- execution is a disciplined process, consisting of identifying information, analysis and evaluation, and documenting information, to achieve engagement's objectives – Statement 2300;
- quality of communications and disseminating results of engagement to proper parties are both needful to foster organizational improvement – Statement 2400;
- added value, effectiveness, and reputation should be measured not statically, on the amount of audits, but dynamically, on the basis of the accomplished improvements – Statement 2500;
- it is not the responsibility of the chief audit executive, but of the management, to resolve the risk – Statement 2600.

4. Main International Laws and Regulations on Governance, Risk, and Control: Institutional references for Internal Auditors

Nicoletta Mincato

1. Premise

The greatest part of essential references for Internal Audit is made up of soft laws, guidelines, models set up by institutional committees (among others) that focus on risk assessment and control with reference to organizational, productive and economic factors. Therefore, from a business-oriented perspective, it is self-evident that such a system of rules must be taken into consideration together with other different requirements established by a certain (not necessarily large) number of hard laws issued from time to time by legislators of different countries.

The aim of this chapter is to offer an overview of the main laws and regulations that, from an international point of view, have had and still have a significant impact on how to design an internal control system as well as on how internal auditors carry out their activities and reach their main goals.

The need for companies to be compliant with an increasingly complex regulatory framework and the need for such regulations to be 'drilled down' in the processes through which business activities are carried out have made compliance and internal audit dramatically important and crucial, not only in order to ensure the achievement of enterprises' goals (in particular, in the end, a 'sustainable' profit), but also to avoid corporate liability as a

consequence of the non-compliance and/or of the occurrence of some negative events these regulations intend to prevent.

The reason for the increasing importance of compliance to hard and soft laws must be found in the commitment of companies, made compulsory by hard laws, to prevent corporate criminal offenses or misconducts that may have a major impact on the market and the stakeholders, in general.

Needless to say, the strict regulations on internal audit and internal control were the consequence of some well-known recent financial scandals that literally 'freaked out' the economy and productive system of some developed countries, such as the United States and Italy.

Nevertheless, some of the domestic and international laws, which are also part of the whole complex control system that is the specific topic of this chapter, either date back in time or are independent of the abovementioned scandals, because they introduced different forms of control in the companies' governance framework, to satisfy widespread interests that involve the transparency, efficiency and accuracy of the functioning of public administration with reference to business transactions (FCPA and U.K. Bribery Act) and the corporate liability for crimes (Legislative Decree 231/2001).

In particular, we will explore the first instances to be met by these regulations, their interconnections and their specificities to be explained in the different context in which they were introduced.

2. The Sarbanes–Oxley Act

The Enron scandal (occurred in 2001 in the market of energy and commodities) gave clear evidence of the problems related to the lack of transparency and its consequences on the stability of financial markets, creating a deep distrust of investors towards them.

The *Public Company Accounting Reform and Investor Protection Act* (also known as the 'Sarbanes–Oxley Act') is a U.S. Federal Law issued on July 30, 2002 as a legislative response to the need to improve corporate governance rules, to ensure accounting record's transparency and accuracy, to promote the quality of financial reporting by internal and external auditors, to enhance supervision on companies' management, thus, trying to prevent the occurrence in the future of other 'scandals' like the Enron's case.

As a matter of fact, the Sarbanes–Oxley Act (hereinafter referred to as SOX) introduced significant changes to companies' corporate governance discipline and financial markets' rules.

The main changes introduced by SOX with the aim of restoring investors' trust and shareholders' protection against possible frauds have been:

1. the introduction of a supervisory body on external auditors;
2. the introduction of effective control on audit companies and on their mutual links and/or relationships with the companies under their control;
3. the enhancement of corporate responsibility rules;
4. the introduction of new disclosure requirements for companies to ensure completeness, clarity and promptness of information to the market;
5. the improvement of quality and transparency of financial reporting and auditing activities;
6. the increase of penalties against managers found guilty of fraudulent behaviors;
7. the improvement of the Security and Exchange Commission's powers.

In order to assure the widest enforcement of such provisions, SOX is applicable to:

a) U.S. companies listed on NYSE and NASDAQ; and
b) foreign companies that issue securities and are subject to compulsory "*registration*" (Sec. 12 SEA, 1934) or "*reporting*"

(Sec. 15 (d)) to SEC (thus, meaning that it is applicable also to Italian companies listed on NYSE or belonging to international groups listed on U.S. markets).

Even though SOX is a complex system of provisions, we will hereby focus on some specific topics that turn out to be particularly relevant and represent a benchmark for auditors and internal auditing. In particular:

- inside the board of directors of listed companies, some of the directors, all being independent, form the Audit Committee that has to meet the requirements of Rule 10A-3 of the Security Exchange Act and Section 301 of SOX, representing an important part of the internal control system and having the following main tasks:
  a. the supervision of company's accounts;
  b. the verification of the company's compliance to laws and regulations;
  c. the appointment of external auditors, determining their compensation, verifying their activities, and authorizing them to carry out further consulting activities for the company, on condition that this does not compromise the quality of their auditing;
  d. the implementation in the adoption of procedures to manage information on accounts, internal control and auditing activities coming from any function of the company itself as well as the so-called 'whistleblower process';
- a certification given by CEO and CFO (under their civil and criminal liability) is aimed at certifying that: (i) annual and quarterly reports meet the requirements imposed by the Security Exchange Act, that is, they "fairly present" (SOX, 2002, Sec. 906) the company's financial conditions (the so-called 'civil certification'); and (ii) any periodic report on company's financial situation "fairly presents [...] in all material respects" (SOX, 2002, Sec. 906) the company's financial conditions (the so-called 'criminal certification').

Along with these material changes and as a result of them, SOX also establishes that it is the liability of management to ensure the company be provided with an adequate system of internal control, whose adequacy and effectiveness must be verified periodically, in order to give "reasonable assurance" (SOX, 2002, Sec. 103) of its global effectiveness. Furthermore, it is necessary for the company and its management to keep evidence both of the controls carried out and the periodical evaluation of the effectiveness and adequacy of the systems of control as a whole.

In particular, SOX introduces the 'new' concept of "integrated audit" (the abovementioned certifications of CEO and CFO also deals with this matter). Indeed, Sec. 404b provides that audit activities on financial statements and on internal control must be carried out together, because their respective contents are strictly and mutually related, as they influence each other. The output of such 'integrated' work will consist of three opinions, to be considered as a whole, with reference to:

1. the effectiveness of internal control on financial reporting;
2. the effectiveness of the management evaluation on its internal control over financial statements;
3. the financial statements.

Hence, SOX has been a forerunner and a fundamental reference to some further regulations and laws that subsequently came into force in many foreign countries. In general, the increasing attention of legislators – in addition to institutional committees and organizations – placed on the system of internal controls and its crucial relevance in a value-creation perspective is, to a certain extent, a 'by-product' of SOX.

As far as the Italian legislation is specifically concerned, we will see how Law 262/2005 and, later, Legislative Decree 39/2010 have both strong connections with the provisions of SOX. Some interesting interconnections might also be found between SOX and Legislative Decree 6/2003 (the so-called 'Riforma Vietti' of corporate law set forth by the Italian Civil Code).

(Sec. 15 (d)) to SEC (thus, meaning that it is applicable also to Italian companies listed on NYSE or belonging to international groups listed on U.S. markets).

Even though SOX is a complex system of provisions, we will hereby focus on some specific topics that turn out to be particularly relevant and represent a benchmark for auditors and internal auditing. In particular:

- inside the board of directors of listed companies, some of the directors, all being independent, form the Audit Committee that has to meet the requirements of Rule 10A-3 of the Security Exchange Act and Section 301 of SOX, representing an important part of the internal control system and having the following main tasks:
  a. the supervision of company's accounts;
  b. the verification of the company's compliance to laws and regulations;
  c. the appointment of external auditors, determining their compensation, verifying their activities, and authorizing them to carry out further consulting activities for the company, on condition that this does not compromise the quality of their auditing;
  d. the implementation in the adoption of procedures to manage information on accounts, internal control and auditing activities coming from any function of the company itself as well as the so-called 'whistleblower process';
- a certification given by CEO and CFO (under their civil and criminal liability) is aimed at certifying that: (i) annual and quarterly reports meet the requirements imposed by the Security Exchange Act, that is, they "fairly present" (SOX, 2002, Sec. 906) the company's financial conditions (the so-called 'civil certification'); and (ii) any periodic report on company's financial situation "fairly presents [...] in all material respects" (SOX, 2002, Sec. 906) the company's financial conditions (the so-called 'criminal certification').

Along with these material changes and as a result of them, SOX also establishes that it is the liability of management to ensure the company be provided with an adequate system of internal control, whose adequacy and effectiveness must be verified periodically, in order to give "reasonable assurance" (SOX, 2002, Sec. 103) of its global effectiveness. Furthermore, it is necessary for the company and its management to keep evidence both of the controls carried out and the periodical evaluation of the effectiveness and adequacy of the systems of control as a whole.

In particular, SOX introduces the 'new' concept of "integrated audit" (the abovementioned certifications of CEO and CFO also deals with this matter). Indeed, Sec. 404b provides that audit activities on financial statements and on internal control must be carried out together, because their respective contents are strictly and mutually related, as they influence each other. The output of such 'integrated' work will consist of three opinions, to be considered as a whole, with reference to:

1. the effectiveness of internal control on financial reporting;
2. the effectiveness of the management evaluation on its internal control over financial statements;
3. the financial statements.

Hence, SOX has been a forerunner and a fundamental reference to some further regulations and laws that subsequently came into force in many foreign countries. In general, the increasing attention of legislators – in addition to institutional committees and organizations – placed on the system of internal controls and its crucial relevance in a value-creation perspective is, to a certain extent, a 'by-product' of SOX.

As far as the Italian legislation is specifically concerned, we will see how Law 262/2005 and, later, Legislative Decree 39/2010 have both strong connections with the provisions of SOX. Some interesting interconnections might also be found between SOX and Legislative Decree 6/2003 (the so-called 'Riforma Vietti' of corporate law set forth by the Italian Civil Code).

3. The internal controls in the Italian legislation

Legislative Decree 6/2003 is rarely considered when discussing internal control systems, but it is for sure the first significant intervention Italian legislators carried out in order to redefine the corporate governance framework. The issues addressed by Legislative Decree 6/2003 specifically refer to organizational models of managing and control, with the purpose to give Italian companies the possibility to choose among alternative governance systems and, at the same time, to simplify corporate regulations to facilitate access to financial markets. Nevertheless, it must be acknowledged that internal control systems owe something to this Decree.

The corporate governance system designed by Legislative Decree 6/2003 comprises three different models that both listed and unlisted companies can decide to adopt: in addition to the 'traditional' system based on the co-existence of a board of directors and a Supervisory board ('*collegio sindacale*'), the latter completely independent and separated from the first and with specific control tasks – in particular with reference to the organizational, administrative and accounting framework of the company and to its actual functioning –, the legislators have introduced a one-tier board ('*monistico*') and a two-tier board ('*dualistico*') system, drawing inspiration from the typical foreign European models of the U.K. and Germany.

Both systems imply a dialectic relationship between a body, whose main task is to manage the company (even through the definition of its organizational framework), and another body in charge of supervising and evaluating how the company is managed and organized.

Despite a quite clear distribution of functions and duties between corporate bodies, achieved through the 2003 reform in order to set up the basis of an internal control framework – according to the characteristics of each governance system –, after

Legislative Decree 6/2003, a certain number of laws and regulations has had a significant impact on the systems of internal control, providing for a large number of bodies responsible for the implementation and accomplishment of internal controls, sometimes, implying duplication of tasks, potential inefficiencies, and relevant and (occasionally) undue compliance costs for the listed companies.

This said, a clear definition and regulation of internal controls is even now set forth only at a soft law level, that is, in the Corporate Governance Code (Codice di Autodisciplina, 2015), whose Principle 7.P.1. states that any listed company:

> *[...] shall adopt an internal control and risk management system consisting of policies, procedures and organizational structures aimed at identifying, measuring, managing and monitoring the main risks. Such a system shall be integral to the organizational and corporate governance framework adopted by the issuer and shall take into consideration the reference model and the best practices that are applied both at national and international level.*

The introduction of the Corporate Governance Code in the market had positive effects, since it forced Italian companies to converge towards international standards of governance.

However, we must promptly highlight that the Code is mainly based on the one-tier board structure ('*sistema monistico*'), even though the vast majority of Italian companies adopts the traditional governance system based on the Board of Directors and the Supervisory Board ('*collegio sindacale*'). Therefore, the Code's application entails the introduction in the traditional system of features that are typical of the one-tier system, such as independent directors and internal committees as 'actors' of the internal control framework, with the consequent (comprehensible) difficulty to clearly distinguish the different roles of Supervisory Board and board committees.

It is important to highlight that it is generally up to the listed companies whether to be compliant or not with the Corporate

Governance Code (it is compulsory only in a small number of cases, as to be listed in the S.T.A.R. segment of the Borsa Italiana). Nevertheless, most Italian companies are compliant and have decided, on a voluntary basis, to adopt an internal control system as set up by the Code, thus, enhancing its positive effect on the whole corporate governance.

A law with a strong link with SOX that has become a reference to internal audit in Italy is undoubtedly Law 262/2005, which represents the first reaction of Italian legislators to some financial scandals (such as those of Cirio and Parmalat) through the introduction of some measures aimed at strengthening the internal control system and improving the quality of financial reporting.

Law 262/2005 sets up a series of requirements listed companies have to comply with, whose basic principles are the same as SOX, and focus on the importance of evaluation, constant control, documentation, correction of inefficiencies, and certification with reference both to the internal control system and to the financial reporting.

In short, Law 262/2005 introduced:

- the certification of the Manager in charge of preparing financial reports on all acts and information provided to the market as far as their conformity to accounting records is concerned;
- the commitment for companies to have adequate administrative and accounting procedures for the processing of financial statements and any other financial report, arranged by the manager in charge of preparing financial reports;
- the certification on the adequacy and effective application of such procedures made by the managing directors and by the manager in charge of preparing financial reports;
- the certification on the correspondence of financial statements to accounting books and records, in compliance with the Regulations issued by CONSOB.

The corporate governance system, as designed by Legislative Decree 6/2003, at first, and then by other laws up to Legislative Decree 39/2010 – as we will see hereinafter –, has increasingly assumed a configuration where subjects or entities that manage the company are confronted with subjects and entities that are in charge of monitoring it from several points of view.

Table 4.3.1 below briefly summarizes the main actors of this system and their respective roles:

Table 4.3.1 Main actors in the corporate governance system and their respective roles, as designed by Legislative Decree 6/2003, at first, and then by other laws up to Legislative Decree 39/2010.

Body	Functions
Board of Directors	– Evaluates the adequacy of the internal control system and its effectiveness; – appoints: a) the director charged with the task of setting up and implementing an effective internal control system; b) the Audit and Risk Committee; c) the person charged with Internal Audit (on advice of the Audit and Risk Committee and after having consulted Supervisory Body).
Internal Audit	– Checks the correct functioning and the adequacy of the internal control system, following an Audit plan based on prioritization of risks; – checks the reliability of IT systems for accounting recognition.
Supervisory Board	Controls the effectiveness of internal control systems (also as Internal Control and Audit Committee).
Audit and Risk Committee (made of independent directors; at least one of them is experienced in accounting or risk management)	– Evaluates, together with the manager in charge of preparing financial reports, the fair use of accounting principles, after consulting the external auditor and the Supervisory Board; – gives opinions on specific aspects regarding the identification of the main risks; – examines the periodic reports of Internal Audit; – verifies the independence, adequacy, effectiveness, and efficiency of Internal Audit.

Body	Functions
Director in charge of internal control and risk management	– Identifies the main risks and submits them to the examination of the Board of Directors; – applies the guidelines set by the Board of Directors, handling the design, implementation, and management of the internal control system and checking its adequacy and effectiveness; – can ask the Internal Audit for verifications; – reports to the Audit and Risk Committee on problems and critical issues.
Manager in charge of preparing financial reports	– Sets up, in collaboration with the responsible functions, adequate administrative and accounting procedures for the preparation of the financial statements and any other financial document; – issues certificates and legal statements with reference to periodic accounting documentation and information.

One of the most recent and relevant interventions of the Italian legislators is Legislative Decree 39/2010, which implemented Directive 2006/43/CE (the so-called 'Audit Directive') and set up a complete discipline of audit activities with reference to accounting, by dividing the areas of competence between the Supervisory Board (internal auditors) and the external Auditors.

In particular, as per Article 16, Paragraph 2 of Legislative Decree 39/2010, in "public interested entities, [...] the statutory audit cannot be entrusted to the Supervisory Board"[2] because in such entities – as provided by article 19 of the same Decree – "the body that monitors the management is (also) charged with the role of Internal Control and Audit Committee",[3] with specific tasks.

[2] Translation mine. Original: "Negli enti di interesse pubblico, [...] la revisione legale non può essere esercitata dal collegio sindacale" (Legislative Decree 39/2010, art. 16, par. 2).

[3] Translation mine. Original: "Il comitato per il controllo interno e la revisione contabile si identifica con: a) il collegio sindacale" (Legislative Decree 39/2010, art. 19, par. 2).

Hence, in the traditional system of governance, the Supervisory Board, should the company be qualified as a 'public interested entity', monitors:

- the financial reporting process;
- the effectiveness of internal control, internal audit (if applicable) and risk management systems;
- the statutory audit on annual and consolidated accounts;
- the independence of auditors/audit firm, especially as far as the provision of non-audit services to the same audited entity is concerned.

The Legislative Decree also establishes a strict relationship between the Supervisory Board (i.e., Internal Control and Audit Committee) and the external auditors, whose specific task – in addition to the others – is to "report to the Internal Control and Audit Committee the main issues revealed during the statutory audit activity, in particular with reference to any relevant deficiency found in the internal control system related to financial reporting process".[4]

The above-examined provisions, on the one hand, increase the number of 'actors' in the internal control framework – also including the support of an external subject (the Auditor) in evaluating the adequacy and effectiveness of the internal control system; on the other hand, they promote the role of the Supervisory Body as a 'real player' in the internal control system, despite the many tasks and powers given to the other bodies, as outlined in the chart above.

In conclusion, the whole framework defined by laws and soft law regulations is a complex system that requires the creation

[4] Translation mine. Original: "Il revisore legale o la società di revisione legale presenta al comitato per il controllo interno una relazione sulle questioni fondamentali emerse in sede di revisione legale, e in particolare sulle carenze significative rilevate nel sistema di controllo interno in relazione al processo di informativa finanziaria" (Legislative Decree 39/2010, art. 19, par. 3).

and the correct interplay of many different committees/bodies, which are asked to cooperate and be efficient in creating and implementing the internal control system as defined by such laws and regulations.

4. The internal controls deriving from the fight against illegal practices of bribery and corruption

As correctly argued in Chapter 1, companies nowadays are urged by stakeholders and the market as a whole to adopt efficient measures against bribery and corruption. Even though some of the regulations provided by some countries are not a novelty and date back to the 1970s, they have become suddenly and dramatically current in recent times, as a consequence of some major scandals and the demand for Corporate Social Responsibility.

What is interesting is that, in a globalized market, the most harmful consequences of bribery for companies, both in terms of damages to their image and reputation, and in terms of economic losses, are perceived in connection with international bribery.

The most accurate and interesting regulation on the subject is the Foreign Corrupt Practices Act (FCPA), a federal law enforced by SEC (Security and Exchange Commission) and DOJ (Department of Justice), initially issued in 1977 and subsequently revised in 1988 and 1998.

According to the Guide to the FCPA issued jointly by SEC and DOJ, the main purpose of this federal law is to make it illegal for companies and/or natural persons acting on behalf of companies to influence any foreign officials or parties with any personal payments or rewards.

The United States Senate, when issuing FCPA in 1977, gave a compelling definition of international bribery and its adverse effects on fair competition (Committee on Banking, Housing, and Urban Affairs United States Senate 1977 (a. title i): 4):

> *Corporate bribery is bad business. In our free market system it is basic that the sale of products should take place on the basis of price, quality and service. Corporate bribery is fundamentally destructive of this basic tenet. Corporate bribery of foreign officials takes place primarily to assist corporations in gaining business. Thus foreign corporate bribery affects the very stability of overseas business. Foreign corporate bribes also affect our domestic competitive climate when domestic firms engage in such practices as a substitute for healthy competition for foreign business.*

The application of FCPA is both based on the nationality principle, according to which it applies to U.S. business, foreign corporations trading securities in the U.S., American nationals, citizens, residents (whether or not physically present in the U.S.); and on the protective principle, which covers foreign natural and legal persons in case they are in the U.S. at the time of the corrupt conduct.

The FCPA is divided into two main sections, the first one dealing with accounting provisions, while the second one with anti-bribery provisions. In the following paragraphs, we will focus on the latter set of provisions but, needless to say, there is a strict connection between the two sets of provisions, since corporate bribery is often concealed through the falsification of corporate books and records as bribes can be mischaracterized as commissions or royalties, consulting fees, intercompany accounts, etc.

The general provision set forth in FCPA (§§ 78dd-1, 78dd-2, 78dd-3) is aimed at prohibiting issuers (their officers, directors, employees or agents), domestic concerns and others subjects acting in the territory of the U.S., to offer to pay, pay, promise to pay, authorize the payment of money or any other value to a foreign official or a foreign political party in order to influence any act or decision in their official capacity, induce them to do or omit any act in violation of their lawful duty or to secure any other improper advantage in order to obtain or retain business. Such payments are prohibited by the FCPA even if made through third parties or intermediaries, when aware that all or a portion

of such money will be offered, given or promised to a foreign official.

It has to be highlighted that companies that merge with or acquire another company assume the predecessor company's (civil or criminal) liabilities. FCPA violations are no exception to this rule.

FCPA provides, however, an important exception in the so-called facilitating or expediting payments, whose purpose is to expedite or secure "the performance of a routine governmental action" (FCPA, § 78dd-2-b), as in the case of obtaining permits or licenses. Such payments are not included in the general prohibition set forth in §§ 78dd-1, 78dd-2, and 78dd-3. Furthermore, the FCPA considers as affirmative defenses the fact that the payment is allowed by written laws and regulations of the foreign official's country or the fact that it is a *bona fide* expenditure, such as travel and lodging expenses incurred by the foreign official.

Several years after the FCPA, another law aimed at fighting against bribery was issued in 2010 and came into force in 2011: the U.K. Bribery Act, issued by the Parliament of the United Kingdom.

The most relevant differences between the two laws find their explanations in the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, adopted in 1997 by the Organization for Economic Cooperation and Development (OECD) that greatly influenced all the laws and regulations of the European countries in the subject matter.

Unlike the FCPA, the U.K. Bribery Act regulates and sets a discipline both for the offense of bribing another person and for the offense of being bribed. The description of the unlawful conduct consisting in bribing another person is quite similar to the one provided for in the FCPA but the bribery is aimed at influencing the performance of a "relevant function or activity" (Bribery Act, 2010, Sec. 1, par. 2, lett. b). The definition of relevant function or activity is not only related to any function of public nature, but also any activity connected with a business (both trade and profession) or performed in the course of a person's employment. Such function or activity should be carried out in good faith, impartially, and in a position of trust by virtue of performing it, regardless the fact that the activity has connection with the U.K. or is performed in a country outside the U.K.

A section of the U.K. Bribery Act is dedicated to the bribery of foreign public officials (Bribery Act, 2010, Chap. 23, Sec. 6). However, what is more significant, especially from the point of view of risk control in managing a company, is the fact that the provisions of the U.K. Bribery Act do not only apply to individuals/employees, but they also apply to the company itself, which is strictly liable, despite the evidence of any kind of intention or positive action. The introduction of this form of corporate liability can be considered a true revolution in the area of corporate criminal law, and the U.K. was not the first European country to introduce it in order to fulfill a requirement of the abovementioned OECD Convention. Among the regulations set forth by European countries, the Italian Legislative Decree 231/2001 is one of the most interesting and it was issued much earlier than the U.K. Bribery Act. Differently from the U.K. Bribery Act, this decree is not exclusively focused on bribery, but we will discuss this in greater details later. However, for the time being, it is important to highlight that the mechanisms through which corporate liability for certain offenses works are nevertheless very (though not thoroughly) similar.

According to the U.K. Bribery Act, a commercial organization incorporated under the U.K. law or even simply carrying on a business in the U.K. is found guilty if a person associated with such commercial organization, who performs services for or on behalf of it in whatever capacity (employee, agent, subsidiary), bribes another person in order to obtain/retain business for the organization or, more generally, in order to obtain/retain an advantage in the conduct of business. In order to avoid prosecution

under the U.K. Bribery Act, the commercial organization must produce evidence of the fact that it has in place adequate procedures designed to prevent bribery that must have been outlined according to the six main principles set out by the U.K. Bribery Act:

- Principle 1: proportionate procedures;
- Principle 2: top-level commitment;
- Principle 3: risk assessment;
- Principle 4: due diligence;
- Principle 5: communication and training;
- Principle 6: monitoring and review.

The release of these procedures inevitably introduces a new benchmark for internal audit, since they become a relevant part of internal control systems.

As previously said, in Italy, Legislative Decree 231/2001, introduced some years before the U.K. Bribery Act, sets out principles and provisions that are quite similar to the ones set forth by the British law.

Legislative Decree 231/2001, however, does not simply oppose bribery of public officials (and, more recently, also of private officers) with reference to business transactions: the corporate liability provided thereto is indeed aimed at discouraging companies' misconducts, first and foremost, in relation to public administration and, in general, in relation to the interests of any stakeholder deserving protection (for example, as for safety at work, environmental issues, etc.).

Undoubtedly, the very first instance that led Italian legislators to adopt such regulation, in accordance with the OECD Convention of 1997, was the combating of bribery and corruption of public officials. However, the mechanism of corporate administrative-law liability arising from personal criminal-law liability – given certain predetermined conditions – has turned out to be very useful also to prevent other crimes (e.g., predicate offenses) as long as they are committed in the sole interest or

to the advantage of the company. In other words, once certain values are considered as deserving protection and companies are identified as the real responsible for offenses to these values, the Legislative Decree 231/2001 has been used as an efficient tool to prevent the commission of some crimes. Such result is the consequence of:

a. some 'protocols' (i.e., some principles the company must comply with in carrying out its activity) defined and implemented inside the organization of the company itself;
b. severe forms of punishment set forth by the Decree with reference to the company.

As in the case of the U.K. Bribery Act, the system provided for by the Italian legislators focuses on the adoption by companies of organizational measures in compliance with laws, guidelines, and judgments' directives. The compliance and control framework set out by the Legislative Decree 231/2001, with the aim of avoiding or limiting corporate liability, is based on the same principles outlined by the U.K. Bribery Act, which may be summarized in the following points:

- the adoption and efficient enactment, prior to commission of the act, of organizational and management models that are capable of preventing offenses of the type occurring through the identification of the activities in relation to which offenses may be committed;
- the provision for specific protocols and procedures for taking decision and for managing financial resources;
- the obligation to disclose information to the Supervisory Board;
- the appointment of a Supervisory Board, which is entrusted with:
  a) supervising the effectiveness and efficiency of the internal system, in terms of adequacy and suitability, to prevent predicate offenses from being committed, and its compliance with the Model, in terms of actual application;

b) updating the Model: the Supervisory Board is responsible for giving company's top management notice of the occurrence of conditions requiring the amendment and/or supplementation of the Model, which is a dynamic document;
c) administering training activities, thus, determining and governing the 'flow of information' from and to the Supervisory Board itself and taking appropriate initiatives aimed at promoting the knowledge of the Model and of its provisions within the company.

The company is not considered liable under Legislative Decree 231/2001 and the requirements provided by law for liability's exemption are met if:

- it adopts a Model capable of preventing the commission of predicate offenses;
- it appoints the Supervisory Board;
- the Supervisory Board has properly fulfilled its tasks of supervision;

UK BRIBERY ACT 2010	FCPA 2003	D. Lgs. 231/2001
Provides for a defense for commercial organizations, consisting of adopting compliance programs	The adoption of compliance programs only allows a reduction of penalty	Provides for a defense for commercial organizations, consisting of adopting compliance programs
It concerns any kind of bribery, whoever the bribed person is	It only concerns bribery of foreign public officials	It concerns any kind of bribery, whoever the bribed person is
The company is responsible for adopting adequate compliance programs (strict liability)	The company is responsible for adopting an adequate accounting system	The company is responsible for adopting adequate compliance programs (strict liability)
No execption: payments to obtain or retain business in an improper manner are banned	Payments considered as legal under the local laws and regulations are allowed also under FCPA	
Facilitation payments are banned	Facilitation payments to facilitate routine governmental acts are allowed	

Figure 4.4.1 A summary showing the differences between the U.K. Bribery Act, the FCPA 2003, and the Italian Legislative Decree 231/2001.

- in order to commit the offense, the Model was fraudulently circumvented.

The Supervisory Board, in particular, is a 'corporate body' that operates in a steady and continuous way and must be provided with autonomous powers of initiative and control (Legislative Decree 231/2001, art. 6, par. 1, lett. b) to carry out the abovementioned activities.

In conclusion, even though Legislative Decree 231/2001 sets up basic principles of internal control that specifically concern the corporate's criminal liability, the whole internal control system is influenced and, from a different point of view, enhanced and completed by the '231 framework'. For this reason, the Supervisory Board must be considered, in most respects, one of the active players of internal control, even if its role is mainly focused on the '231 framework'.