COMPLIANCE KEYS MONOGRAPH

MOLINS

Compliance

INDEX

Main definitions in the field of Compliance

- **Corrective action:** Action to eliminate the causes of a nonconformity or noncompliance and prevent its recurrence.

- **Senior management:** Person or group of persons who direct and control an organization at the highest level.

- **Audit:** Systematic and independent process for obtaining evidence and evaluating it objectively to determine the extent to which audit criteria are met.

- **Competent authority:** Any authority designated to receive complaints and to respond to complainants, and/or designated to perform Compliance functions, in particular with regard to follow-up.

- **Internal reporting channel:** Any internal reporting channel available to an entity to enable reporting of breaches of European Union law.

- **Competence:** The ability to apply knowledge and skills to achieve the intended results.

- **Compliance/Fulfillment:** The fulfillment of the organization's compliance obligations, both external and self-imposed.

- **Conflict of interest:** A situation in which business, financial, family, political, personal or external interests could interfere with the judgment of the organization's members when carrying out their duties in the organization.

- **Compliance:** Fulfillment of a requirement.

- **Work context:** Present or past work activities in the public or private sector through which, regardless of the nature of those activities, individuals may obtain information about violations and in which those individuals could suffer retaliation if they disclosed such information.

- **Compliance culture:** Values, ethics, beliefs and behavior that exist in an organization and that interact with the organization's structures and control systems to produce norms of behavior that lead to compliance.
- **Whistleblowing:** The verbal or written communication of information about violations.

- **External whistleblowing:** The verbal or written communication of information about violations to the competent authorities.

- **Internal whistleblowing:** The verbal or written communication of information about violations within a legal entity in the private or public sector.

- **Whistleblower:** A natural person who publicly communicates or discloses information on violations obtained in the context of his or her work activities.

- **Performance:** Measurable result.

- **Effectiveness:** Degree to which planned activities are carried out and planned results are achieved.

- **Outsourcing:** Agreement whereby an external organization performs a function or process of the organization.

- **Facilitator:** A natural person who assists a whistleblower in the whistleblowing process in a work context, and whose assistance must be confidential.

- **Compliance function:** Person or group of persons with responsibilities and authorities for the operation of the compliance management system.

- **Public official:** Any person holding a legislative, administrative or judicial office, whether appointed by succession or elected, or any person exercising a public function, including for a public agency or for a public company, or any officer or agent of a public national or international organization or any candidate for public office.

- **Information about violations:** Information, including reasonable suspicions, about actual or potential wrongdoing, which has occurred or is very likely to occur in the organization in which the whistleblower works or has worked or in another organization with which the whistleblower is or has been in contact in connection with his or her work, and about attempts to conceal such wrongdoing.

- **Violations:** Actions or omissions which: (i) are unlawful and relate to the acts and activities of the European Union, or (ii) distort the object or purpose of the rules laid down in the acts and activities of the European Union.

- **Infringements:** Actions or omissions that: (i) are unlawful and relate to the acts and policy areas of the European Union, or (ii) distort the object or purpose of the rules laid down in the acts and policy areas of the European Union.
- **Investigation:** All those actions aimed at verifying the verisimilitude of the facts reported through the Internal Information System.

- **Measurement:** The process of determining a value.

- **Continuous improvement:** Recurrent activity to improve performance.

- **Members of the organization:** The members of the governing body, managers, employees, workers or temporary employees or under collaboration agreement and volunteers of an organization and the rest of persons under hierarchical subordination of any of the above.

- **Non-conformity:** Non-compliance with a requirement.

- **Non-compliance with Compliance:** Non-compliance with Compliance obligations.

- **Objective:** Result to be achieved.

- **Compliance Obligations:** Requirements that an organization is obliged to comply with, as well as those that an organization voluntarily chooses to comply with.

- **Organization:** A person or group of persons having their own functions with responsibilities, responsibilities and relationships for the achievement of their objectives.

- **Compliance Body:** Body of the organization endowed with autonomous powers of initiative and control entrusted with the responsibility of supervising the operation and observance of the compliance management system.

- **Governing body:** A person or group of persons having ultimate responsibility and authority for the activities, governance and policies of an organization to whom senior management reports and is accountable.

- **Stakeholder:** Person or organization that may affect, be affected, or be perceived to be affected by a decision or activity.

- **Person concerned:** A natural or legal person referred to in the complaint or public disclosure as the person to whom the infringement is attributed or with whom the infringement is associated.

- **Personnel:** Individuals in a relationship recognized as an employment relationship under national law or practice, or in any contractual relationship whose activity is dependent on the organization.

- **Policy:** Intentions and direction of an organization as formally expressed by its top management.

- **Compliance Policy:** The will of an organization, as formally expressed by its senior management or governing body, in relation to its Compliance objectives.

- **Procedures:** Specific way of carrying out an activity or process.

- **Information management procedure:** Procedure that establishes the necessary provisions so that the Internal Information System and the existing internal information channels comply with the requirements.

- **Process:** A set of interrelated or interacting activities that use or transform inputs to produce outputs.

- **Register of information:** Book-record of the information received and of the internal investigations to which they have given rise, guaranteeing, in any case, confidentiality.

- **Retaliation:** Any action or omission that is prohibited by law, or that, directly or indirectly, involves unfavorable treatment that places the persons who suffer it at a particular disadvantage with respect to another in the work or professional context, solely because of their status as informants, or because they have made a public disclosure, unless there is objective justification.

- **Requirements:** Established need or expectation, usually implicit or mandatory.

- **Head of the internal information system:** Individual or collegiate body appointed by the administrative or governing body of the organization, responsible for the internal information system, in particular, for its management and the processing of investigation files, independently and autonomously from the rest of the organizational bodies of the entity or organization.

- **Response:** The information provided to complainants on the actions planned or taken to follow up on their complaint and the reasons for such follow-up.

- **Public disclosure or public disclosure:** The making of information about violations available to the public.

- **Risks:** Effect of uncertainty on objectives.

- **Compliance Risk:** Probability of occurrence and the consequences of non-compliance with an organization's compliance obligations.

- **Criminal risk:** Risk related to the development of conduct that could constitute a crime, according to the regime of criminal liability of legal entities established in the Spanish Criminal Code or, in the case of entities without legal personality, with the regime of accessory consequences established in the same legal text.

- **Penalties:** Consequences foreseen in cases of commission of infractions.

- **Complaint follow-up:** Determination of the status of a process system or activity. That is, any action taken by the recipient of a complaint or any competent

authority in order to assess the accuracy of the allegations made in the complaint and, where appropriate, to resolve the reported violation, including through measures such as internal investigations, inquiries, prosecutions, recovery actions, or the closing of the proceeding.

- **Management system:** A set of interrelated or interacting elements of an organization that establishes policies, objectives and processes to achieve those objectives.

- **Internal reporting system:** Preferred channel for reporting actions or omissions that may constitute breaches of European Union law or infringements of a serious or very serious criminal or administrative nature.

- **Business partner:** Any party, other than members of the organization, with whom the organization has, or expects to establish, any type of business relationship.

- **Third party:** Person or body that is independent of the organization.

Which legal entities can be held criminally liable in Spain?

When defining which collective entities are liable to criminal liability, Article 31 *bis* of the Spanish Criminal Code refers to "legal entities". This term is rather generic and general, so that it should be understood as including any collective entity that has its own legal personality.

Consequently, collective entities such as capital companies, foundations, associations and civil societies may be held criminally liable when the requirements set out in Article 31 *bis* of the Spanish Criminal Code are met.

Therefore, collective entities without legal personality would be left out. For example:

- Groups of companies;
- Communities of property;
- Capital companies in the process of incorporation or;
- Civil societies without legal personality.

However, in this scenario, Article 129 of the Spanish Criminal Code provides for the possibility of applying a set of consequences ancillary to the sentence to these entities without legal personality. Specifically, it stipulates that "*In the case of offences committed within, with the collaboration of, through or by means of companies, organisations, groups or any other type of entities or groups of persons which, because they do not have legal personality, are not covered by Article 31 bis, the judge or court may impose on these companies, organisations, groups, entities or groups one or more*

consequences ancillary to the penalty corresponding to the perpetrator of the offence, with the content provided for in letters c) to g) of section 7 of Article 33. It may also order the definitive prohibition to carry out any activity, even if it is lawful".

Notwithstanding the above, Article 31 *quinquies* of the Spanish Criminal Code *excludes the possibility of criminal liability for public entities*. In particular, it establishes that "*The provisions relating to the criminal liability of legal persons shall not be applicable to the State, territorial and institutional public administrations, regulatory bodies, agencies and public business entities, international organisations under public law, or others exercising public sovereign or administrative powers*".

However, paragraph 2 of the same article provides for an exception. This is that public commercial companies that execute public policies or provide services of general economic interest may be criminally liable. This would be the case, for example, of a municipal trading company created by a city council for the development of certain public services. However, they can only receive the penalties of a fine or judicial intervention, unless these collective entities are instrumentalised in order to avoid possible criminal liability.

For which crimes can a legal person be liable in Spain?

In view of the configuration of **the model of attribution of criminal liability to legal entities** introduced by the Spanish legislator in the reform of the Criminal Code carried out by Organic Law 5/2010, of June 22nd legal entities **cannot be criminally liable for any crime**, but only for those in which this possibility is expressly provided for.

This is what is known as **a model or *numerus clausus* catalog** (as opposed to a *numerus apertus* model, in which legal entities could be liable for any crime defined in the Criminal Code).

The *numerus clausus* catalog of offenses for which legal entities in Spain can be held liable has **been reformed on several occasions since its introduction until reaching its current version**, which **includes more than forty (40) offenses.**

Specifically, **the reforms that have affected the list of offenses** for which legal entities may be liable have been the following:

- Organic Law 3/2011, of January 28th: in matters related to the general electoral system.
- Organic Law 6/2011, of June 30th: in matters of smuggling.
- Organic Law 7/2012, of December 27th: in matters of transparency and the fight against tax and social security fraud.

- Organic Law 1/2015, of March 30th: introducing various offenses that may generate criminal liability for the legal person and the possibility of obtaining an exonerating or mitigating circumstance of criminal liability for the implementation of Compliance Systems, as will be developed in the following ComplianceKeys.

- Organic Law 1/2019, of February 20th: transposing European Union Directives in the financial field (highlighting the introduction of the crime of embezzlement in the *numerus clausus catalog*) and terrorism and other international issues.

- Organic Law 10/2022, of September 6th: in the area of conduct against integrity (crimes of harassment at work, sexual harassment, among others).

Thus, the **current list of offenses** for which, in accordance with Article 31 *bis* of the Criminal Code, legal entities may be criminally liable, would include the following types:

1. Crimes against moral integrity (art. 173.1 CP).
2. Human trafficking (art. 177 *bis* CP).
3. Crime of sexual harassment (art. 184 CP).
4. Prostitution, exploitation, and corruption of minors. (arts. 187 to 190 CP).
5. Discovery and revelation of secrets and computer trespassing. (arts. 197 to 197 *quinquies* CP).
6. Fraud and other frauds. (arts. 248 to 251 *bis* CP).
7. Frustration of execution and punishable insolvency. (arts. 257 to 261 *bis* CP).
8. Computer damages. (arts. 264 to 264 *quater* CP).
9. Crimes against intellectual and industrial property. (arts. 270 to 277 CP).
10. Crimes of discovery and disclosure of trade secrets. (arts. 278 to 280 CP).
11. Withdrawal of commodities and staple products (art. 281 CP).
12. Misleading advertising (art. 282 CP).
13. Securities fraud (art. 282 *bis* CP).
14. Fraudulent automated turnover (art. 283 CP).
15. Price-fixing and market manipulation (art. 284 CP).
16. Insider trading (arts. 285 to 285 *quater* CP).

17. Fraud of communications and interactive services (art. 286 CP).
18. Money laundering (arts. 301 and 302 CP).
19. Illegal financing of political parties (art. 304 *bis* CP).
20. Crimes against the Public Treasury and Social Security (arts. 305 to 310 *bis* CP).
21. Fraud against the general budgets of the European Union (art. 306 CP).
22. Public subsidy and aid fraud (art. 308 CP).
23. Crimes against the rights of foreign citizens (art. 318 *bis* CP).
24. Illegal construction, building or urbanization (art. 319 CP).
25. Environment crimes (arts. 325 to 331 CP).
26. Crimes of risk caused by explosives and other materials (art. 348 CP).
27. Public health: drugs and medical devices (arts. 359 to 362 *sexies* CP)
28. Public health: food fraud (arts. 363 to 366 CP).
29. Public health: drug trafficking (arts. 368 to 369 *bis* CP).
30. Counterfeit means of payment (art. 386 CP).
31. Counterfeiting of credit and debit cards and travellers' cheques (art. 399 *bis* CP).
32. Corruption offences: public and private sector (arts. 286 *bis* and *ter* and 419 to 430 CP).
33. Embezzlement (art. 432 to 435 CP).
34. Hate and discrimination offences (art. 510 and 510 *bis* CP).
35. Terrorism (arts. 572 to 580 *bis* CP).
36. Smuggling (art. 2 Organic Law 12/1995).

Finally, a **brief reflection should be made as to whether a *numerus clausus* model** (extensive and expansive as the current one) is the **most correct option** for the purpose of determining for which offenses legal entities may be liable.

Thus, it is clear that a ***numerus clausus*** model provides **greater certainty** when it comes to **knowing which specific risks a given company must control at any given time**.

However, its **expansive tendencies and its possible incorrect definition** (for example, including conduct that is not typical of normal business contexts, such as the prostitution of minors or organ trafficking, and leaving aside conduct that is clearly typical of business environments, such as crimes against workers' rights) **can distort these purposes**.

In this context, it **would be worth considering the possibility of introducing**, as has been done in other jurisdictions (as could be the case, among others, in the United States and the Netherlands), **a *numerus apertus* model that would be self-regulating according to the criminological needs observed at any given time** (thus, a more flexible model would allow determining which crimes would make sense to generate criminal liability for legal persons in accordance with the attribution requirements established in Article 31 *bis* of the Criminal Code according to the circumstances of each specific case).

When can legal entities be subject to criminal liability in Spain?

As has been introduced in other ComplianceKeys, since the **reform introduced in the Criminal Code by** Organic Law 5/2010, **legal entities** (such as corporations, foundations, associations, etc.) **may be criminally liable for crimes committed within them.**

However, **Article 31 bis of the Criminal Code** establishes a series of specific requirements that must be **cumulatively** fulfilled for legal entities to be criminally liable, these are the following:

1. The first requirement is that **the offense committed is part of the *numerus clausus*** catalog of **offenses that may generate liability for legal entities** (see ComplianceKeys #4).

2. The offense has been committed by (i) a **legal representative or those authorized to make decisions on behalf of the legal person or who have powers of organization and control** (in general, administrators and managers); or (ii) **those acting under the command or orders of these** (in general, employees, agents or other persons related to the legal person).

3. That whoever has committed the offense has done so **in the name or on behalf of the legal person** or **in the exercise of its corporate activities**.

4. That the offense has been committed **for the direct or indirect benefit of the legal entity**. Direct or indirect benefit shall be understood as both **clear gains**, e.g., contracts, increase in turnover or market share or position, as well as other **more incidental benefits**, such as cost savings or penalties.

It should be noted that **the criminal liability of the legal entity in no case excludes the individual criminal liability** of the person or persons who have committed or participated in the crime.

Thus, only when **the above requirements are cumulatively met**, not having an **effective Compliance System**, **criminal liability may be attributed to legal entities**.

What are the consequences for a company if a crime is committed within it?

Having analyzed in other ComplianceKeys **the legal entities that can be criminally liable** in Spain (ComplianceKeys #2), the **crimes that can generate criminal liability** for legal entities in Spain (ComplianceKeys #3) and, finally, the **requirements for the attribution of such liability** to legal entities (ComplianceKeys #4); we will now study the **specific consequences that can be generated for legal entities by the commission of criminal conduct within them.**

First, obviously, the **conviction of a legal person for the commission of a crime is associated with the imposition of penalties**. These penalties necessarily **differ** from those attributable to their flesh-and-blood counterparts, the **natural persons**.

Thus, **Article 33.7 of the Criminal Code** lists the **possible penalties** to be imposed on legal entities:

- **Daily fine** of between **thirty (30) and five thousand (5,000) euros** for a **period of up to five (5) years** or **proportional, i.e**., **between twice and more than six times the profit obtained** or **the damage caused**.
- **Dissolution of the legal entity** (definitive penalty).
- **Suspension of its activities** for up to **five (5) years.**
- **Closure of its premises and establishments** for up to **five (5) years.**
- **Prohibition to carry out in the future certain activities definitively** or up to **fifteen (15) years.**
- **Disqualification to obtain public subsidies and aid**, to **contract with the public sector** and to **enjoy tax or Social Security benefits and incentives** for up to **fifteen (15) years.**
- **Judicial intervention** for up to **five (5) years.**

However, the commission of criminal conducts is also associated with **other negative consequences for the legal entity different from the penalties** established in Article 33.7 of the Criminal Code:

- **The prohibition to contract with the public** sector: in accordance with Article 71.1 of the Public Sector Contracts Law, in the event that the offenses committed are any of the following:
    - Crimes of terrorism, constitution or integration of a criminal organization or group, illicit association;
    - Illegal financing of political parties;
    - Trafficking in human beings;
    - Corruption in business;
    - Influence peddling;
    - Corruption;
    - Fraud;
    - Offenses against the Public Treasury and Social Security;
    - Offenses against workers' rights;
    - Embezzlement;
    - Money laundering;
    - Crimes related to land and urban planning, protection of historical heritage and the environment.
- **Imposition of accessory consequences**: According to certain jurisprudential sectors, the imposition of accessory consequences to the penalty of Article 129 of the Criminal Code, as will be explained in the following ComplianceKeys.
- **Civil liability derived from offenses and other associated costs**: the commission of criminal conduct, in addition to the specific penalties of fines that may be imposed, may give rise to other economic costs such as civil liability derived from the crime (i.e. the compulsory reparation of the damages generated by the criminal conduct), expenses associated with litigation, etc.
- **Reputational and business impact**: the commission of criminal conduct also has negative consequences with respect to the development of the corporate purpose or activity of the legal entity within which it was committed.

  These impacts are not trivial, and may involve **damages with an economic cost whose scope is indeterminable and uncontrollable, long-term economic burdens** and, ultimately, result in the legal entity being **unable or less able to**

produce or market its core business (elimination of demand or elimination of the ability to provide products and services).

To sum up, it has been observed in this ComplianceKeys the **seriousness of the consequences associated with the commission of criminal conduct** and **the need to prevent and mitigate them**, being the **Compliance Systems the tools to do so**.

What are the accessory consequences of Article 129 of the Criminal Code?

In parallel to the penalties that can be imposed on legal entities (ComplianceKeys #5), Article 129 of the Spanish Criminal Code regulates a series of punitive consequences that can be applied to entities without legal personality in the event that an offence is committed in the course of their activities.

As has been introduced, the addressees of these consequences, called accessory consequences to the penalty, are in principle only entities without legal personality (such as, for example, irregular commercial companies, commercial establishments, groups of people who are not constituted in any kind of association, pharmaceutical offices, communities of owners, etc.).

However, exceptions have been noted in recent case law. Thus, there are rulings in which accessory consequences to the penalty of Article 129 of the Spanish Criminal Code are imposed on entities with a legal personality (i.e., among others, Spanish Supreme Court Ruling No. 162/2019 of 26 March).

On the other hand, in the same way as in the area of criminal liability of legal entities (ComplianceKeys #3), not every offence can give rise to the imposition of consequences ancillary to the sentence.

Specifically, the list of offences that can give rise to the application of accessory consequences is made up of: (i) offences that can give rise to criminal liability for legal entities in accordance with Article 31 bis of the Spanish Criminal Code; and (ii) the following specific offences:

- Genetic manipulation offences (arts. 159 to 161 SCC).
- Offence of altering prices in public tenders and auctions (art. 262 SCC).
- Offence of refusal to carry out inspections (art. 294 SCC).
- Offences against workers' rights (arts. 311 to 317 SCC).
- Offence of counterfeiting currency (art. 386 SCC).
- Offence of unlawful association (art. 515 SCC).

- Offences relating to criminal organisations and groups (arts. 570 bis and ter SCC).

• Offences relating to terrorist and terrorist organisations and groups (arts. 571 to 579 SCC).

Of the above offences, offences against workers' rights stand out, as well as offences of altering prices in public tenders and auctions, insofar as they are risks that can affect numerous entities.

With regard to the specific accessory consequences which, in accordance with Articles 129 and 33.7 (letters c) to g)) of the Spanish Criminal Code, could be imposed on unincorporated entities, these are as follows:

- Suspension of activities for up to five (5) years.
- Closure of premises and establishments for up to five (5) years.
- Prohibition to carry out certain activities in the future on a definitive basis or for up to fifteen (15) years.
- Disqualification from obtaining public subsidies and aid, from contracting with the public sector and from enjoying tax or Social Security benefits and incentives for up to fifteen (15) years.
- Judicial intervention for up to five (5) years.
- Definitive prohibition to carry out any activity, even if lawful.

As a small reflection, it can be observed that, although the accessory consequences of Article 129 of the Spanish Criminal Code are not strictly speaking penalties, they coincide almost in their entirety with the penalties imposed on legal entities, and can also cause considerable damage to the entities on which they are imposed.

Can criminal liability be transferred to a company for the purchase of another legal entity that has committed a criminal offence?

As has been analysed in other ComplianceKeys, legal entities may be criminally liable for offences committed in the course of their activities.

However, Article 130.2 of the Spanish Criminal Code establishes an exception to this issue that deserves special development. This is the transfer of criminal liability to a company through the acquisition in the broad sense (takeover, merger, among other

structural modifications) of another legal entity that has previously committed a criminal offence.

It should be noted that this transfer of liability is not automatic. In accordance with the provisions of the Spanish Criminal Code and the relevant court decisions on the matter, the acquiring companies will not be criminally liable for criminal acts committed by the companies they acquire when:

- The acquiring company did not control the acquired company at the time of the commission of the offences. According to this statement:
    - A company could be liable for offences committed by a company B when it had some kind of control over the latter at the time of the commission of the offences (e.g. by imposing strategic decisions, sharing directors or shareholders, etc.).
- The legal personality of the acquired company is not extinguished during the acquisition process. According to this statement:
    - A company could be liable for offences previously committed in company B when the transaction by which it acquired company B extinguished its legal personality (e.g. by a takeover).

However, it should be noted that, even if the legal personality of the acquired company has been extinguished, the transfer of criminal liability can be avoided in court.

In this sense, there are some judicial precedents in which such a transfer has been avoided (for example, Decision 246/2019 of the Audiencia Nacional, of 30 April, in the case of the takeover of Banco Popular by Banco Santander), the discussion on this issue is still alive and kicking.

The possible criminal relevance of Christmas gifts

Christmas is often **synonymous with joy, rest and gifts**. In a business context, **gifts are synonymous with a good relationship with a customer, supplier or other third party**, but they can also **mask other, less innocent intentions**.

Thus, **what at first glance may appear to be a mere gift could lead to serious criminal legal consequences**, both for the **individuals** who give or receive it, and for the **entities** of which they are part of.

In this context, this ComplianceKeys will analyze, on the one hand, the **possible criminal relevance of some Christmas practices from the perspective of corruption offenses**, especially in the private sector; and, on the other hand, it will list some **behaviors that should be avoided in any case**.

First of all, **in order to discern when a Christmas gift** can hide a **corrupt practice**, it is necessary to know **what is considered corruption** by the **Spanish regulations and jurisprudence**.

Article 286 *bis* of the **Spanish Penal Code** defines (in simplified form) the following conducts as **constituting a crime of corruption in business or between private individuals**:

- **Passive corruption**: the receipt, solicitation or acceptance of an undue advantage or benefit (or promise thereof) as consideration for favoring another in a business relationship.

- **Active corruption**: the promise, offering or granting to a third party of an unjustified benefit or advantage as consideration for favoring him or a third party in a business relationship.

However, obviously, **not every gift constitutes a corruption offense**. Since the giving of gifts is a generally accepted and practiced business practice, **only those that are not considered socially appropriate** (not so much from a taste perspective, but from a normative adequacy perspective) **may have criminal relevance**.

In short, **although the line between what is considered socially appropriate and what is not can be very thin** (and sometimes non-existent), it is not always clear whether the gifts are socially appropriate or not, from the study of the jurisprudence on the matter, it is derived that **in order for a gift not to be considered corrupting, it must meet the following requirements**:

- The gift should have a **minimum value** (the value of the gift should be determined based on the industry and the potential recipient).
- Although of minimal value, the gift itself matters, **it may not be unusual**.
- The gift **must not have the ability to influence the specific person who is to receive it** (therefore, the recipient and the timing of the gift matters).

On the other hand, as regards **corruption in the public sector**, regulated in **articles 419 and following of the Criminal Code**, the above requirements must be applied in a **stricter manner than in the private sector**, and each gift to be given must be carefully analyzed.

Also, it should be taken into account that **the above requirements are not only applicable to gifts**, but are **extensible to other attentions** such as **invitations to lunches and dinners**.

In view of the above, **the following practices**, **by way of example**, should be **avoided**:

- Giving or acceptin **high-value gifts** (such as, for example, mobile devices and other electronic items, among others).

- Giving or accepting **luxurious or exotic gifts** (e.g., travel, lavish dinners, invitations to sporting events, etc.).
- The giving or acceptance of gifts at **decisive moments in the relationship with the third party** (for example, in the negotiation phase of a contract, the granting of a license, among others).
- In general, and if it can be avoided, **the giving of gifts to members of the public sector**.

By way of **conclusion**, in view of the widespread practice of **gift-giving at this time of the year**, as well as taking into consideration the **seriousness of the penalties associated with corruption offenses** (which may include fines of up to five times the amount of the benefit obtained), it is convenient to carry out **awareness-raising actions** to prevent what should in principle be a **festive season** from having **very negative consequences for all parties involved.**

Liability of legal persons in the European Union

The regulation of corporate liability for the commission of crimes or administrative offenses within companies differs significantly among the different Member States of the European Union.

Indeed, there is currently no EU directive or regulation unifying the regulation of the liability of legal persons for crimes or administrative offenses committed within their sphere of competence. However, there are several directives that advocate a homogeneous prosecution of certain offenses at the European level. For example, among others:

- Directive 2017/1371 of 5 July 2017 on combating fraud affecting the financial interests of the Union through criminal law;
- Directive 2018/1673 of 23 October 2018 on combating money laundering by means of criminal law;
- Directive 2008/99/EC of 19 November 2008 on the protection of the environment through criminal law; or
- Directive 2011/36 of 5 April 2011 on preventing and combating trafficking in human beings and protecting victims.

Consequently, the absence of a harmonized legal text at the EU level means that Member States have to legislate at the national level on how to configure the liability of legal persons, causing significant differences between countries.

Certainly, this disparity in national regulations affects (i) the very nature of liability (criminal vs. administrative); (ii) the crimes or administrative offenses that can generate corporate liability (closed vs. open list); (iii) the status and procedural regulation of

corporate liability (criminal vs. administrative procedure); (iv) and the possibility of avoiding or reducing corporate liability (legal provision for exemption from liability vs. no legal provision), among other issues.

Below is a table with a summary of the state of affairs in the twenty-seven (27) Member States of the European Union:

Country	Nature of liability	Closed or open list of offenses / infractions.	Legal possibility of exemption for having *Compliance*
Germany	Administrative	Open list	No
Austria	Criminal	Open list	Yes
Belgium	Criminal	Open list	No
Bulgaria	Administrative	Closed list	No
Cyprus	Criminal	Open list	No
Croatia	Criminal	Open list	No
Denmark	Criminal	Open list	No
Slovakia	Criminal	Closed list	No
Slovenia	Criminal	Closed list	No
Spain	Criminal	Closed list	Yes
Estonia	Criminal	Closed list	No
Finland	Criminal	Closed list	Yes
France	Criminal	Open list	No
Greece	Administrative	Closed list	No
Hungary	Criminal	Open list	No

Ireland	Criminal	Closed list	No
Italy	Administrative	Closed list	Yes
Latvia	Administrative	Open list	No
Lithuania	Criminal	Closed list	No
Luxembourg	Criminal	Open list	No
Malta	Criminal	Closed list	No
Netherlands	Criminal	Open list	No
Poland	Administrative	Closed list	No
Portugal	Criminal	Closed list	Partial
Czech Republic	Criminal	Closed list	No
Romania	Criminal	Open list	No
Sweden	Administrative	Open list	No

Liability of legal persons to the other Member States that are part of the Council of Europe

As we advanced last week with ComplianceKeys #9, the regulation of corporate liability for the commission of crimes or administrative offenses in the case of companies differs significantly between different countries.

Along the same lines, in ComplianceKeys #10 we addressed the liability of legal persons in the other Member States of the Council of Europe.

On this basis, attached is a table summarizing the state of play in the nineteen (19) Member States of the Council of Europe that are not part of the European Union:

Country	Nature of the liability	Closed or open list of offenses / infractions	Legal possibility of exemption to dispose of Compliance

Albania	Criminal	Open list	No
Andorra	Administrative	Closed list	Yes (only for certain cases such as in the prevention of money laundering and financing of terrorism)
Armenia	Criminal	Closed list	Yes
Azerbaijan	Criminal	Closed list	No
Bosnia and Herzegovina	Criminal	Open list	Yes
Georgia	Criminal	Closed list	No
Iceland	Criminal	Open list	No
Liechtenstein	Criminal	Closed list	Yes
North Macedonia	Criminal	Closed list	Yes
Montenegro	Criminal	Closed list	Yes
Monaco	Criminal	Open list	No
Norway	Criminal	Open list	Yes
United Kingdom	Criminal	Closed list	Yes (only in certain laws such as the UK Bribery Act or the Criminal Finance Act)
Republic of Moldova	Criminal	Closed list	No
San Marino	Criminal	Open list	No
Serbia	Criminal	Closed list	No

Switzerland	Criminal	Closed list	No
Turkey	Administrative	Closed list	Yes (only in sectorial regulations such as the banking legislation)
Ukraine	Criminal	Closed list	Yes

Liability of legal entities in East Asia and Oceania

In this week's ComplianceKeys #11, we briefly outline the regulation of the liability of legal entities in the different countries that are part of Eastern Asia and Oceania.

As can be seen, the majority of countries in Eastern Asia and Oceania foresee the criminal liability of legal entities and only four countries (Bangladesh, India, the Philippines and Sri Lanka) foresee the administrative liability.

It should be noted that Indonesia has recently (January 2nd) passed the Law 1/2023 which introduces the criminal liability of legal entities, a factor that could encourage the others Southeastern Asia countries mentioned above, to incorporate the criminal liability of legal entities.

In any case, there is attached below a summary-table about the state of play:

Country	Nature of liability	Closed or open list of offenses / infractions	Legal possibility of exemption due to the availability of Compliance
Australia	Criminal	Closed list	Yes
Bangladesh	Administrative	Closed list	No
Cambodia	Criminal	Closed list	Yes (only for certain specific offenses).
China	Criminal	Closed list	Yes (only for very specific conduct, for example, in competition terms).
Hong Kong	Criminal	Closed list	No

India	Criminal	Closed list	No (only, and not very succinctly, for corruption offenses).
Indonesia	Criminal (until 2022 it was Administrative	Open list	Yes
Japan	Criminal	Closed list	Yes
Laos	Criminal	Open list	Yes
Malaysia	Criminal	Closed list	Yes (only for certain specific offenses).
New Zealand	Criminal	Closed list	Yes
Papua New Guinea	Criminal	Closed list	Yes
Philippines	Administrative	Closed list	No
Singapore	Criminal	Closed list	Yes
South Korea	Criminal	Closed list	Yes, in specific laws.
Sri Lanka	Administrative	Closed list	No
Thailand	Criminal	Closed list	No
Taiwan	Criminal	Closed list	Yes
Vietnam	Criminal	Closed list	Yes

Liability of legal entities in West Asia

Continuing with the **analysis of the state of international regulation on criminal liability of legal entities;** in ComplianceKeys #12 we will briefly analyze the regulatory framework around this issue in different countries belonging to the **West Asia region**.

Thereupon, although these regions may offer **interesting business opportunities for organizations** that decide to venture into them, as will be seen below, different legal issues determine the **need for adequate control measures**.

To this effect, **most of the jurisdictions analyzed** (Israel, Lebanon, Pakistan, Qatar, Saudi Arabia, the United Arab Emirates and the United Arab Emirates) provide for the **possibility of attributing criminal liability to legal entities** within which criminal conduct has been committed in accordance with their state regulations.

In several cases, the attribution of liability in these systems is based on a **system of quasi-strict liability**. Thus, the criminal liability of the legal entity **will depend to a large extent on the criminal liability of certain individuals within it**, without requiring other complex additional elements (such as, for example, the analysis of the benefit to the entity, the lack of prevention and control measures, etc.).

Linked to the quasi-strict attribution of criminal liability to legal entities in some of the countries analyzed, there is the issue of the **lack of exonerating or mitigating effect that the correct implementation of Compliance Systems** by legal entities could have in those jurisdictions.

However, although there is no direct benefit linked to the adoption of **Compliance Systems** positivized in the legislation of the countries analyzed, it should be noted that these systems will be of **great relevance in order to prevent and detect in their early stages the criminal conduct** of the members of the organizations that, ultimately, could generate criminal liability for legal entities.

The following **table illustrates** the status of the regulations on the criminal liability of legal entities in the different West Asian countries analyzed:

Country	Nature of liability	Closed or open list of crimes/offenses	Legal possibility of exemption due to the implementation of Compliance Systems
Israel	Criminal	Open list	No (however, the Israeli Attorney General's Office takes into consideration the adoption of appropriate control measures that represent a proper ethical culture in the organization may be taken into account for the purpose of mitigating the penalty to be imposed).
Kazakhstan	Administrative	Closed list (although, very extense)	No

Lebanon	Criminal	Open list	No
Pakistan	Criminal	Open list	No
Qatar	Criminal	Open list	No
Saudi Arabia	Criminal	Closed list	No
United Arab Emirates	Criminal	Closed list	No (only in sector-specific legislation, such as those related to public tenders).

Criminal liability of legal entities in Central and South America

In the last decade, the criminal liability of legal persons has been incorporated into the Criminal Codes of the different Ibero-American countries. Proof of this is that more than half of the countries already have a specific provision in their Criminal Code or in a specific law that establishes the criminal liability of legal persons. However, it is interesting to note that the Republic of Cuba already established the criminal liability of legal persons in 1997.

Along the same lines, it can also be observed that in countries such as Brazil, the system of criminal liability of legal entities has only been established for a specific type of crime (environment), an interesting element that indicates a possible start to the future expansion of the types of crimes that entail criminal liability of the legal entity.

Finally, it is important to highlight the important similarity between the analyzed systems in Central and South America and the continental regimes, with special influence of the Spanish Criminal Code.

A table with a summary of the status of the issue in the different countries is attached below:

Country	Nature of the liability	Closed or open list of crimes/offenses	Legal possibility of exemption due to the availability of Compliance
Argentina	Criminal	Closed list	Yes
Bolivia	Criminal	Closed list	Yes

Brazil	Criminal	Closed list (only crimes against the environment)	No
Chile	Criminal	Closed list	Yes
Colombia	Administrative	Closed list	Yes (Transparency and ethics programs)
Costa Rica	Criminal	Closed list	Yes
Cuba	Criminal	Closed list	No
Dominican Republic	Criminal	Closed list	No
Ecuador	Criminal	Closed list	Yes
El Salvador	Administrative	Closed list	No (only for specific conducts such as, money laundering).
Guatemala	Criminal	Open list	No
Mexico	Criminal	Closed list	No (only some federal entities do take them into consideration)
Nicaragua	Criminal (accessory consequences)	Open list	No
Panama	Criminal	Closed list	Yes
Paraguay	Administrative	Closed list	Yes
Peru	Criminal	Closed list	Yes
Uruguay	Administrative	Closed list	No
Venezuela	Administrative	Closed list	No

Criminal liability of legal persons in Africa

In this week's ComplianceKeys #14, the second to last article on this subject, we will briefly analyse the **regulation of the criminal liability of legal persons and the status of Compliance Systems** as a mechanism for exemption from said criminal liability in **different African countries**.

From the study carried out, it has been observed that the issue of the **criminal liability of legal persons has not, for the time being, had a great deal of progress in the different jurisdictions analysed**. Although most of the countries under study (Kenya, Morocco, Nigeria and South Africa) have allowed the attribution of criminal liability to corporate bodies, these countries d**o not generally have developed a system that would make it possible to foresee what criteria will be taken into account to determine this attribution**.

In this respect, the case of **Kenya** stands out, where, although its **criminal law does not expressly provide for the possibility of attributing criminal liability to legal persons**, this has not proved to be an obstacle to the motivation via case law of the criminal liability of these entities by considering them **equivalent**, for the present purposes, to **natural persons**.

On the other hand, **the exonerating (or mitigating) effect of Compliance Systems in the jurisdictions analysed has not been generally regulated either**. However, this **does not mean that companies operating in these States should not self-regulate**, but rather the opposite. The adoption of effective Compliance Systems will make it possible to prevent the commission of criminal conducts within the legal entities operating in these countries, thus **anticipating the barriers to corporate defence and avoiding the legal uncertainty** caused by the lack of regulation in this area.

Finally, **the South African regulation on the matter stands out positively**, which succinctly establishes that legal persons may be liable for the actions or omissions of their directors or employees when certain circumstances are observed (that the actions or omissions have been observed in the exercise of the functions of the employee at the company, in the interest of the legal person, among others). The **adoption of Compliance Systems** may be taken into account positively, although not automatically.

A **table with a summary** of the status of the issue in the different countries analysed is attached below:

Country	Nature of liability	Closed or open list of offences / infringements	Possibility of legal exemption due to *Compliance*
Egypt	Administrative	Closed list (sanctions regulated in specific administrative regulations)	Not regulated

Kenya	Criminal (not regulated differently from the criminal liability of natural persons)	Open list	Not regulated
Morocco	Criminal	Open list (although specific provisions are established with respect to terrorist offences, corruption of minors and discrimination)	Not regulated
Nigeria	Criminal	Closed list	Not regulated
South Africa	Criminal	Open list	Possibility of exemption or mitigation of criminal liability for the implementation of Compliance Systems, although this is not automatic.

Criminal liability of legal persons in the United States and Canada

We close the ComplianceKeys series on the state of regulation of the criminal liability of legal persons in different countries with an analysis of Canada and the United States.

Before assessing the current state of this issue, it is worth noting that many consider **the United States to be the place of origin of corporate liability** for offences committed within it, mainly as a result of the *New York Central & Hudson River Railroad* v. *United States* case.

Furthermore, it is certainly the **country with the longest track record and practical application** with respect to corporate liability and Compliance Systems, mainly through sanctions and out-of-court settlements with the *U.S. Department of Justice* [DOJ]) or the *U.S. Securities Exchange Commission* [SEC]). This is the case, for example, of the agreements reached with ORACLE and DANSKE BANK in 2022 with the *U.S. Securities Exchange Commission* (SEC).

Canada also regulates corporate liability. In particular, there is a legal provision, namely in the Criminal Code, which provides for criminal liability for legal persons within which an offence has been committed.

Thus, both Canada and the United States have a body of law that supports the application of corporate criminal liability, for example, through the *Foreign Corrupt Practices Act* (FCPA) in the United States, or the Criminal Code and the *Corruption of Foreign Public Officials Act* (CFPOA) in the case of Canada, as well as a firm judicial and punitive application that develops this issue, in which the *Sentencing Guidelines* in the United States or the case of *Canadian Dredge* and Dock Co. vs *The Queen* in Canada are noteworthy.

However, the main difference in the regulation of corporate liability between the two countries is that in the United States the *respondeat* superior principle applies, which implies a broader or more automatic application of corporate criminal liability. In contrast, in Canada, in order to attribute criminal liability to legal persons, all the requirements of the Canadian Criminal Code must be met, which implies a more limited application.

A summary of the state of the issue in the different countries analysed is attached below:

Country	Nature of liability	Closed or open list of offences/infringements	Possibility of legal exemption due to Compliance
Canada	Criminal	Open list	It is provided for in certain laws, such as the anti-money laundering legislation.
United States	Criminal	Open list	Not regulated

The report and the criminal risks map

Any Compliance Program or System is composed of a set of elements that are usually always present regardless of the purpose or scope of the Program or System in question. We are talking about, for example, elements such as having an internal Compliance body or person in charge, an internal communication mechanism, training, etc..

Among these *non-negotiable* elements, we find the report and the criminal risk map. However, the truth is that, depending on the specific purpose and scope of the Compliance Program or System, the report and risk map can be extended beyond criminal risks, also incorporating other Compliance risks (tax; money laundering; environment; among others).

Article 31 *bis* 5.1 of the Criminal Code requires Compliance Programs or Systems to include an **assessment of criminal risks**: "*They shall identify the activities in whose scope the crimes to be prevented may be committed*". Section 4.6 of ISO 37301 on Compliance Management Systems and section 6.2 of UNE 19601 on Criminal

Compliance Management Systems also require the identification and assessment of risks.

What does the preparation of a criminal risk report and map consist of? In short, preparing a criminal risk report and map consists of analyzing the activities, organizational structure and relations with third parties, i.e. the ecosystem of a given organization, with the aim of detecting and prioritizing, through an assessment, the criminal risks to which a given organization is exposed due to its specific activities.

This is very important, since the evaluation and prioritization of criminal risks will mark the subsequent development and implementation of the Compliance Program or System. Consequently, an ethereal analysis or copying the report and the map of a third party is not possible, since each organization faces its own criminal risks. For example, the criminal risks of a construction company have nothing to do with those of a company in the pharmaceutical sector. Even between organizations in the same sector, the report and risk map may differ significantly depending on the dependence on public procurement, the countries of operation, the supply chain, etc.

When should the criminal risk report and map be prepared? Generally, it takes place during the initial phases of the design of the Compliance Program or System, as it allows for an in-depth study of the activities and organizational structure of the organization. In addition, the adoption of policies, procedures and other control mechanisms should be carried out based on the risks detected, especially in those risks assessed with a higher criticality.

However, the criminal risk report and map **must be current at all times**, so it should be **reviewed periodically and properly updated** when there are internal or external reasons that may cause a change in the identification or assessment of criminal risks. For example, the launch of a new line of business, the acquisition of a company, changes in applicable legislation, sanctions or relevant non-compliance, among other reasons.

Thus, the criminal risk report and map is a **key element** in any Compliance Program or System, which should take place at an early stage of its design and should be reviewed and updated appropriately.

Compliance body: single-person or collegiate?

Having analyzed in the previous ComplianceKeys the **state of criminal liability of legal entities at the international level**, the following publications will again take a national approach and analyze some issues related to the **main elements that make up Compliance Systems**.

In this sense, in accordance with article 31 *bis* 2. 2ª of the Criminal Code and all national and international technical standards on Compliance, one of the essential elements for the effectiveness of any Compliance System is the "**Compliance Body**".

Criminal law regulations are **relatively sparse** regarding the **characteristics of this Body**. The aforementioned provision only establishes that the supervision of the functioning and compliance of the Compliance System must be entrusted to a **body of the legal entity with autonomous powers of initiative and control** or that is legally entrusted with the function of supervising the effectiveness of the internal controls of the legal entity.

In this regard, the legal entities that decide to adopt a Compliance System **must reach several decisions** regarding the configuration of the Compliance Body: Should an individual person be appointed or should a collegiate body be appointed? Who should constitute the Compliance Body? What functions should the Compliance Body have?

This ComplianceKeys will seek, briefly, to shed light on one of the issues raised above: **some factors to be taken into account when choosing whether to set up a single-person Compliance Body** (either under the name of Compliance Officer, Head of Compliance, among others**) or a collegiate body** (through a Compliance Committee, Ethics Committee, etc.). In any case, this second option is not an obstacle to the appointment of a Compliance Officer among the members of the collegiate body.

As it has been introduced, the regulation established in this regard in the Criminal Code does not provide an answer to this (and other) question. From going to the **Circular of the State Attorney General's Office 1/2016**, on the criminal liability of legal entities, it can be concluded that the **vagueness of the regulation is intentional**. This vagueness would seek to **provide freedom to legal entities to configure their Compliance Bodies in a way that suits their size, activity and resources**.

Specifically, the aforementioned Circular states the following: "[...] *the regulation refers to a compliance body (compliance officer or head of compliance) which, **depending on the size of the legal entity**, may be made up of one or more persons, with adequate training and authority*".

The decision to configure the Compliance Body as a unipersonal or collegiate body will be of a **strategic nature**, and it should be borne in mind that each option has its **advantages and disadvantages**.

As an illustration, some of the **advantages and disadvantages** commonly associated with each of the options are shown schematically below.

Option	Advantages	Disadvantages
Single-person body	+ Greater agility in decision-making. + In general, greater responsibility and commitment	- Increased possibility of existence (or, as the case may be, relevance) of conflicts of interest.

	as the Compliance function falls on a single person. + In general, less need for resources. + Identification of the Compliance System with an individual who, if correctly chosen, can generate greater confidence in the members of the legal entity.	- Adoption of relevant decisions on Compliance matters in a non-consensual manner, by a single individual. - Possibility that the workload generated by the Compliance function is difficult to assume by a single individual.
Collegiate body	+ Consensual adoption of decisions on Compliance matters. + Easier processing of communications that may eventually affect a member of the Compliance Body. + Possibility of constituting the Compliance Body incorporating complementary technical profiles (legal, IT, labor). + Attractive option for medium-sized entities that do not have the resources to hire a person specifically dedicated to the development of the compliance function but have a Compliance System of a certain complexity.	- Slower decision-making and execution of decisions (difficulty in convening meetings, adopting certain conflictive decisions, reacting to urgent situations, etc.). - Possible configuration of a collegiate body with executive management profiles (conflicts of interest).

In addition, it should be remembered that the Criminal Code provides for the possibility that, in the case of **small legal entities**, the compliance function may fall directly on their **management body**.

In order to **recapitulate** the different issues discussed in this article, the conclusions to be drawn from the above are that **each entity will be free to choose**, depending on its size, the sector in which it operates, the nature of its activities, taking into consideration the advantages and disadvantages associated with the decision, **the configuration of the specific Compliance Body that will lead the development and supervision of its Compliance System**.

The functions and responsibilities of the Compliance Officer

In the last **ComplianceKeys *(*ComplianceKeys #17*)*** a brief introduction was made to one of the basic characteristics of Compliance bodies: their possible **configuration as single-person bodies** (for example, through the figure of the Compliance Officer) or as **collegiate bodies** (for example, as an Ethics and Compliance Committee).

Delving deeper into the characteristics of this relevant figure for any Compliance System or *Compliance* Programme, in this **ComplianceKeys #18** we will offer **a brief outline of the main functions and responsibilities that this body must assume**, bearing in mind that it will be up to each organisation to define its specific functions.

This **basic issue** is somewhat complex to put into practice. This is due to the fact that the **regulatory framework makes little pronouncement on the matter**. In this sense, **article 31 *bis* .2 of the Criminal Code** only establishes that: ***"the supervision of the functioning and compliance of the prevention model implemented has been entrusted to a body of the legal person [...]".***

With regard to this brief reference, it is worth highlighting a fundamental aspect: **the Compliance body is in charge of supervising and promoting the operation and observance** of the Compliance Programme or System, but not of crime prevention or the Compliance System itself.

In this context, **different members** of the organisations must **participate in the Compliance function, that is, in the functioning of the prevention and control mechanisms that make up the Compliance Programmes or Systems** (for example, in the purchasing or payment circuits, by carrying out audits, among others).

Thus, **the Compliance body is not in charge of observance in practice with the Compliance Programme or System**, only of its **supervision and of promoting its proper functioning**. In this sense, **the observance falls to each and every one of the members** that make up an organisation (regardless of their hierarchical position or their functions in the entity).

As is usual in Compliance matters, **self-regulation, technical standards and professional practice have filled the regulatory gap** regarding the question of **what functions and responsibilities** Compliance bodies should assume.

Thus, without being exhaustive, some of the **main functions and responsibilities** that, according to **standards** and **best practices in the field**, Compliance bodies should assume are the following (and which in many cases can be outsourced in whole or in part):

- **Analysing the risks that, in the abstract, may affect an organisation** (through what are generally known as Risk Reports, whether these are criminal -most

frequently- or cover other Compliance matters such as money laundering, tax, etc.).

- **Directing the development and implementation of the Compliance Programme or System** (leading the development of internal regulations taking into consideration the characteristics and risks of the organisation).

- **Managing the Ethics or Whistleblowing Channel and, where appropriate, directing the internal investigations that may have to be carried out** (it should be noted that this issue is likely to vary greatly in each different organisation).

- **Ensuring that the Compliance Programme or System is adapted to the organisation** (analysing legislative changes, responding to changes in the organisation's own activity, etc.).

- **Training, awareness-raising and communication activities in the area of Compliance** (with the aim of ensuring, creating or maintaining the ethical business culture and the effectiveness of certain organisational controls).

- **Among other functions** (such as the execution of certain controls, representation of the legal entity before authorities, representation within the framework of legal proceedings, etc.).

On the other hand, in order to guarantee its **impartiality**, and in relation to the **responsibilities that may arise from the performance of its activities**, it is not usually advisable for the Compliance body to assume decision-making functions (for example, with regard to the sanctioning of a certain member of staff as a result of an internal investigation).

In **conclusion** and recapitulation of the above, it can be established that the **scarce regulatory framework regarding the functions of the Compliance** body makes it necessary to resort to **self-regulation standards** (such as UNE 19601 or ISO 37301 standards), as well as **best practices in the field**. Furthermore, it should be borne in mind that **no two Compliance bodies will perform exactly the same functions**: these must be adapted to the **specific reality** of the organisations of which they form part.

Compliance body, internal or external?

In the last **ComplianceKeys** we have offered a brief analysis of some of the **main characteristics** of a prominent figure of any Compliance System: **the Compliance body**. Thus, previous publications have dealt with issues such as **its configuration as a unipersonal or collegiate body** (ComplianceKeys #17) or its **main functions and responsibilities** (ComplianceKeys #18).

This ComplianceKeys will address another equally essential issue with regard to this body: its **configuration as an internal or external body in relation to the legal entity in question**.

Firstly, it should be pointed out that, as with other characteristics relating to the Compliance body, the **legal-criminal regulation in this area is relatively sparse**. Thus, Article 31 *bis* 2.2 of the Criminal Code only establishes that: "*the supervision of the functioning and compliance of the prevention model implemented has been* ***entrusted to a body of the legal person*** *[...]*".

Thus, the Criminal Code only establishes that the **governing bodies of legal entities** (as they are originally responsible for preventing crime in the entities they manage) must **assign the duty to supervise the operation and compliance of the Compliance System to a body of the legal entity**.

The wording of this precept, by referring to "an organ of the legal entity", might seem to **indicate that the functions and responsibilities** (ComplianceKeys #18) of the Compliance bodies **can only be carried out by internal bodies**. However, the **practical interpretation** of this provision **has not been so restrictive**.

As can be seen in the **Circular of the State Attorney General's Office 1/2016**, although an **internal body of the legal entity must be designated** to exercise a **general oversight function of the Compliance System**, this **does not imply that this body must itself perform all the tasks** that characterise the **Compliance function** of a legal entity.

Moreover, the Circular expressly states that **there is also no objection to legal entities being able to outsource** the different compliance activities.

Thus, as a conclusion, from a **joint reading of Article 31 *bis* 2.2ª of the Criminal Code and its interpretation contained in Circular 1/2016 of the State Attorney General's Office**, it can be argued that, although legal entities must **necessarily have an internal body responsible for the Compliance function** in order to have a **Compliance System that can be considered effective**, this does not imply that **each and every one of the tasks that make up this function must be carried out by this body**.

Moreover, it should be taken into consideration that the **outsourcing of some of the responsibilities** of the Compliance function (such as, among other issues, the analysis of the criminal legal risks associated with the activities carried out by an entity, the development of certain internal regulations, the execution of training, among others) **may be of greater benefit than its internal development**. This is simply because of the **objectivity and specialised knowledge that a third party external to the legal entity in question may have.**

Is the Code of Ethics a key element of the compliance management system?

The Code of Ethics could be defined as the **normative constitution of an organisation, that is, the fundamental regulation from which all others are derived**. It will also be the soul of the organisation, a document that sets out the principles and values that should govern it, and which each and every member of the organisation must comply with.

Functionally, the **Code of Ethics is a very useful tool for business management**, whose objective is to ensure that employees comply with the regulations to which the organisation is subject and that they carry out their activity in accordance with the values it has established and which constitute the essence of the corporate culture.

It is important that the Code of Ethics is alive, that it is not merely a document or a proclamation of good intentions, and that **it is binding for both employees and managers of the organisation**. It is now common practice that third parties, especially collaborators and suppliers, are also bound to comply with the fundamental principles of the Code of Ethics (to a greater or lesser extent and sometimes through a specific Code of Conduct for third parties and/or specific contractual clauses).

In order to proclaim the fundamental principles of the organisation, **it is highly recommended that the corporate Code of Ethics is published on the website and accessible to third parties**.

In terms of content, the **Code of Ethics** must be able to offer guidelines, orientations and be the synergy of all the existing sectoral multi-regulation that applies to the specific organisation. In other words, **it must contain the principles on which the organisation's internal and specific regulations are developed**.

In any case, and despite the fact that it is binding for the members of the organisation, including third parties, and is published on the website, for the Code of Ethics to be truly a code, and, moreover, an ethical one, **it is essential that it is supported by the vertical structure of the organisation, that it reaches all areas of the organisation**. This cannot be achieved without the active participation of the organisation's administrative and management body, through what is called an appropriate tone from the top.

It is these management bodies that must **promote a true culture of compliance**. In order to aim for efficient risk management, it is necessary to influence top management, generating an organisational culture that tends towards absolute compliance with the legal system.

As a result of the above, **it may be recommended to establish a qualitative remuneration system for compliance with the Code of Ethics and, in general, for compliance with Compliance regulations.** This requirement is imposed in most legal

systems (United States, Chile, Italy) and is also noted in national and international Compliance technical standards.

Last but not least, although the Spanish Criminal Code does not mention training among the requirements established for an "organisational and management model" in Article 31 bis 2º, **experience shows the importance of continuous training and awareness as an essential element to guarantee the experience of Compliance** and, as far as this article is concerned, of the Code of Ethics and its principles.

Regular and ongoing training and awareness is one way to ensure the proper functioning of the Code of Ethics and the Compliance structure and rules.

In any case, training and awareness-raising measures are highly efficient tools insofar as they are cost-saving for the organisation, that is, **the more the experience and compliance with the Code of Ethics is ensured, the less costs the organisation will need to develop controls to ensure compliance.**

Training and awareness in Compliance

In the last ComplianceKeys we made a brief comment on one of the most important elements that make up a Compliance System: the Code of Ethics or Code of Conduct (ComplianceKeys #20).

In this **ComplianceKeys #21**, we follow the same line as the previous one, and we will deal with another equally essential issue regarding the configuration of a correct Compliance System: **training and awareness in matters of Compliance**.

Firstly, it is worth mentioning that staff training and awareness-raising on Compliance has already been the subject of controversy in the legal panorama, to such an extent that the Public Prosecutor's Office, in **Circular 1/2016 of 22 January**, on the criminal liability of legal persons in accordance with the reform of the Spanish Criminal Code carried out by Organic Law 1/2015, already emphasised its relevance, stating that "the organisation and management models are not only aimed at avoiding criminal sanctions for the company **but also at promoting a true ethical business culture**". In addition, the **Supreme Court**, in its ruling of 29 February 2016, indicates that a criminal risk training model must be developed that transmits to employees and managers the criminal risk prevention model or program implemented in the company. In order to promote this ethical business culture, it will be necessary to carry out training and awareness-raising actions.

Likewise, the regulatory standards on Compliance, such as **UNE 19601 and ISO 37001**, speak, among many other issues, of the importance of **designing appropriate and effective training** for employees to communicate Compliance risks, focusing on the need to train staff on criminal risk and how to avoid it. Thus, training is understood as an essential element of any organisation's management system, being the channel through which the organisation's staff becomes aware of the culture of compliance.

With the appropriate Compliance training, **irregular situations** that have become "normalised" in the organisation and over the years have become common practices commonly accepted by employees, customers and suppliers, such as certain behaviours that constitute corruption, **can be stopped**. These are often not perceived as negative.

Why is training and awareness-raising important in the organisation?

Designing and implementing a Compliance System is important, especially to mitigate risks, but it will not be efficient if managers and employees are not aware of it and do not understand it as useful and advantageous for the organisation. It is essential that staff **know the basic principles and values** on which their organisation is based, and, above all, the basic guidelines for behaviour and diligence that are applicable in their day-to-day work.

In addition, employees have the right to be informed of all obligations imposed on them in their professional activity by virtue of the employer's duty to ensure compliance with the law and to clarify possible infringements committed.

It is therefore necessary to carry out actions through training, awareness-raising and sensitisation with the aim of achieving an effective change in the operations and in the conscience of the staff.

What should appropriate and effective training look like?

The objective of a training plan or program should be to ensure that all staff are competent to fulfil their professional role and commitment to Compliance.

Thus, good training is that which succeeds in raising awareness and transmitting a culture of compliance, and to this end, it must be configured as follows:

- **Tailored** to the Compliance obligations and risks of the workforce, in relation to their roles and responsibilities, and focusing, where necessary, on knowledge gaps.
- **Practical and understandable** for the different stakeholders and sensitivities of the target audiences.
- **Aligned** with internal policies and the reality of the organisation.
- **Relevant** to the daily work performed.
- **Be up to date** with the internal and external regulations that may be applicable.
- **Attractive and entertaining**.

How can effective training and awareness-raising be achieved?

Ethics and compliance are complex issues, and there is no single method that guarantees success for compliance efforts. However, a combination of training, incentives, culture and monitoring is undoubtedly necessary, so success will lie in determining the right mix for each organisation.

Therefore, the best approach will be to **develop the right training and awareness-raising strategy on the organisation's values and internal policies**. In any case, the training and awareness-raising strategy should always be tailored to the organisation and its specific needs at any given time.

What is the purpose of staff awareness-raising and training?

A correct Compliance System must aim not only to prevent and effectively detect malpractice or conduct in the organisation, but must also contribute to creating a true ethical culture, committed to compliance with the internal and external regulations to which it is subject. It is vital that **all staff internalise the values and principles** of the organisation, thus providing them with the **tools to make good decisions**. All this can be achieved with an appropriate Compliance training plan, tailor-made for each organisation.

In short, the Compliance System has no sense, nor effect, if the staff (from directors and managers to employees) do not know about it, as it is clear that "***what is not known, is not communicated***".

What is the ethical channel?

Ethical channels have acquired great relevance since the recent and novel publication of Law 2/2023, of February 20, *regulating the protection of persons who report regulatory infringements and the fight against corruption* (hereinafter Law 2/2023).

Although Law 2/2023 has encouraged all Spanish companies with more than fifty (50) employees to have a mandatory reporting system, the ethical channel was already an indispensable and key tool for any Compliance System, as it is a requirement of article 31 bis 5.2 of the Spanish Criminal Code for "organization and management models". Likewise, it is also an essential element of any technical standard in Compliance at national and international level. Moreover, there is even the ISO 37002:2021 standard on whistleblowing management systems.

In this sense, the ethical channel could be defined as **the means** by which organizations allow **the channeling of queries or complaints** related to **suspicions of infringing behavior or malpractice** within the same. The channel also makes it possible for the organization to be aware, while respecting **anonymity**, of irregularities, non-compliance, infractions, or violations of current legislation or the organization's internal regulations (such as the Code of Ethics and other policies and protocols) by employees, or even by third parties related to the organization.

One of the main objectives of the ethical channel is to **strengthen the culture of information and integrity** in organizations, as a mechanism to prevent and detect threats to the public and private interest. In this way, it shows commitment to employees and stakeholders, generating trust and demonstrating that the issues and concerns that are communicated will be processed appropriately.

The ethical channel can have different formats, always complying with the requirements established in Law 2/2023 of February 20, for example:

- A **software** created and enabled for such use. This is the most popular option.
- A web form.
- A postal address.
- A telephone line.

In addition to the aforementioned modalities, the aforementioned Law 2/2023, of February 20, provides for different configurations, such as a face-to-face meeting at the request of the communicating party.

Beyond the legal obligation, the implementation of an ethical channel also means a **competitive advantage** before the internal or external public of the organization, since, broadly speaking, and among others:

- ✓ Determines an image of transparency, in that it allows free and confidential communication between the lower and upper echelons of the organization, projecting the organization's ability to adequately deal with conflicts that may arise.

- ✓ Represents a sign of commitment, highlighting the ethical values of the organization and establishing effective mechanisms to avoid possible irregularities.

- ✓ Reduces reputational and economic costs, since early detection of non-compliance considerably reduces its impact.

- ✓ Maintains a solid and balanced growth in the organization.

- ✓ Promotes a work environment based on respect and ethics.

In conclusion, the ethical channel is a **vital element of prevention** in organizations, since no one knows better the irregularities that are committed in them than those who are inside, so that having an instrument to communicate these facts is presented as a great benefit for any organization, which should strive to **promote its use** and carry out an **appropriate management procedure**.

Criminal Compliance, what is it?

The term **Compliance** can be defined as **regulatory compliance**, or **compliance with that which must be complied with**. The scope of the regulatory compliance that a given entity must ensure can be very broad, as well as the totality of rules and regulations applicable to its specific activity.

However, the term **Criminal Compliance** is often used to refer to those compliance structures that entities adopt to **prevent the commission of crimes** within them, under the term "Criminal Compliance Systems". That is, the main objective of Compliance is based on crime prevention.

Criminal Compliance Systems, also called "Crime or Criminal Risk Prevention Programs or Models", have their **origin**, mainly, in the **reform of the Criminal Code** produced by the Organic Law 5/2010, of June 22nd.

This reform of the Criminal Code introduced, for the first time in Spain, the **criminal liability of legal entities**. In short, this means that, in certain cases, when a crime is committed in a given entity, both the individual who commits the crime and the entity to which he/she belongs or represents may be criminally liable.

Since the Criminal Compliance Systems have their origin in this reform of the Criminal Code, in general, they are designed to **comply with the requirements that article 31 bis of the Criminal Code** demands to **avoid the criminal liability of legal entities**. That is:

(i) Adopting and effectively implementing the Criminal Compliance System prior to the commission of the crime;
(ii) Designate a Compliance body;
(iii) Identify activities that may pose a criminal risk;
(iv) Adopt protocols and procedures to avoid such risks;
(v) Manage financial resources appropriately to prevent such risks;
(vi) Establish mechanisms for reporting potential risks and non-compliance;
(vii) Adequately sanction non-compliance with the Criminal Compliance System;
(viii) Review and update the Criminal Compliance System.

In this way, the Criminal Compliance Systems seek to **regulate the social activities of the entity to ensure regulatory compliance** and, by extension, to comply with the requirements of article 31 bis of the Criminal Code in order to **avoid the possible criminal liability** for the legal entity that could result from the commission of certain crimes in its activities (for example, crimes of fraud; misleading advertising; tax fraud; crimes against natural resources and the environment; bribery; etc.).

However, limiting the Compliance System to strictly criminal compliance can lead to a serious **problem of prevention, detection and correction of non-compliance and undesired conduct**. In this sense, a Criminal Compliance System entails significantly delaying the lines of defense of the legal entity, resulting in a much smaller margin for reaction and correction.

On the other hand, **transversal or general Compliance Systems** have a **much broader scope** than strictly Criminal Compliance Systems. The objective of these systems is to manage regulatory compliance in order to prevent **all types of non-compliance** which, of course, also include non-compliance with criminal regulations,

thus allowing better management of the risks of regulatory non-compliance and anticipating, at **an earlier stage**, the materialization of crimes within an entity.

Recent Supreme Court case law on Compliance

After more than (10) **ten years** since the introduction of the **criminal liability of legal entities in the Spanish Criminal Code**, the **Supreme Court** has had the opportunity **to rule** on issues affecting **Compliance** on numerous and diverse occasions.

Thus, this ComplianceKeys #24 will provide a **list of the most relevant rulings of the Supreme Court on Compliance** in the last two (2) years:

Supreme Court jurisprudence on Compliance		
Year	**Decisions**	**Main issues**
2022	STS 36/2022, of January 20	The Supreme Court convicts the legal entity and its administrator for the crime of fraud. The Court understands that there **is no double conviction for the same fact (*bis in idem*) as the administrator is not the partner owner of the capital stock of the legal entity.** Consequently, the conviction does not imply a double penalty.
	STS 56/2022, of January 24	The Supreme Court analyzes the **employer's powers of access to employees' corporate email**. In particular, the High Court dismissed the appeal filed on the grounds that the **search of the corporate email of the employees who had allegedly committed irregularities violated their privacy rights**, insofar as the corporate control measure had been carried out without the necessary guarantees.
	STS 264/2022, of March 18	**It rejects the possibility of holding a sole proprietorship criminally liable due to its fully instrumental nature.** Specifically, the Court understands that, given that the company has only one partner and administrator, the assets of which are confused and diluted with those of the legal entity, the latter cannot be condemned.

		It is alleged that the legal entity lacks sufficient organizational development to differentiate it from the natural person. Consequently, **article 31 *bis* of the Criminal Code cannot be applied given the impossibility of differentiating between the natural person (partner and administrator) and the legal entity and the impossibility of implementing a regulatory compliance program in the latter.**
	STS 747/2022, of July 27th	The Supreme Court **excludes the conviction of the legal entity by virtue of the principle of *non bis in idem*, since it is a sole proprietorship** that corresponds one hundred percent (100%) to the convicted natural person. In particular, the High Court understands that when the individual convicted as a natural person is the sole owner of the company, it is not possible to punish the legal entity as well.
	STS 792/2022, of September 29th	Addresses and maintains, mainly for procedural aspects, the **imposition of the suspension of activities of a company for a period of two (2) years for the commission of a crime against employees' rights** under articles 129.3 and 33.7.c) of the Criminal Code.
	STS 813/2022, of October 14	It advocates the **need to implement compliance programs / Compliance Systems in companies** also to avoid and prevent internal fraud and economic damage to companies.
2023	STS 1014/2022, of January 13, 2023	The Supreme Court, as a note, pronounces in this ruling on the **effectiveness of Compliance Systems** to prevent **criminal conduct of which companies may be victims**. In this sense, Compliance Systems not only mitigate the conducts that may generate a **possible corporate criminal liability**, but also hinder what the High Court calls "**self endangerment**".

		Thus, the Supreme Court considers that, although the **conduct being prosecuted cannot entail the criminal liability of the legal entity** (these are crimes of misappropriation, which are not susceptible to generate the attribution of criminal liability of the legal entity under article 31 *bis* of the Criminal Code), of which **the legal entity itself** (a sports club) **would have been a victim**, these could have been **avoided with control measures aimed at preventing the abuse of personal relationships** (through controls relating to seizures, for example). In this sense, also, Provincial Court of Madrid Decision 90/2023, of February 22, 2023.
	STS 89/2023, of February 10	In the present decision, the Supreme Court resolves in **cassation** the famous "**Pescanova Case**". Among other issues regarding the criminal liability of legal entities, it is worth mentioning the analysis carried out in this ruling regarding the element of "**direct or indirect benefit**", required both in the cases of letter a) (**crimes committed by directors**) and in those of letter b) (**crimes committed by employees**) of article 31 *bis* of the Criminal Code, in order to attribute **criminal liability to legal entities.** The Supreme Court points out that, in fact, what article 31 *bis* of the Criminal Code requires, as an indispensable element for the criminal liability of the legal entity to be established**, is not that the legal entity has obtained as a consequence of the crimes committed in its name or on its behalf a real**, direct or indirect benefit, but that **those criminal acts have been committed "for the benefit" of the legal entity.** Thus, **legal entities** may be **convicted** for criminal conduct that may even have **caused them some kind of damage**, when they were **originally carried out with the purpose of bringing them some kind of benefit**, direct or indirect.

	STS 321/2023, of May 9	The Supreme Court, in the present decision, upholds the appeal of the Public Prosecutor's Office in the sense that the **criminal liability of the legal entity does not exclude the individual criminal liability**, that is, of the material perpetrators of the criminal conduct. In this sense, the Public Prosecutor's Office and the High Court agree that the **system of criminal liability of legal entities complements that of natural persons, but does not replace it**. It is not a question of deciding whether the criminal consequences are to be borne by the natural person or by the legal entity, but whether, **in addition to the natural person, the entity on whose behalf he acted must be criminally sanctioned**. This double sanction will be applicable when the conditions set forth in **article 31 *bis* of the Criminal Code** are met. Finally, it establishes that **only if the legal entity can be identified with the person criminally responsible** (in the case of very small entities, for example) would it be possible to waive one of the convictions (that of the legal entity) so **as not to violate the prohibition of *ne bis in idem*** (punishing the same person twice, for the same facts, on the same grounds).