management should support and engage with the company's compliance efforts. They should specify integrity and honor values. Culture of compliance should start from the top
Align compliance with enterprise risk management	The compliance program should specify risks in each strategic area
Train and test	Companies should invest in the training and education of employees because education and skills are the basis of a sound culture of compliance
Incentivize ethical behavior	Employees are much more likely to learn when compliance is linked to remuneration. Employees will then incorporate policies and compliance directives into everyday activities
Do not ignore compliance errors	Mistakes are likely to occur a second time if they are not analyzed and acted upon. Violation of bank rules may also be an indication that the internal policy needs to be modified
Put effective technology in place	The right technology and data architecture, both within and outside the compliance function, can go a long way toward improving compliance efficiency and effectiveness. Automating controls can help lower costs and increase reliability, especially where there is a wide array of tools to support the compliance risk management process, either standalone or part of a wider solution.

Source www.deloitte.com and www.lockpath.com

banks to suffer heavy operational losses. Fines can be very high and can place the normal activity of the organization at risk. The best way to avoid problems with law is to improve the culture of compliance so that it becomes an inalienable part of the corporate culture. This may not solve all of a bank's problems, but banks should be able to show that

noncompliant employees are just that, rather than symptoms of a systemic problem.

The peculiarity of compliance risk compared to other risks is that it is closely linked to reputational, image, and strategic risk in having an impact on the entire organization. This means it should be managed ex-ante, with an emphasis on prevention rather than on sanctions for unethical or noncompliant behaviors. The culture of compliance is, in fact, one of the best tools to prevent unlawful behaviors among employees.

5.2 Internal Controls System and Risk Management in Banks After the Crisis

During the financial crisis, Financial Authorities started to pay more attention to bank risk governance, and new documents (EBA 2011; Bank of Italy 2013 and 2014) redefined the internal control and risk management framework. Moreover, in 2014, the Financial Stability Board (FSB) published its Guidelines on risk culture. Because weakness in risk culture is often considered to be a root cause of the global financial crises, these guidelines emphasize the importance of a sound risk culture. In particular, the FSB (2014) highlights that a sound risk culture should ensure an appropriate risk-reward balance consistent with the risk appetite declared in the Risk Appetite Framework. It highlights that a sound risk culture underpins a strong system of controls in line with the characteristics of the institution, the quality of data and models used by the institution and, finally, identification of all limit breaches and deviations from established policies.

Bank of Italy (2013) incorporated the EBA guidelines in Circular No. 263/2006, 15th amendment (subsequently included in Circular 285/13—1st amendment of May 2014, on prudential regulation according to CRD IV), which redefined the framework of internal governance. The new regulation contained many important innovations. The three different levels, first line control, risk controls, and internal auditing were retained, but the law also underlined the existence of the following three "line of defense:"

- Risk management systems: the process to identify, measure, control and manage risks of banks;
- Internal control systems: a system of effective controls is an important element of bank management and a foundation of good functioning;
- Internal audit: the most important aim of the internal audit function is to ensure the independence of the internal control system from all the other functions and members of the organization (IIA 2015).

The three line of defense are effective only if risk culture is a component of the internal control system. A sound risk culture in an organization arises from the repeated behavior of its members. Culture, behavior, and attitude are the three key components. Risk culture refines the concept of organizational culture to focus on the collective ability to manage risk. It is important for financial institutions because they need to take risks for achieving their objectives, and it impacts on the ability to take strategic risk decisions and deliver on performance promises.

Risk culture can be seen as a component of the internal control system, because dissemination of a sound risk culture and similar values among all members of a company make it possible to improve control over the different business lines. The propagation of company values means staff can operate in compliance with rules and beliefs of the organization, and take only appropriate and carefully considered risks.

In line with this, the FSB (2014) also emphasizes the important role played by sound risk culture. It notes that "*a sound risk culture should emphasize throughout the institution the importance of ensuring that: i) an appropriate risk-reward balance consistent with the institution's risk appetite is achieved when taking on risks; ii) an effective system of controls commensurate with the scale and complexity of the financial institution is properly put in place; iii) the quality of risk models, data accuracy, capability of available tools to accurately measure risks, and justifications for risk taking can be challenged, and iv) all limit breaches, deviations from established policies, and operational incidents are thoroughly followed up with proportionate disciplinary actions when necessary.*"

In order to achieve the best results from the risk culture, it is important to be aware of the main indicators:

1. a correct tone at the top;
2. strong accountability;
3. effective communication and challenge;
4. a sound remuneration policy.

In this case too, the tone at the top is set by top management (board of management and executive management) who disseminate the organization's values and risk culture. Only if they can show the whole organization at all levels that they are the first to respect the organization's values, can they promote a sound risk culture throughout the organization.

Accountability concerns the prompt identification, management, and escalation of emerging and unexpected risk issues. Accountability is important because successful risk management requires employees at all levels to understand the core values of the institution and its approach to risk. Employees should know their responsibilities and role inside the organization, and be aware that they are held accountable for their actions. A sound risk culture is the basis for an effective challenge in the organization and in the decision-making process.

Regarding effective communication and challenge, the bank should promote an environment where there is open discussion and where employees are encouraged to express their point of view, and which enables the professional growth of the individual employee and the team. Communications need to be open and effective and in order to improve the environment where employees operate.

Finally, in order to encourage employees in correct behavior in line with the organization risk culture, financial and nonfinancial incentives should be in line with the goals of the bank. The most important incentives are the promotion system and the remuneration policy. Risk management and compliance are important in charge with the hiring process, decisions about promotions and remuneration and they should underpin the development, appraisal, and evaluation of the entire organization.

The risk culture is the keystone of the financial institution. Risk culture is an important tool that can help to balance the operation of a business. Thanks to its risk culture, the company can create more value for its stakeholders, because it can operate in line with its strategy and can pursue higher levels of performance. It can also operate in line with its declared risk appetite and manage risks correctly (Protiviti 2013).

5.2.1 The First Line of Defense: Operational Management

The first line of defense is based on the business units that operate at the "lowest" level, in other words, the units in close contact with clients. These carry out different activities, from the production of goods to the provision of financial services, depending on the company type and the industrial sector (FSI 2015). In line with the kind of work, the control activities are granular and refer to the individual transaction. The aim of the first line of defense is to perform the first level of control and provide immediate notification to the appropriate management levels. In their day-to-day control, business units need to take into account the institution's risk tolerance/appetite and the policies, procedures, and controls (EBA 2011). The types of control are defined in the systems and process under the guidance of operational management, so the role of first line of defense is played by the operational management team (IIA 2013).

It is important to distinguish the two types of control that an operational manager can make; prevention and detection. In order to prevent any kind of undesirable actions, duties should be separated. For the purposes of prevention, proactive controls should be activated. Examples include approving payments for making purchases and ordering and accepting inventories, receiving bills and approving payments, authorizing returns and issuing refunds. Internal detection controls are designed to identify problems that really exist, and provide evidence that a loss has occurred. The main aim is to detect and correct errors or fraud. Examples of detection controls are monthly bank statements, review and verification of refunds, and supervision of petty cash accounts.

Both types of control are essential to an effective internal control system. Prevention is essential because it is proactive and emphasizes quality, while detection is important because it can confirm whether there has been a loss.

5.2.2 The Second Line of Defense: The Internal Control System

In a perfect world, a second line of defense would not be needed because the first line would be sufficient for effective risk management. In the real world, however, a single line is insufficient (IIA 2013).

The second line of defense aims to ensure effective control over the different functions and business lines. It is based on three different functions:

- A risk management function (and/or committee) aims to simplify and monitor the implementation of effective risk management practices;
- A compliance function aims to monitor various and specific risks. This function reports directly to senior managers;
- A controllership function that aims to monitor financial risks and financial reporting issues.

The responsibilities of these functions vary according to their specific nature. Table 5.3 reports the most important responsibilities.

The internal control system can be considered effective when it is able to recognize and assess the risk continually. It is fundamental that the internal control system is revised periodically and aligned with the new or previously uncontrolled risks. The second line of defense has to ensure that the first line can operate as intended (Schwizer 2013).

The financial crisis of 2007–2009 underlined the importance of sound risk management practices in the banking system. It showed clearly that banks are institutions that operate principally with risks. For this reason, a risk management framework able to identify, measure, control, and manage banks' risks is fundamental. The relationship

Table 5.3 Responsibilities of the second line of defense

Responsibilities
Supporting management policies, defining roles and responsibilities, and setting goals for implementation
Providing risk management frameworks
Identifying new and emerging issues
Identifying changes in the implicit risk appetite in the organization
Helping the management team into develop controls in order to manage risks and issues
Providing guidance and training on risk management processes
Making sure that risk management practices are effectively implemented by operational management, and continuously monitoring the process
If the risk scenario or regulatory change, the second line of defense must alert the operational management
Monitoring the adequacy and effectiveness of internal control, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies

Source IIA (2015)

between risk management and risk culture is very close, and in fact, one of the prerequisites for a strong risk culture is a comprehensive and independent risk management function under the direct responsibility of the Chief Risk Officer (CRO), or of senior management (EBA 2011).

Authorities, in fact, have given increasing attention to this and made efforts to improve the attention and the independence of the risk management function. One of the suggestions is the creation of risk committee in the Board of Directors, independent from other committees such as the control committee, and the requirement that a CRO be appointed.

Moreover, the Basel Committee 2015 guidelines on corporate governance for banks underline the importance of proper risk management procedures and specify that a sound risk management function must be independent and must be led by a CRO. The CRO should be of sufficient status, should be independent and he or she should have the access to the BoD. In recent years, the figure of CRO has become more important, and today the CRO reports to the CEO or directly to the Board of Directors in many banks (KPMG 2016). This shows

the increased importance attached to the risk management function in banks, because in the past the CRO usually reported to the CFO. Furthermore, the CRO can have the power of veto when present at meetings of a member of the BoD. Finally, the CRO should assess the coherence of single operations with the Risk Appetite Framework (RAF), defined and approved by the BoD (Schwizer 2016).

A recent Green Paper (European Commission 2010) also highlights certain recommendations with regard to the risk management function:

- delineating board-level responsibilities;
- creating a board-level risk supervision committee;
- defining a chief risk management who is familiar with the complexity of the organization;
- making sure that there is a cooperation between the risk supervision committee and the other parts of the firms, and also between the BoD and the supervisory authorities.

The risk management function and the compliance function both play a crucial role in the dissemination of risk culture. This is because the role of the two functions is to support management policies and indications, and because they play a monitoring role on the adequacy and efficiency of internal control system and the effectiveness of risk management practices.

The effective positioning of the risk management organization requires that the CRO should be a member of the Board of Directors and make available strategies, plans, transactions, and deals expected and respected by executive and line management (Protiviti 2013). In addition, the CRO is responsible for establishing and nurturing a learning culture with regard to risk. The CRO knows that improvement of policies and processes underpin any successful organization.

In conclusion, the second line of the defense function is separate from the first line, but is still under the control and direction of senior management and typically performs some management functions. The second line is essentially a management function taking responsibility for many aspects of the management of risk (IIA 2015). The second line of defense can be seen as an important tool in disseminating risk culture

among all levels of organizations. The tone from the top is not sufficient to achieve an effective risk culture; all control functions need to base their behavior on the risk culture guidelines defined by the BoD and senior managers.

5.2.3 The Third Line of Defense: The Internal Audit Function

The model proposed by the Bank of Italy (2013; 2014) provides for a third line of defense represented by the internal audit function.

The most important aim of internal audit function is to evaluate the effectiveness and efficacy of the internal control system of the organization. In the second line of defense, a high level of independence is not possible. But the third level provides assurance on the effectiveness of the governance, risk management, and internal controls. In order to be really independent, the internal audit function should not be directly involved in the choice of models and tools used to manage banking risks. In particular, the internal audit function reports directly to the board and senior management, and in bigger banks, a specific audit committee exists in the BoD.

One of the main goals of the internal audit function is to verify both the work of the compliance function and the work of risk management. In this second aspect, it is important to verify governance of aspects of risk management such as risk appetite, reporting systems, and disclosure.

Typically, the third line of defense has no management functions because it is required to protect its objectivity and organizational independence.

Finally, internal audit (IA) is also the function that maintains relations with the outside world and in particular with supervisors. The internal auditor should be independent from the other functions and should offer consultancy which is independent and objective, in order to add value and improve company's operations. IA is the third line of defense because it controls the work of the other lines and monitors the effectiveness of the entire internal control system. To achieve this

result, it is important to have a sound system of communication inside the organization which allows the internal audit to use all information and to have a clear overview of the company's risk and control framework. The responsibilities of the IA function include a key role in disseminating risk culture across different levels, particularly in consulting and assurance, depending on the complexity of the internal and external environment and the level of maturity of the organization. Obviously, it is crucial for IA to be supported by the Board of Directors in their role and responsibilities (Carretta and Schwizer 2015). In this way, the Board of Directors and the senior management can spread the risk culture through the internal control functions across all levels of the organization.

In order to achieve this aim, Internal Audit should include the risk culture of the organization within the scope of its corporate governance assessments, and it is useful to specifically mandate IA for this.

5.3 Conclusions

The concept of culture appeared before the financial crisis and authorities and regulators have talked about it for many years. It has been linked to many issues. Early on, it was linked to control; authorities focused on the "culture of control" and the internal control system was the most important tool to ensure good functioning of the banks. In a later phase, the "culture of compliance" was more talked about, and bank aim was broadly to operate according to internal and external rules. Compliance with rules means operating in line with the requirements of authorities and improving reputations. The implementation of compliance requirement is expensive, but operating in noncompliance can expose banks to higher costs in terms of fines and damage to reputation.

Finally, during the financial crisis, authorities and regulators issued many documents on the importance of a sound culture of risk. The correct definition of risk, the bank's risk appetite and risk tolerance became fundamental for an effective risk management and internal control system.

On one hand, regulators have defined guidelines and frameworks for banks and banks, on the whole, have well-defined internal control systems and a good risk management framework. However, recent events such as the Libor scandals, the failures of four Italian banks, and the manipulation of the exchange market, etc. are signs that regulation is not always enough to create an efficient system of controls.

The only way lying open to banks and financial intermediaries in order to reduce or eliminate negative events exposing them to fines, reputational risk, and sanctions is to disseminate a sound risk culture. This needs to be done with the help of the Board of Directors and senior management; the tone at the top is the key tool for banks in creating a strong risk culture. Only where a bank can define and disseminate values of integrity, honesty, and attention to the risks among all levels of the organization can the risk management function and internal control system achieve their objectives.

Notes

1. COSO (2004) provides a graphical representation of an Internal Control System. ICS is shown as a cube which depicts the interrelationships between the categories of objectives (top), the components of ICS (front), and the entity's business structure (side). This representation is also used for the Enterprise risk management system.
2. The other group of principles are: risk recognition and assesment; control activities and segregation duties; information and communication; monitoring activities and correcting deficiencies; evaluating of internal control systems by Supervisory Authorities.
3. https://www.theguardian.com/business/2011/oct/25/ubs-admits-internal-controls-failed.
4. https://www.ft.com/content/e8df0443-8d50-389f-a890-aa1b57d6f0a4; http://www.dfs.ny.gov/about/press/pr1611041.htm; https://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=17179875853 https://www.bloomberg.com/news/articles/2015-05-19/nordea-handelsbanken-fined-for-breaching-money-laundering-rules-i9uyxw7d http://www.bankinfosecurity.com/chase-a-6356

http://www.reuters.com/article/us-bnp-paribas-settlement-sentencing-idUSKBN0NM41K20150501
https://www.justice.gov/opa/pr/ing-bank-nv-agrees-forfeit-619-million-illegal-transactions-cuban-and-iranian-entities-0.

Bibliography

Basel Commitee on Banking Supervision. Framework for internal control systems in banking organization, September, 1998.

Basel Committee on Banking Supervision. Guidelines on corporate governance principles for banks. Issued for comments by 9 January, 2015, Consultative document.

Basel Committee on Banking Supervision. Compliance and compliance function in banks, April, 2005.

Carretta, Alessandro, and Schwizer Paola. *Risk Culture*. Milan, ITA: Associazione Italiana Internal Auditors (2015).

Compliance and Compliance Function in Banks, Basel Committee on Banking Supervision, April, 2005.

Corporate Governance in Financial Institutions: Lessons to be Drawn from the Current Financial Crisis, Best Practices. Accompanying Document to the Green Paper "Corporate Governance in Financial Institutions and Remuneration Policies {COM(2010) 284 Final}", European Commission, Brussels, June 2, 2010.

Creating a Robust Risk Culture: Evolving Role of the CRO, KPMG, February 17, 2016.

Direttiva 213/36/UE del Parlamento Europeo e del Consiglio (CRD IV), Banca d'Italia, 26 Giugno 2013.

Disposizioni di Vigilanza per le Banche, Regulation 285/2013, Banca d'Italia, 17 Dicembre 2013.

Directive 285, 17 December 2013, Banca d'Italia, 1st amendment of May 2014.

Enterprise Risk Management—Integrated Framework, Executive Summary, Committee of Sponsoring Organizations of the Treadway Commission, September, 2004.

Establishing and Nurturing an Effective Risk Culture. Fourth in a Series, Online http://www.protiviti.com/en-US/Documents/White-Papers/Risk-Solutions/

CRO-Series4-Establishing-and-Nurturing-an-Effective-Risk-Culture-Protiviti.pdf, Protiviti, 2013.

European Commission. Corporate Governance in Financial Institutions: Lessons to be drawn from the current financial crisis, best practices. Accompanying document to the Green Paper "Corporate governance in financial institutions and remuneration policies {COM(2010) 284 final}", SEC(2010) 669, Brussels, 2 June.ù, 2010.

Framework for Internal Control Systems in Banking Organization, Basel Committee on Banking Supervision, September 1998.

Guidance on Supervisory Interaction with Financial Institutions on Risk Culture. A Framework for Assessing Risk Culture, Financial Stability Board, 2014.

Guidelines on Corporate Governance Principles for Banks, Consultative Document, Basel Committee on Banking Supervision, 9 January, 2015.

Guidelines on Internal Governance, GL 44, European Banking Authority, September, 2011.

Internal Control—Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission, 1992.

Institute of internal auditors. The three lines of defense in effective risk management and control, Position Paper, January 2013, 2013.

Institute of internal auditors. 2015 Financial discussion and analysis, Report 2015, 2015. http://annualreport.theiia.org/reports/2015-financial-discussions-and-analysis.html#navbar.

Risk Culture Under the Microscope. Guidance for Boards, Institute of Risk Management, London, 2012.

Schwizer P. *Internal Governance*. Nuove regole, esperienze e best practice per l'organizzazione dei controlli interni nelle banche, EGEA, Milan, 2013.

Schwizer. Internal Control: tools and processes. In *Doing Banking in Italy: Governance, Risk, Accounting and Auditing issues*, Carretta A., Sargiacomo M. (edited by) (2016), McGraw-Hill, London, 2016.

The "Four Lines of Defence Model" for Financial Institutions, Occasional Paper n. 11, Financial Stability Institute, December, 2015.

The Three Lines of Defense in Effective Risk Management and Control. Position Paper, Institute of Internal Auditors, January, 2013.