UNIVERSITAT DE BARCELONA

FACULTAT DE DRET

Criminal compliance system

Implementation of a compliance model in the information technology security sector

Màrquez Postigo, Sandra

NIUB: 20016080

Bachelor's Degree Final Project (TFG) of Law

Mentor: Dr. Javier Cigüela Sola

Academic year 2023-2024

ABSTRACT

The concept of Compliance has gone from being a new trend in business management to consolidating itself as a key resource in those organisations committed to ethical integrity, good governance and long-term sustainability. This work explores, through a literature review, the intricate landscape of criminal compliance in the IT security sector by examining its main legal framework, its fundamental components, the essential steps for the design and implementation of a criminal compliance system (CCS) and the main challenges companies may face. The analysis emphasizes how effective compliance programmes serve as a critical bulwark against criminal activity, mitigating risks, safeguarding reputation and fostering a culture of ethical conduct. Particularly, it addresses the unique challenges and opportunities presented by the rapidly evolving field of cybersecurity, underlining the critical role of robust CCS in mitigating cybercrime risks. It is therefore an arduous process that requires proactivity, effort and sufficient investment of resources, involvement, ongoing commitment and continuous training by all members involved as well as multidisciplinary professionals with sufficient subject-matter expertise and experience to correct mistakes, make improvements and adapt to the changing world of compliance, specially, in cyberspace.

El concepto de *compliance* ha pasado de ser una nueva tendencia en la gestión empresarial a consolidarse como un recurso clave en aquellas organizaciones comprometidas con la integridad ética, el buen gobierno y la sostenibilidad a largo plazo. Este trabajo explora, a través de una revisión bibliográfica, el intrincado panorama del cumplimiento penal en el sector de la seguridad informática, mediante el estudio de su principal marco jurídico, sus componentes fundamentales, los pasos esenciales para el diseño y la implantación de un sistema de cumplimiento penal (SCP) y los principales retos a los que pueden enfrentarse las empresas. El análisis hace hincapié en cómo los programas de cumplimiento eficaces sirven de baluarte fundamental contra la actividad delictiva, mitigando los riesgos, salvaguardando la reputación y fomentando una cultura de conducta ética. En particular, aborda los retos y oportunidades únicos que presenta el campo de la ciberseguridad, de rápida evolución, subrayando el papel fundamental de unos SCP sólidos para mitigar los riesgos de ciberdelincuencia. Se trata, por tanto, de un proceso arduo que requiere proactividad, esfuerzo y suficiente inversión de recursos, implicación, compromiso constante y formación continua por parte de todos los miembros implicados así como profesionales multidisciplinares expertos en la materia y con suficiente experiencia para corregir errores, introducir mejoras y adaptarse al cambiante mundo del cumplimiento, especialmente, en el ciberespacio.

Título: Sistema de *compliance* penal: Implementación de un modelo de *compliance* en el sector de la seguridad informática

Keywords: Criminal compliance system, Compliance management system, Compliance programme, risk management, cybersecurity.

Palabras clave: sistema de cumplimiento penal, sistema de gestión del cumplimiento, programa de cumplimiento/*compliance*, gestión de riesgos, ciberseguridad

Table of contents

I. Introduction

Due to numerous spectacular scandals regarding economic crime (mainly in United States –from now on, U.S.–, but also in Europe[1]) and its pernicious consequences (not only in terms of company reputation but also in terms of social impact; Tiedemann, 1972; Sieber, 2013; PwC[2], 2022), new controls have been developed and implemented, in which the compliance programmes stand out (Sieber, 2013). In this regard, different concepts related to it have been established and spread out worldwide –even to the public sector[3]–, such as (Engelhart, 2018; Sieber, 2013): *compliance programme*, *corporate management*, *codes of ethics/conduct* or *integrity codes* or *business ethics*, *risk management* and *corporate social responsibility*. These ideas are defined to guide business management, adding ethic values, as well as to hinder and prevent economic criminality.

In fact, compliance has traditionally been justified on the basis of the criminological deterrence theory (Beccaria, 1957; Bentham, 1789; Chalfin and Justin, 2017; Johnson, 2019; Roxin, 1997; von Hirsch et al., 1999), according to which punishing a behaviour will not only decrease the violations by the wrongdoer (specific deterrence) but also by others (general deterrence). This view has been developed into the economic model of deterrence (Becker 1968; see also Bentham, 1789; Chalfin and Justin, 2017; Johnson, 2019;), which envisions crime as a gamble undertaken by a rational individual and has framed punishment in terms of costs, explaining compliance in terms of a cost-benefit equilibrium. On the other hand, psychological theories focused on motivation provide another perspective: granting rewards (Deci et al., 1999) or imposing fines (Gneezy and Rustichini, 2000) for a certain behaviour is a form of extrinsic motivation that weakens intrinsic motivation and ultimately undermines compliance.

Regardless of the theoretical model, the importance of effective compliance programmes is well-known and widespread. Notwithstanding, failure persist, which means that organisations repeatedly fail to comply with legal and regulatory requirements and their own internal policies and norms (Root, 2019). That is, in spite of the increased trend of adopting new controls and corporate ethics programmes, the observed unethical behaviour in several companies does not decrease accordingly (Andreoli and Lefkowitz, 2009; Hofeditz et al., 2015; PwC, 2022). In Root's point of view (2019, p. 203), the causes of these compliance failures are many and varied, including "general enforcement deficiencies, difficulties associated with overseeing compliance programmes within complex organizations, and failures to establish a culture of compliance throughout the organizational structure.".

[1] Some examples of this are: WorldCom (U.S., 2002; with –*only*– economic damages amounting to USD 107 billion; PBS, 2002), Enron (U.S., 2001; USD 60 billion; Bondarenko, 2024), Parmalat (Italy, 2003; 15 billion euros; Rimkus, 2016) or FlowTex (Germany, 2000; 2.3 billion euros; von Lampe, 2002).

[2] The PwC (PricewaterhouseCoopers)'s global economic crime and fraud survey 2022, with 1296 respondents in 53 countries, enquires about organisations' attitudes towards fraud and financial and economic crime.

[3] For instance, the Catalan government approved in 2021 its own Code of ethics through the Agreement GOV/164/2021, of 26 October, on the adoption of the Code of Ethics for public service in Catalonia by the Government of the Generalitat and the Administration of the Generalitat and the entities of its public sector (Generalitat de Catalunya, 2023).

The main problem is though the obvious negative aftermath it has: On the one hand, internal effects include not only economic losses, debilitation of its financial activity and loss of new business opportunities, and business/operational disruption, but also the alteration of the organisation's culture, minimising the commitment, the performance and the workers' aspirations, as well as increasing incidents and more non-compliance (Askew et al., 2015; Clark and Leonard, 1998; FCPA guide, 2020; Grant and Visconti 2006; Janat et al., 2021; A. Jimenez, 2019; McDonald and Nijhof, 1999; PwC, 2022; Teichmann et al., 2023). On the other hand, some external and social repercussions are damage to the brand, its reputation and ethical culture, negative impact on customer loyalty, more regulatory action and control, but more significantly and generally, it undermines development, destabilizes governments, erodes societal trust and curbs economic growth (Ariely and Mann, 2013; Askew et al., 2015; FCPA guide, 2020; Grant and Visconti 2006; Hoseah, 2014; Janat et al., 2021; A. Jimenez, 2019; PwC, 2022; Teichmann and Wittmann, 2024).

In light of the above, doubts about the effectiveness of such tools propagate and weaken at the same time the social perception of its effectiveness (about the effectiveness perception, see Màrquez, 2022), which debilitate even further the possibility to ensure the ethical behaviour and hinders even more the compliance programmes' adequate implementation (since its own implementers do not trust nor believe in it). Which justify the need to keep investigating about its methods and procedures as well as to bring new points of view. That is why this study pretends to put some more light into these company controls and processes, exploring several possibilities, in order to detect its weaknesses and difficulties/obstacles to develop more effective compliance programmes.

Particularly, it is going to be focused on the information technology security field, and specially, cybersecurity, since it remains a critical concern for compliance in 2024: a research by CPR (2022)[4] points out a 38% increase in global cyberattacks in 2022 (compared to 2021) or an increase of 125% in 2021 (compared to 2020), which makes cybersecurity a top priority in this regard, and even more so considering that remote and hybrid working are becoming the norm (Chigada and Madzinga, 2021; CPR, 2022; Cremer et al., 2022; Franco et al., 2024; Griffiths, 2024; IBM, 2023; Jain, 2024; Li and Liu, 2021; PwC, 2024; Sobers, 2024; World Economic Forum, 2023)[5].

[4] According to Check Point Research (2022) research, the three most attacked industries in 2022 were Education/Research, Government and Healthcare; and Africa experienced the highest volume of attacks with 1875 weekly attacks per organisation, although North America, Latin America and Europe showed largest increases in cyberattacks in 2022 (compared to 2021). It must be noted, though, that this research was carried out on the basis of data collected from the Check Point Software, which is neither scientifically representative nor comparable to the whole population (it hence can only be considered as an approximation of empirical reality, as well as most of the studies discussed in this section).

[5] Other significant results are the following: data breaches cost businesses an average of USD 4.35 million in 2022 (Griffiths, 2024) or USD 4.45 million in 2023 (IBM, 2023; Sobers, 2024), which is the highest average on record (for example, the ransomware NotPetya in 2017 caused a damage amounted to USD 10 billion; Cremer et al., 2022); the most common cyber threat facing is phishing (Griffiths, 2024); 72.7% of all organisations worldwide fell prey to a ransomware attack in 2023 (Statista, 2024); 74% of cybersecurity breaches are caused by human error (Sobers, 2024); the average time to identify a breach is 207 days (IBM, 2023); the likelihood that a cybercrime entity is detected and prosecuted in the U.S. is estimated at around 0.05%. (World Economic Forum, 2022).

In this way, the present project is divided into two parts: (1) First, it consists of a summary of the state of the art in the field of criminal compliance, with particular attention to the definition of the different fundamental concepts in this topic and its basic international regulation. And (2) second, it addresses, through a review of the scientific literature, the main elements, diagnosis, design, implementation and evaluation of a criminal compliance system in the information technology security sector, as well as its main challenges, so as to avoid and prevent possible problems and failures. With this purpose, several books, articles, reports, surveys, as well as rules and standards have been reviewed from databases such as *Dialnet*, *Web of Science* and *Scopus*, and the academic searcher *Google Scholar*.

II. Compliance: state of the art

1. What is Compliance? definition and theoretical framework

1.1. Conceptualization

Although scandals and economic criminality keep bursting within organisations all over the world, they repeatedly bet their efforts on compliance programmes –whether it is out of fear of sanction, harm, retribution, or ridicule– (Root, 2019). But what is meant by Compliance?

One can encounter many different definitions, which can be summed up as follows (Antich, 2017; del Rocío, 2019; Engelhart, 2018; Root, 2019; Sieber, 2013; Teichmann et al., 2023; Vera, 2017: World Compliance Association, 2024): *Compliance* comprises a set of procedures and good practices that can or must adopt a company in order to identify and clarify operational and legal risks faced by the own enterprise and establish internal mechanisms with the aim to prevent, manage, control and react against them[6].

In short, it refers to a “firm’s effort to ensure that it and its agents adhere to legal and regulatory requirements, industry practice, and the firm’s own internal policies and norms.” (Root, 2019, p. 205; see also Artaza, 2013). In this sense, Silva and Montaner (2014) states that compliance means, to a great extent, self-supervision, or, according to Arocena (2017), regulated self-regulation to prevent criminal unlawful acts that are ultimately monitored *ex post* by the State. Actually, building a solid foundation of Compliance enlarges the company’s probability of avoiding criminal liability for an illegal act (Teichmann et al., 2023).

[6] The ISO 31000 defines *risk* as the effect of uncertainty on an organisation's objectives, measured by its consequences, its probability of occurrence and its level of detection, that is, it shifts emphasis from past preoccupations with the possibility of an event to the possibility of an effect and, in particular, an “effect on objectives”. And for Cassidy et al. (2001), there are five types of risk: (1) strategic, which affects an organisation's ability to achieve its goals; (2) financial, which may turn out into a loss of assets; (3) operational, which influences an ongoing management process; (4) compliance, which refers to the observance of both internal and external regulations; (5) reputational, which has an effect on the image, brand or both.

Yet, it is not only reduced to compliance in itself –comply with norms and regulations– nor specific to the criminal field, but includes all conducts and commitments imposed by the positive law (*hard law*) as well as the strategies, standards and codes of ethics voluntarily assumed by the company (*soft law*) with the intent to promote and satisfy the obligations attributed to the legal entity (Antich, 2017; Engelhart, 2018; Vera, 2017). For instance, it protects the economic values of the company and the interest of the capital market and equity holders and includes additional rules in regard to Labour Law that improves worker's, client's and supplier's conditions as well as ensures the worldwide protection of human rights –impeding, for example, forced labour or discriminatory treatment[7]– (Pereira et al., 2022; Sieber, 2013).

Along the same lines, Engelhart (2018, p. 2) understands compliance as the adherence to regulations, which "can be of a legal or of a non-legal nature, especially in cases of ethical and moral guidelines or social conventions.", and complying with the second ones can play a role in guaranteeing adherence to legal regulations. Thus, a compliance programme is a combination of measures that have both ethical and legal implications (Kotlán et al., 2023; Teichmann et al., 2023).

In this regard, a succinct clarification is needed (Antich, 2017): *Compliance programme* is a delimited concept, concrete and objective, although the word Compliance can also be used to refer to it in an abbreviated form. And, as stated, it can be limited to the criminal field (Pascual, 2016) or include all kinds of risks, such as administrative or occupational hazards (Carrau, 2016; Nieto, 2015; Sáiz, 2015): in this work, even though all the risks will be considered, it will be focused on the criminal compliance programme. While *Compliance* is a word with a broader scope which addresses all the actions and programmes of a legal entity so as to implement an authentic culture of compliance with law, as well as everything related to normative compliance –in the sense of adherence to norms–, or even to compliance function –which is referred to the supervisory and monitoring body– (for instance, the Compliance Officer). On the other hand, *Compliance system* comprises both the whole compliance programme and the compliance function; namely, an all-in-one management system (Antich, 2017).

Furthermore, it is important to stress that the Compliance system adopted may vary based on the definition of the forbidden behaviour or what is understood as socially antinormative (Blackwell, 1992). Moreover, the compliance culture must be integrated in all the aspects of the organisation, including its strategic global objectives (WCA, 2019, 2024).

In fact and due to the huge financial scandals of bad practices and corruption, it is now compulsory that the conceptualization of compliance also result from the union between the principles of good corporate governance (referred to internal corporate leadership measures, focused on aligning and achieving corporate goals), the efficient risk management (in order to pinpoint and analyse risks that might jeopardize corporate goals)

[7] In this regard, some of these initiatives are the following: Organisation for Economic Cooperation and Development (OECD) Guidelines for Multinational Enterprises on Responsible Business Conduct (OECD, 2024), United Nations (UN) Global Compact Strategy 2021-2023 (UN, 2021) or Monitoring Compliance with International Labour Standards (ILO, 2019).

and Compliance; that is, the “GRC” (Governance, Risk, Compliance) (Engelhart, 2018; Hodges and Steinholtz, 2017).

Lastly, a note on Corporate Social Responsibility (CSR) must be added (Afsharipour and Rana 2014; Chaturvedi et al., 2019; Homann, 2022; Pollman, 2021): it is a form of self-regulation –intrinsically motivated– where corporate measures and guidelines are designed to help companies and organisations create positive social impacts (among other, on their environment –environmental, social, and governance (ESG)–, stakeholders, and consumers). And it can be related to compliance, due to the fact that CSR should be considered an important aspect of business compliance to achieve long-term sustainability within the business, since CSR or ESG activity might help to quantify or mitigate compliance, regulatory, litigation, and other business risks (CFA Institute 2017; Pollman, 2021). Yet they can be differentiated: whereas CSR are voluntary measures and thus seen as internally-facing, compliance ensures adherence to external regulations –although it should not only be viewed from a legislative perspective, but also, and even more importantly, from an ethical conscience point of view (Homann, 2022).

1.2. Criminal compliance

The management and organisational models try to comply with the different regulatory blocks to which legal entities are obliged, such as provisions on crime prevention, occupational risks, intellectual and industrial property, personal data protection, information security, competition law or money laundering. This diversity of topics can be dealt with in a segmented way, which can result in repeated, incoherent or omitted policies or procedures due to a lack of or poor communication between departments (Antich, 2017; Vera, 2017).

Compliance –or *Corporate Compliance* models– covers all the company’s management and organisational models, namely (Vera, 2017): IT Compliance, Legal Web Compliance, Criminal Compliance, Finance Compliance, Unfair Competition Compliance, Occupational Risks Compliance, Data Protection Compliance, among others. This work is focused on the Criminal Compliance System (CCS), although other aspects related to other regulatory blocks may be examined on a cross-cutting basis.

Particularly, *criminal compliance* “refers to the set of measures and procedures implemented by a company or organisation to prevent and detect possible crimes or criminal offences that may be committed by its employees or members.” (Elías and Muñoz, 2023; see also Antich, 2017). Continuing with the Engelhart’s definition, “is the part of compliance that deals with the adherence to criminal law” (2018, p. 2). Its main aim is to ensure compliance with criminal laws and regulations through the implementation of internal policies and procedures to prevent, detect and manage any possible risk of committing crimes or criminal offences within the organisation (Engelhart, 2018; Elías and Muñoz, 2023). Apart from complying with criminal laws and regulations and preventing the commission of crimes, Elías and Muñoz (2023) underline as some of the significant purposes of criminal compliance the following: protect the reputation and image of the company, improve business efficiency and effectiveness and protect employees and members of the organisation by setting clear policies and procedures that foster an ethical work environment.

1.3. Precedents

In the Continental law criminal liability has traditionally been solely attributed to natural persons, since it was considered the only subjected with capacity to act. Nevertheless, the Hudson sentence establish in 1909 a model of imputation of the criminal liability of legal entities based on the *doctrine of respond at superior* (specially, in civil matters)[8], according to which criminal liability is attributed to the legal person for those crimes committed by its directors or employees when they act in the exercise of their functions and with the intention of producing a benefit for the organisation (G. Jimenez, 2019; Vera, 2017).

Notwithstanding, it is not until 1977 with the Foreign Corrupt Practices Act (or FCPA) that the concept of compliance appears, with the main aim to restore the trust, prestige and international image of the U.S. after several huge financial and corruption scandals (such as Lockheed). This regulation defended that an effective compliance programme or Compliance is a crucial element to ensure and respect internal controls and that it also fosters an organisational culture that stimulates ethic conduct and commitment to –all kinds of– compliance (del Rocío, 2019; G. Jimenez, 2019; Teichmann et al., 2023).

In addition, the Department for International Trade set up the Trade Compliance Centre, which is a specific compliance advisory centre that issues guidelines and reports and advises companies on how to comply with local and international regulations. Moreover, the Committee of Sponsoring Organisations of the Treadway Commission (COSO) was created, which is dedicated to assisting and providing guidance to companies on internal and accounting control, risk management, business ethics and fraud prevention (COSO, 2023).

Later on, in 1984 the American judicial system was reformed introducing the possibility to allay criminal liability to those organisations that had previously adopted and effectively implemented a Compliance and Ethics Program. Gradually, this idea made an impression on Continental Law and European society became increasingly aware of the need to incorporate these models of criminal liability of the legal entity so as to avoid the detrimental outcome to the general interest (Vera, 2017): the first European regulatory reference is the Directive 2004/39/CE (on markets in financial instruments).

2. Corporate criminal law: corporate criminal liability

In light of the above, it is now necessary to succinctly address what corporate criminal liability means and implies: this concept, which has penetrated and evolved in the legal regimes of countries around the world either to reflect the general public opinion that

[8] Case NY Central & Hudson River Railroad Co. vs. U.S., 212 U.S. 481 (1909), by the U.S. Supreme Court.

companies should be sanctioned when they allow financial crimes to be committed or benefit from them or in response to the international regulations in this area, stipulate that a company can be held criminally liable for the illegal behaviour of its employees (Teichmann et al., 2023). In short and according to Teichmann et al. (2023, p. 2), “compliance protects against corporate criminal liability”; that is why these authors consider that both concepts are mutually supportive and complimentary.

The implications of corporate criminal liability remarkably diverge across jurisdictions[9], but it is a common denominator the fact that having a compliance programme does not automatically entail that a corporation will not be criminally held accounted for, and in this regard, the role and conduct of people in management positions are critical (G. Jimenez, 2019; Teichmann et al., 2023). On the other hand, and despite of the mainly preventative benefit to criminal liability of compliance, it can also result in advantages when the system is implemented once criminal liability proceedings have commenced, which constitutes the repressive function of compliance and is concerned with evaluating past behaviour (Engelhart, 2018; Teichmann et al., 2023)[10]. Finally, Compliance can also play a significant role in the sentencing phase of a criminal prosecution against a company, either with a reduced sentence, even when the compliance programmes failed to prevent the commission of said crime, or even as an exculpatory circumstance (Engelhart, 2018; Teichmann et al., 2023). In this sense, it is fundamental, among others, the determination of whether the measures were or not transparent, fairly applied and published.

Yet, although a “comprehensive and coherent compliance system can contribute to saving a company from any wrongdoing and often mitigating or even excluding its liability for the misconduct of its employees” (Teichmann et al., 2023, p. 3), it can be argued that such programme is not a luxury but a necessity that requires a costly endeavour in order to meet the tall regulatory demands (CMS, 2021).

In any case, though, the company benefits too from the effective implementation of a compliance programme beyond avoiding legal liability: in summary, improves the company's image and reputation, guarantees stability and crime prevention and ensures a better overview of the corporation’s operations; in Teichmann et al.’s words, “protects itself against the likelihood of a bad apple causing rot” (2023, p. 2).

3. Information technology security: clarification of concepts

This section aims to clarify several terminologies used in the field of study, since some of them may be overlapped and often –mistakenly– used interchangeably:

On the one hand, **information technology** (IT) is the creation, processing, storage, security, and sharing of all types of electronic data using networks, computers, storage,

[9] See, for example: for Germany, Dubber and Hörnle (2014); for Spain, Matallín and Fernández (2023); for other European countries, CMS (2021); for United Kingdom, Kotlán et al. (2023); or for U.S., Stessens (1994).

[10] One example of this is the Siemens corruption case in 2006 (Engelhart, 2018).

and other infrastructure, physical devices, and procedures; in short, it is the use of computer systems or devices to access information and address commercial or organisational challenges on a broad scale (Cosker, 2023).

On the other hand, **information security** is the protection of an organisation's digital files and data, paper document, physical media and even human speech against unauthorized access or use, disclosure or alteration of its primary goal (IBM, 2023). It refers to the preservation of confidentiality, integrity and availability of information (this so-called CIA triad will be further discussed when addressing ISO/IEC 27001); in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved (Australian National University, 2023).

Along the same lines but with a narrower scope, **IT security** is concerned with protecting physical IT assets and data centres, as well as the physical security of facilities that store paper files and other media (IBM, 2023).

Therefore, IT includes computers and everything that can be done with them, whereas IT security "is the practice of protecting an organisation's IT assets –computer systems, networks, digital devices, data– from unauthorized access, data breaches, cyberattacks and other malicious activity" (IBM, 2023).

Namely, IT security deals with all aspects of protecting IT assets against cyber threats. That is why it must be alluded to **cybersecurity**, which focuses on the protection of digital data and assets from cyberthreats, which are malicious actions from external and internal threat actors, and accidental threats posed by careless insiders (Cosker, 2023; IBM, 2023). It has the narrowest scope, in the sense that it is not concerned with protection of paper or analogue data (IBM, 2023).

Lastly, an **information security management system** (ISMS), which will be further developed when studying the legal framework (part I.4), is a set of policies and procedures for systematically managing an organisation's sensitive data[11]. It "includes the processes, people, technology, and procedures that are designed to protect against unauthorized access, use, disclosure, disruption, modification, or destruction of information." (Dutton, 2021), and some of its benefits are cost savings, risk reduction and enhanced competitiveness.

4. Legal framework

Compliance and regulatory frameworks are sets of guidelines and best practices that constitute *soft law* and are often determined by legislation or regulatory bodies such as ANSI (American National Standards Institute), ISO (International Standards Organisation), HIPAA (Health Insurance Portability and Accountability Act) and SOX (Sarbanes-Oxley Act). There may also be industry-specific compliance regulations as

[11] A management system can be defined as a "set of interrelated or interacting elements of an organisation to establish policies and objectives as well as processes to achieve those objectives (ISO 3701:2021, 3.4).

well as international guidelines that only apply to organisations operating in a particular country. For instance, the European Union's General Data Protection Regulation (GDPR; Regulation (EU) 2016/679) has punitive effects on the activities of international organisations operating in Europe. Furthermore, business compliance may also include written values, ethics, policies, and rules highlighted in the employee handbook.

Organisations follow these guidelines to meet regulatory requirements (so as to provide reasonable security within the requests of legal liability and due diligence), improve processes and strengthen security (with the intention of gaining value, optimising results and reducing costs), and achieve other business objectives (such as becoming a public company). Another reason for opting for a practical guide is the fact that small and medium-sized enterprises cannot or find it more difficult to access a certifiable system, so it is more appropriate for them to implement and evaluate solutions according to their business (Bleker and Hortensius, 2014).

The current work is going to focus on the ISO standards, which are one of the primary international standards for how businesses handle regulatory compliance, namely, the compliance management systems (CMS). These technical norms and standards, elaborated by ISO (an international non-governmental organisation created in 1947) serve as a way of finding common references both at a technical level and in the management of quality, safety and efficiency of products and services (Matallín and Fernández, 2023; WCA, 2019). At present it has published more than twenty thousand standards that apply to all sectors of industry (for example, ISO 14971 for the risk management of medical devices; Matallín and Fernández, 2023), but it will only be dealt with the most important ones linked to criminal compliance, and in particular the IT security sector, to serve as a reference for the case study (part II):

4.1. ISO 37301 (2021): compliance management systems

ISO 37301, which repeals ISO 19600 (2014), is an international standard for CMS, which "provides guidelines for establishing, developing, implementing, evaluating, maintaining, and improving an effective and responsive compliance management system within organizations." (regardless of their size). It is crucial for organisations looking to ensure adherence to laws, regulations, and ethical standards within their operational context. It helps in mitigating risks, fostering a culture of integrity, and enhancing organizational governance and reputation." (ISO 37301).

Some of the benefits of its compliance are (ISO 37301): (a) promotion of ethical business practices and reduction of the risk of non-compliance; (b) enhancement of trust among stakeholders; (c) improvement of management processes and operational efficiency; and (d) support of corporate governance and responsibility.

Finally, it must be added that ISO 37301 covers a broader scope of compliance issues in comparison to ISO 37001 (2016)[12], which focuses specifically on anti-bribery management systems[13].

4.2. ISO 31000 (2018): risk management

ISO 31000, reviewed and confirmed in 2023, is an international standard that affords principles and guidelines for risk management (regardless of the sector and the risk's nature), which outlines a comprehensive approach to identifying, analysing, evaluating, treating, monitoring and communicating risks across an organisation (EALDE, 2020; ISO 31000; Matallín and Fernández, 2023; Serafín and Bello, 2023). The risk management process set out in the regulation is dynamic, iterative, in continuous feedback and it must be adapted to each organisation following the principle of proportionality (del Rocío, 2019; Lerma, 2012; Sarker, 2018).

According to ISO 31000 (see also EALDE, 2020; Serafín and Bello, 2023), it is important for many reasons: (a) "it fosters a shared understanding of risks, their nature, and ways to manage them across an organization" (comprehensive understanding); (b) "the guidelines help embed risk management into an organization's governance, strategy, planning, reporting processes, policies, values, and culture" (strategic decision-making); (c) its implementation "can lead to efficiency gains, as it helps organizations recognize potential threats and opportunities in time, allocate resources wisely, and enhance stakeholder confidence" (operational excellence); (d) it "equips organizations to anticipate and address risks head-on, turning potential challenges into strategic advantages" (proactive approach, rather than being purely reactive); (e) "a structured approach to risk management signals to stakeholders –from investors to customers– that the organization is robustly prepared to navigate uncertainties, reinforcing trust and credibility" (stakeholder confidence).

Along the same lines, the benefits of its implementation are the following (ISO 31000): (a) "standard risk management principles, framework and process"; (b) "guidance for implementing risk management practices"; (c) "tools for contextualizing risk management to any organization"; (d) "criteria for monitoring, reviewing and continually improving risk management"; and (e) "foundation for integrating risk management throughout an organization".

It is complemented by ISO/IEC 31010 (2019)[14], risk management, which includes risk assessment techniques in a wide range of situations that provides recommendations on

[12] ISO 37001 (anti-bribery management systems), last reviewed and confirmed in 2022, will be replaced by ISO/DIS 37001, which is currently under development (ISO 37001). As minimum criteria applicable to criminal compliance, it refers to the ethical content and in the operational aspect, to the risk identification and the establishment of operational controls (Serafín and Bello, 2023).

[13] ISO 37001:2016 provides a framework for organisations to implement and maintain an anti-bribery management system (ABMS), helps organisations identify and mitigate bribery risks throughout their operations and demonstrates an organisation's commitment to ethical conduct and compliance with anti-bribery laws.

[14] It is published as a double logo standard with ISO and IEC (International Electrotechnical Commission).

how to approach the process of risk identification, analysis and evaluation (Matallín and Fernández, 2023; ISO/IEC 31010).

4.3. ISO 37002 (2021): whistleblowing management systems

This document, which is generic and intended for all organisations, offers "guidelines for establishing, implementing and maintaining an effective whistleblowing management system based on the principles of trust, impartiality and protection in the following four steps: a) receiving reports of wrongdoing; b) assessing reports of wrongdoing; c) addressing reports of wrongdoing; d) concluding whistleblowing cases." (ISO 37002:2021). The whistleblowing management system can be stand-alone or can be used as part of an overall management system

4.4. ISO on the IT security sector

The legal framework in the field of IT security, with particular emphasis on cybersecurity, is specified below:

ISO/IEC 27000:2018 (*Information technology – security techniques*)[15], applicable to all types and sizes of organisation, provides the overview of ISMS, as well as terms and definitions commonly in relation to the ISMS family of standards[16] (ISO/IEC 27000; Serafín and Bello, 2023). It addresses the protection of personal data, disclosure of confidential information, prevention of attacks on business and government systems.

Although it applies to any compliance system, it is not feasible to use it as a minimum criterion (Serafín and Bello, 2023). Lastly, it is comprised of ISO/IEC 27001:2022, its comprehension annex **ISO/IEC 27002:2022**[17] and **ISO/IEC 27701:2019**[18], which provide a common language to address governance, risk and compliance issues related to IT security.

On the other hand, **ISO/IEC 27001:2022** (*Information security, cybersecurity and privacy protection*) is the world's best-known standard for ISMS, which defines the requirements it must meet[19]. This standard[20], which promotes a holistic approach to

[15] It will be replaced by ISO/IEC WD 27000, which is currently under development (ISO/IEC 27000).

[16] It is certified through principles of process control (Serafín and Bello, 2023).

[17] ISO/IEC 27002:2022 (*Information security, cybersecurity and privacy protection*) establish, implement, and improve an ISMS focused on cybersecurity. However, whereas ISO/IEC 27001 outlines the requirements for an ISMS, ISO/IEC 27002 offers detailed best practices and control objectives related to key cybersecurity aspects, including access control, cryptography, human resource security, and incident response.

[18] ISO/IEC 27701:2019 (*Security techniques*), which will be replaced by ISO/IEC DIS 27701, provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS) complementing ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organisation. What's more, it ensures compliance with GDPR and other data privacy requirements.

[19] Conformity with ISO/IEC 27001 means that an organisation or business has put in place a system to manage risks related to the security of its data, and that this system respects all the best practices and principles set out therein (ISO/IEC 27001).

[20] It is also certified, which is one way to demonstrate to stakeholders and customers that the company is committed and able to manage information securely and safely (ISO/IEC 27001).

information security, “provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an” ISMS”, as well as “helps organizations become risk-aware and proactively identify and address weaknesses” (ISO/IEC 27001; see also Koza & Öztürk, 2023). Complying with this standard is “a tool for risk management, cyber-resilience and operational excellence” (ISO/IEC 27001).

Hence, the benefits of conformity with ISO/IEC 27001 are: (a) “resilience to cyber-attacks”; (b) preparation for new threats; (c) “data integrity, confidentiality and availability”; (d) “security across all supports”; (e) “organization-wide protection”; and (f) cost savings.

Lastly, it must be highlighted the three principles of information security –called the CIA triad– according to this standard (ISO/IEC 27001): (1) Confidentiality, which means that only the right people can access the information held by the organisation. (2) Information integrity, which refers to the fact that the data that the organisation uses to pursue its business or keeps safe for others must be reliably stored (not erased nor damaged –accidentally–). (3) Availability of data, which signify that the organisation and its clients can access the information whenever it is necessary so that business purposes and customer expectations are satisfied.

Furthermore, **ISO/IEC 27031:2011** (*Information technology – Security techniques*)[21] and the **ISO/IEC 27035** series (*Information technology – Information security incident management*)[22] help organisations to effectively respond, diffuse and recover from cyber-attacks. Finally, there are also ISO/IEC standards defining encryption and signature mechanisms that can be integrated into products and applications to protect online transactions, credit card usage and stored data.

III. An effective criminal compliance system in the IT security sector

In this section is addressed the criminal compliance system (CCS) in the IT security sector in a more practical manner through a literature review, in which the implementation process is detailed and the main challenges and problems tackled.

[21] This standard, which will be replaced by ISO/IEC FDIS 27031 and applies to any organisation, “describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects […] for improving an organisation's ICT readiness to ensure business continuity” (ISO/IEC 27031).

[22] This series includes ISO/IEC 27035-1:2023 (*Concepts and principles*), ISO/IEC 27035-2:2023 (*Guidelines to plan and prepare for incident response*) and ISO/IEC 27035-3:2020 (*Guidelines for ICT incident response operations*), and together they aim to reduce the impact of security incidents by enhancing detection, response, and recovery capabilities; improve overall information security posture by addressing incidents systematically; and promote continuous improvement by learning from incidents and implementing lessons learned.

1. Essential elements

According to the author and the specific industry, there are several essential elements for any criminal compliance system, or even for any global compliance system of a company or organisation. Some of the most sounded pillars are the following (Antich, 2017; del Rocío, 2019; Elías and Muñoz, 2023; Engelhart, 2018; Enseñat, 2016; Hermoso, 2018; Matallín and Fernández, 2023; Moscariello et al., 2022; Pereira et al., 2022; Vera, 2017; WCA, 2019):

(1) **Leadership commitment** (or "leadership and compliance culture", "governance", "top level commitment")[23]: for many authors, it is the cornerstone of any successful and effective programme, and it is fundamental that the top management build and spread a solid commitment and support towards Compliance that is robust, explicit and obviously visible; which is known as "tone from the top". Hence, a culture that does not accept non-compliance in any form is promoted, as well as gathered up in a written and formal document that is not only internally (among others, in the Code of ethics) but also externally published and frequently reminded. But as many empirical investigations demonstrate (Capdeferro et al., 2023; Màrquez, 2022), this commitment can not remain mere expectations, but needs to be continuously translated into action at all levels: enough resources must be allocated, and the compliance objectives must align with business goals, defining roles, responsibilities, and accountability throughout the organisation. One of the most repeated elements that contribute effectively to the establishment of an ethic culture that ensures compliance is the creation of an ethical leader, who is the person trained in ethics and with the capacity to advise on decision-making and guide in good attitudes and good practices (who can be either the compliance officer or any other person) (Capdeferro et al., 2023; Jannat et al., 2022; Kar, 2014: Màrquez, 2022).

(2) **Compliance function or designation of a compliance officer** (or compliance body)[24]: following the international recommendation[25], the company should designate a criminal compliance officer to centralise all the organisation's compliance activities (including overseeing and coordinating the implementation of the criminal compliance programme as well as being responsible for the continuous training of the company's staff and for reporting to the company's management committee and board of directors)[26]. It thus acts as a counterweight to the company, monitoring and steering the compliance process[27]. According to Enseñat (2016) or WCA (2019), it can be a cross-functional compliance committee coordinating all the compliance functions across the organisation.

[23] Antich (2017); del Rocío (2019); Elías and Muñoz (2023); Enseñat (2016); Hermoso (2018); Moscariello et al. (2022); Pereira et al. (2022); WCA (2019).

[24] Antich (2017); del Rocío (2019); Elías and Muñoz (2023); Enseñat (2016); Hermoso (2018); Moscariello et al. (2022); Vera (2017); WCA (2019).

[25] The European precedent of the compliance function is found in the Directive 2004/39/EC on markets in financial instruments (MiFID I), now repealed by Directive 2014/65/EU (MiFID II).

[26] ISO 37301 defines compliance function as the "person or group of persons with responsibility and authority for the operation of the compliance management system" (3.23).

[27] For WCA (2019), the main aims of this compliance body are: (a) monitoring of compliance with the programme; (b) continuous training of the company's personnel; (c) revisions and modifications of the compliance system in the event of regulatory or business changes; (d) custody of the documentation

(3) **Risk assessment**[28]: it consists of identifying specific potential threats (to information security) –and particularly, risks of non-compliance with criminal laws and regulations that may affect the company and its employees– and evaluating their likelihood and impact based on the company's size, structure, industry or activity, operations, and location. Therefore, prioritization efforts become clear in order to effectively direct resources first toward mitigating significant risks. This risk analysis should be ongoing and regularly updated, which entails the continuous development and implementation of controls to mitigate these identified risks. In this regard, some international standards, such as the already explained ISO 31000 (part I.4.2.), clarify and point out the general principles and guidelines for risk management.

(4) **Policies and procedures** (and standards or values, or "policies and controls)[29]: the company should establish clear, concise, and accessible policies, including operational procedures, circulars and work instructions, as well as controls that can be put in place to manage relevant risks and, at the same time, promote ethical behaviour and comply with criminal laws and regulations. Specifically, clear policies –and standards and values– provide guidance on expected behaviours (defining what is acceptable and what unacceptable), whereas procedures outline steps for routine activities and how to report potential misconduct related to data protection measures within the organisation's cybersecurity landscape. In short, they represent and clarify the rules of the game. Moreover, they should be (apart from efficient) written, in a precise, clear, understandable –even, translated, when necessary–, practical and accessible way for all employees. For Matallín and Fernández (2023), these guidelines are complementary but differentiated from Codes of ethics or conduct, which are the document par excellence of the criminal compliance management system.

(5) **Communication, training and raising awareness** (or just "education" or "training and awareness")[30]: the company should offer both regular training sessions and ongoing communication to foster awareness among all employees and members of the organisation about criminal compliance policies and procedures and the importance of compliance with criminal laws and regulations, since a well-informed workforce is crucial for them to know what and how to do in every moment[31]. Particularly, these programmes should be focused on knowledge about specific regulatory requirements and general best practices in cybersecurity hygiene among employees at every level and, above all, for those who handle the organisation's sensitive data.

regarding Compliance; and (e) any other management aimed at guaranteeing compliance with the programme.

[28] Antich (2017); del Rocío (2019); Elías and Muñoz (2023); Engelhart (2018); Enseñat (2016); Hermoso (2018); Vera (2017); WCA (2019).

[29] Antich (2017); Elías and Muñoz (2023); Engelhart (2018); Enseñat (2016); Hermoso (2018); Matallín and Fernández (2023); Moscariello et al. (2022); Pereira et al. (2022); WCA (2019).

[30] Antich (2017); Elías and Muñoz (2023); Engelhart (2018); Enseñat (2016); Hermoso (2018); Matallín and Fernández (2023); Moscariello et al. (2022); Pereira et al. (2022); Vera (2017); WCA (2019).

[31] For WCA (2019), the ultimate goal of the training process includes: learning, awareness-raising, commitment, culture of compliance and continuous improvement.

(6) **Monitoring and evaluation** (or "monitoring systems", "monitoring and verification" or "supervision and control")[32]: the company should continuously monitor and evaluate the effectiveness of the criminal compliance programme (including policies and procedures) in order to identify and address possible weaknesses –in this case, unusual activity indicative of non-compliance or cyber-attacks (early enough for a proactive response to avoid potential damage escalating into more serious breaches)– and improve the implementation of the programme; mostly, before substantial changes that affect the organisation, such as the start of a new activity, changes in the company or in its structure or activity, and legislative developments that require adaptation. In this sense, is specially recommendable to follow the legal framework (mainly, the ISO standards, such as the ISO 37301), and specially for the IT security sector, the implementation of technical controls in IT systems: for instance, information leakage prevention mechanisms, intrusion detection systems (IDS), logical access control measures. For Enseñat (2016), the responsibility of the supervision lies with the Compliance Officer.

(7) **Reporting and investigation mechanisms, the whistleblowing channel**[33]: many authors put this backbone together with the monitoring and evaluation, although this one can be differentiated from the other and reduced to the internal reporting channels. The company should establish a confidential, anonymous and secure whistleblowing channel for employees and members of the company to report possible violations of criminal compliance policies and procedures or just suspected misconduct. Moreover, the ensuing investigation –if needed– must be thorough and objective.

(8) **Continuous improvement** (or "periodic reviews and audits")[34]: some authors address this pillar together with the monitoring and evaluation, since it is the main aim of the supervision and control process: correct the mistakes or possible new risks detected as well as adapt new controls when needed in order to update the compliance programme. Therefore, the culture of compliance is reaffirmed and encouraged and the commitment to continuous learning and improvement is demonstrated. In fact, the crux of this backbone is, for Engelhart (2018), to move forward on the basis of "lessons learned".

(9) **Response plans** (or "disciplinary system", "disciplinary regime" or "consequences of non-compliance")[35]: this one is focused on detailing how to proceed during different types of incidents (data breaches or failed audits), helping quickly restore normal operations through corrective actions designed around lessons learned, improving overall resilience against future challenges and security standards. It may seem similar to the continuous improvement, but in this case the actions are more focalised in fair and consistent disciplinary response for confirmed violations. Notwithstanding it, there is consensus that

[32] Antich (2017); del Rocío (2019); Elías and Muñoz (2023); Engelhart (2018); Enseñat (2016); Hermoso (2018); Matallín and Fernández (2023); Pereira et al. (2022); Vera (2017); WCA (2019).

[33] Antich (2017); Elías and Muñoz (2023); Engelhart (2018); Enseñat (2016); Hermoso (2018); Matallín and Fernández (2023); Pereira et al. (2022); Vera (2017); WCA (2019).

[34] Antich (2017); Elías and Muñoz (2023); Engelhart (2018); Enseñat (2016); Hermoso (2018); Matallín and Fernández (2023); Vera (2017); WCA (2019).

[35] Antich (2017); del Rocío (2019); Engelhart (2018); Enseñat (2016); Hermoso (2018); Moscariello et al. (2022); WCA (2019).

consequences cannot be limited to sanctions alone: incentives (for compliance) are crucial to encourage and promote the adherence to the Compliance programme. On the other hand, exists evidence that disciplinary measures must meet three premises: severity – better: proportionality–, certainty and celerity of the sanction (deterrence theory: see specially, von Hirsch et al., 1999).

Finally, some authors add as a fundamental element (10) **due diligence** (or third-party management)[36]: for some organisations, it is mandatory, and it is specific for relationships with third parties, such as suppliers, business partners and customers, so as to identify potential risks of non-compliance with criminal laws and regulations. However, Pereira et al. (2022) question its effectiveness, specially for mitigating the risk in third parties' relationships and in the possibility to cause financial and reputational damage to an organisation[37].

Furthermore, the OECD (2018) has published a *Best Practice Principles for Regulatory Enforcement and Inspections guide* offering a checklist of 12 criteria that "can be used to identify strengths and weaknesses, gauge actual performance, and pinpoint areas for improvement" in regard to ensure regulatory compliance, which are: evidence-based enforcement, selectivity, risk focus and proportionality, responsive regulation, long-term vision, co-ordination and consolidation, transparent governance, information integration, clear and fair process, Compliance promotion, professionalism and reality check.

Lastly, is essential to bear in mind that an effective programme –and thus, CCS– is not a static document but a dynamic and ever-improving process that adapts to the organisation's evolving needs and risks.

2. Implementation process

The Compliance process –generally referred to as the implementation process of a compliance programme– includes a series of actions or operations conducing to an end, which, in this case, is ultimately the prevention of crimes. For Root (2019), it consists of four stages (prevention, detection, investigation and remediation) that help to better identify failures –the root cause of compliance–when corporate misconducts are committed, since the evaluation is focused on which phase did the breakdown(s) occur (rather than on how or why did it happen): (1) *Prevention* comprises actions undertaken to prevent compliance failures –reasonable risks– from happening[38]. (2) *Detection*

[36] Elías and Muñoz (2023); Matallín and Fernández (2023); Moscariello et al. (2022); WCA (2019). See also Quinn et al. (2023).

[37] After their empirical study, Pereira et al. (2022, p. 97) conclude that for greater effectiveness is important that the company chooses to adopt criteria and strategies specifically focused on those third parties most exposed to integrity risk: "By limiting the scope of third parties to be monitored, the company has a robust and appropriate capacity to monitor its relationships, as well as greater chances to react quickly and appropriately when third parties are suspected of wrongdoing."

[38] An example of a prevention failure is the Enron scandal in the late 1990s (Root, 2019, p. 221): On the one hand, Arthur Andersen LLP, who was the external actor meant to withhold Enron's certification or approval of certain activities, failed to do so. On the other, the company's "board of directors approved a series of transactions fraught with serious, atypical conflicts of interest".

involves the organisation's policies targeted at identifying misconduct, risks or errors (including potential risks that might harm third parties or itself)[39]. (3) *Investigation* includes the company's policies and practices aimed at determining the existence of and, if relevant, scope of the compliance failure, so as to gather sufficient knowledge to determine the suitable next steps[40]. (4) *Remediation* involves a company's strategies for responding to and recovering from the misconduct detected on the previous stages, including a victim's compensation as well as the development of a robust set of policies and procedures to prevent similar misconducts[41]. Even though the fourth stage cannot occur without a failure in any of the previous phases, the author still considers it essential to invest efforts in an appropriate evaluation to remediate misconduct.

Along the same lines but in a more extended manner, this process is usually explained under the designation of a Compliance system (in which the Compliance programme is its foundation), which includes different elements and phases, following the Deming cycle or PDCA (plan-do-check-act) model (Grijalvo et al., 2002) to ensure continuous improvement. It can also be referred to as "Compliance organisation and management model" or "crime prevention and detection model", and the "Compliance system manual" is often its materialization (as a sign of the company's commitment towards compliance and good business practices).

Hereafter it is going to be detailed the CCS, with special interest in the IT security –and more precisely, cybersecurity– particularities, since it presents specific challenges and requires tailored adjustments.

2.1. Planification

First and foremost, the aim of the CCS and thus its manual must be clearly established and understood: the ultimate objective is to prevent crimes and ensure compliance, as well as to foster an ethical code and good practices in the company. Hence, this document should serve as an internal operating protocol with the measures and actions to be taken at all times in the event of any misconduct, which must be aligned with the values promoted by the firm to maintain coherence. And so as to avoid criminal liability, this manual can also be useful as documentary evidence.

2.1.1. Context of the organisation

Prior to any action, the entity where the CCS is to be implemented must be carefully studied in order to know its organisation, structure and internal functioning. Based on the author, though, one order or another should be followed (for instance, del Rocío, 2019;

[39] General Motors ignition switch scandal in 2014 was a detection problem, due to a lack of identification and understanding of the full scope of the defect (Root, 2019).

[40] Is one example of it the Wells Fargo fake account scandal in 2016, in which bank officials blocked a thorough and proper investigation, exacerbating the inappropriate conduct (Root, 2019).

[41] For instance, Credit Suisse Securities (USA) LLC "failed to address deficiencies in its anti-money laundering compliance program[me]", for which "was fined $16.5 million by the Financial Industry Regulatory Authority (FINRA) in December 2016" (Root, 2019, p. 226).

WCA, 2019) –and there are authors that include it with the risk mapping or even skip this phase (such as Pereira et al., 2022; Vera, 2017), which to my mind is very relevant.

Be that as it may, the introduction of any Compliance system manual or the planification of the company's CCS should address –always in writing, up to date and in a clear and understandable manner– the following:

(a) The **legal framework**, that is, the regulations applied to the activity of the company, which entails a thorough and conscious comprehension of the reality, since non-compliance with commercial, tax or labour law obligations could signify criminal liability (WCA, 2019). All these rules help the firm transversally to design controls which prevent the commission of misconducts and crimes. Depending mainly on the industry, the specific activity and the region of the company, the legal framework differs: for instance, if the firm is active (e.g. in relation to sensitive personal data, such as financial or commercial activity) in the EU (European Union), it must take into account, in addition to the domestic regulations of the country in question and the ISO standards cited above (part II.4), the GDPR and cybersecurity regulations such as the EU Cybersecurity Act (Regulation (EU) 2019/881), the EU Cyber Resilience Act (which is still a proposal), or the NIS 2 Directive (Directive (EU) 2022/2555)[42].

(b) The **background and organigram of the firm and the legal entity**, so as to frame the economic, financial and legal reality of the company to then adequately tackle its needs and reduce its risks (del Rocío, 2019; Hermoso, 2018; Matallín and Fernández, 2023; WCA, 2019): it should be considered the nature, scale and complexity of the business activity of the firm (in this case, related to the IT security sector, and particularly, cybersecurity), its size and structure with the company organisation chart (management structure, number of employees, volume of operations), and the geographical areas in which it operates (international, national, local).

And (c) the **leadership and commitment**, since any Compliance system must carry the unmistakable message that it has the approval and encouragement of the company's governing body and senior management (del Rocío, 2019; Hermoso, 2018): the recording of its approval and details in the minutes of the General Meeting will serve as evidence. As many ISO standards remember (such as ISO 37301) and as already stated, the company's leadership executes an essential role in the successful design and

[42] Other rules that make up the regulatory framework for compliance that should be taken into account depending on the circumstances of the company are: Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law, FCPA (Foreign Corrupt Practices Act, 1977), OECD Anti-Bribery Convention (1997), United Nations Convention against Corruption (2003), Transparency International's Business Principles for Countering Bribery (2003), Transparency International's Business Principles for Countering Bribery (2003), Transparency International's OECD Anti-Bribery Convention (1997), UN Convention against Corruption (2003), Transparency International Business Principles for Countering Bribery (2003), International Chamber of Commerce Anti-Corruption Rules (2005), UK Bribery Act (2010); Sarbanes-Oxley (SOX), PCI DSS (Payment Card Industry Data Security Standard), NIST (National Institute of Standards and Technology), SSAE-16 (Standards for Attestation Engagements No. 16), AT-101 (auditing standard), FedRAMP (U.S. Federal Risk and Authorization Management Program), Privacy Shield (replaced U.S.-EU Safe Harbour) and HIPAA/HITECH (U.S. Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health).

implementation process of the CCS: it is very important that the management bodies demonstrate leadership and commitment to ethics and integrity. To that end, they must foster and defend as fundamental values of the company the culture of compliance; adopt, implement and keep improving continuously an effective and tailored CCS, as well as provide it with all the necessary resources and formal approve the Compliance programme and policy (del Rocío, 2019; ISO 37301, 5.1).

2.1.2. Risk mapping: diagnosis and risk assessment

Furthermore, a system diagnosis or risk mapping is essential (Casanovas, 2013; OECD, 2022), which is a tool based on different information systems that aims at identifying risks, defining their causes, knowing their consequences, assessing the likelihood and the existence of factors that can mitigate the consequences of the risk, or the likelihood of the risk materialising (Vera, 2017; WCA, 2019). Namely, this risk mapping reduces uncertainties –understood as probabilities (Knight, 1921) that may result into potential loss with a significant financial impact– and provides three valuable contributions: integrated information on the overall exposure of the company, a synthesis of the total economic value of the risks taken at any point, and the exploration of those sources of risk (WCA, 2019).

Therefore, it is not a first step that is only carried out –by the Compliance Officer (Enseñat, 2016)[43]– at the beginning of the development of Compliance, but rather this assessment must be constantly reviewed and readjusted and updated to the specific sectors of the activity (Antich, 2017; Carrau, 2016; Enseñat, 2016; Matallín and Fernández, 2023; Nieto, 2015; OECD, 2022; Pereira et al., 2022; WCA, 2019)[44].

For Escudero (2015), the definition of risks becomes fundamental to prioritise and size the actions to be taken so that the CCS (with the Legal Compliance Manual) turns out to be effective from a practical point of view and to ensure that the available resources are invested efficiently. In this sense, ISO standards are of help, for example (further information in part I.4): ISO 31000:2018, completed by ISO/IEC 31010:2019; ISO 37301:2021; and the ones related to IT security: ISO/IEC 27000:2018, ISO/IEC 27001:2022 and its comprehension annex ISO/IEC 27002:2022 and ISO/IEC 27701:2019[45].

According to most of the literature reviewed (Antich, 2017; del Rocío, 2019; Nieto, 2015; Enseñat, 2016; Escudero, 2015; Vera, 2017; WCA, 2019), the risk mapping is a process divisible into three phases. Before that, though, ISO 31000 underlines the relevance of

[43] For Antich (2017) and Nieto (2015), it should be done by someone with enough knowledge of the legal framework and specialised in Criminal Law.

[44] This revision should be performed as a regular updating –at least, once a year (although it should be once every six months or sooner depending on the sector)–, after any legislative or organisational change and in case of any risk event (Antich, 2017; Carrau, 2016).

[45] According to ISO 37301 (2021, 4), the initial stages of the CCS include understanding the organisation and its context, and the needs and expectations of interested parties, determining the scope of the CMS, as well as clearly establishing the CSM, Compliance obligations and compliance risk assessment. Once all this is cleared, it can be proceed to the next step.

specifying the –acceptable– risk criteria, that is, the amount and type of risk that the company can or cannot take, which “should be aligned with the framework and adapted to the purpose and scope of the activity”.

Once this has been done, the first phase is **risk identification**, which consists of the detection, recognition and description of risks –existing and potential–, in order to design the adequate corrective measures (Vera, 2017; WCA, 2019). Those risks are usually linked to criminal risks (such as, in cybersecurity: data breaches, cyber extortion, denial-of-service attacks, insider threats) to prevent crimes (which depends on the Criminal Code in question), but it cannot only be referred to them, since administrative illicit is placed in the pre-criminal offence sphere. Thus, the prevention of the latter may result in the prevention of crimes (Antich, 2017; Nieto, 2015)[46].

In order to carry out this first stage, a diagnosis has to be prepared in which the organisation’s situation and all the company's activities should be analysed to obtain a detailed account of the events or scenarios that, if they were to occur, could give rise to economic, financial or reputational losses as a result of non-compliance (Antich, 2017; Carrau, 2016; del Rocío, 2019; Vera, 2017; WCA, 2019). To this end, it is important to have detailed knowledge –through in-depth interviews, record reviews, brainstorming and questionnaires (WCA, 2019)– of the functioning of the firm and its environment, as well as the regulations and particularities of the specific sector, which is why it is essential to involve the different departments and, in general, the legal entity –and, even, its own customers and suppliers– (Antich, 2017; Carrau, 2016; Escudero, 2015; Hermoso, 2018; Vera, 2017)[47]. Moreover, international standards must be taken into account to be more efficient; for example, ISO 31000:2018 (together with ISO/IEC 31010:2019) outlines the general principles and guidelines of risk management.

The second step is **risk analysis**, which consists of reviewing the risks identified in order to classify them according to the risk level, in order to be able to later assess the priority of its management (del Rocío, 2019; Pereira et al., 2022; Vera, 2017). This analysis –or risk matrix (its graphical visualisation; see table 1)– takes into account two elements (Antich, 2017; del Rocío, 2019; Escudero, 2015; Matallín and Fernández, 2023; Vera, 2017; WCA, 2019): (a) probability (or frequency) and (b) impact (or severity).

[46] For those crimes that there is no administrative offence of reference, such as bribery, Nieto (2015) suggests that the Code of Ethics could be used as a “flanking rule”.

[47] For Carrau (2016), both internal (like administrative and tax obligations, personal data management) and external (including elaboration processes: purchasing, sales, manufacturing, packaging, transport) activities should be taken into account in this diagnosis. On the other hand and due to the differences between organisations, Enseñat (2016) suggests to deliver several questionnaires according to the type of risk (for her, related to the activity; products and services; distribution channels; geographical area; and rules of conduct) that can help the Compliance Officer in this identification. This author proposes a risk classification of three levels in which the risks in the lower level will carry a less detailed description than the ones located above (for example and in regard to cybersecurity, to employ penetration testing methodologies and skills, the Certified Ethical Hacker (CEH) specialised license is required to identify and exploit vulnerabilities in systems; or the Certified Information Systems Security Auditor (CISA) for information security auditing, risk management, and control implementation; or the Certified Information Systems Security Manager (CISM) in relation to security governance, risk management, and program development for information security programs).

Table 1. Example of a risk matrix (5x5)

Impact: *how severe would the outcomes be if the risk occurred?*

Probability: *what is the likelihood the risk will happen?*

	Insignificant	**Minor**	**Significant**	**Major**	**Severe**
Almost certain	Medium	High	Very high	Extreme	Extreme
Likely	Medium	Medium	High	Very high	Extreme
Moderate	Low	Medium	Medium	High	Very high
Unlikely	Very low	Low	Medium	Medium	High
Rare	Very low	Very low	Low	Medium	Medium

(a) By *probability* assessment, it is understood the likelihood of a risk materialising into a certain event before any control or mitigating action (Matallín and Fernández, 2023; WCA, 2019). For Escudero (2015) and Matallín and Fernández (2023), the following factors should be considered: the company's activity (and likely offences), its economic situation, its history (specially, previous requirements and sanctions), its compliance culture (for instance, internal controls, employee training or process documentation) and aspects related with the personnel (such as frequent staff turnover). According to WCA (2019), previous occurrence of the risk, its frequency in organisations in the same sector, the complexity of the risk and the number of people involved in the review and approval process are other factors to take into account. For example, for a company in the IT sector without enough security measures and training of its employees, the occurrence of phishing and ransomware attacks compared to other cybercrimes –as stated above– is pretty high.

(b) By *impact* analysis, it is referred to the severity of the damage to the company's strategic objectives that would be caused if the risk were to materialise in a certain event, considering not only financial factors, legal aspects and the applicable penalties and sanctions, but also the reputational damage –and the effort/difficulty of recovering the levels of trust– and stakeholders directly or indirectly affected (Antich, 2017; Escudero, 2015; Matallín and Fernández, 2023; WCA, 2019). For example, for a company with sensible data (such as a public institution like the police or the European Central Bank) a data breach or almost any cybercrime would more likely result in a severe damage.

Once the risk matrix is finished, the third phase is **risk evaluation** (Antich, 2017; del Rocío, 2019; Escudero, 2015; Matallín and Fernández, 2023; Vera, 2017; WCA, 2019), which focuses on risks management, depending on priorities (according to the results of the risk analysis). In this sense, it is important to remind the principles and guidelines of ISO 31000:2018, and particularly, that in any case, an analysis exercise has to be carried out in relation to the need to implement additional controls, either to avoid risks (for example, by preventing a certain activity), to reduce them (for example, by eliminating the source of the risk, reducing its probability or impact), to share or transfer them (for example, by modifying contracts with third parties or taking out insurance policies) or to accept them (for example, by monitoring their evolution).

To make this decision, it is important to identify and assess the company's controls[48], based on surveys and staff interviews as well as the analysis of the controls in relation of

[48] Enseñat (2016) suggests three types of controls: (a) preventive (policies and procedures; organisational controls; and process controls); (b) reactive –or corrective (WCA, 2019)– (disciplinary measures; and

each risk (Antich, 2017; Enseñat, 2016; Nieto, 2015; Pascual, 2016; WCA, 2019)[49]. Having assessed the design and effectiveness of each control, the *residual risk* must be estimated in each case (Enseñat, 2016), which is the risk assumed by the company after the implementation of controls and preventive measures; therefore, it is calculated with the *inherent risk* and the *effectiveness of the controls for each risk*[50].

Lastly, for Casanovas (2013), a proper risk assessment not only points out the risks, but also the processes and the people or position close to them, which is fundamental for the design of an effective and efficient Compliance programme (or controls).

2.2. Design

Based on the information obtained in the planification stage and with the aim to neutralize the identified risks (to avoid, prevent and detect crimes), tailored measures, controls and action protocols must be designed, taking into account the size of the company, location of its facilities, its sector, among other factors (Antich, 2017; Matallín and Fernández, 2023). It is important to put it all in writing, to benefit from the possibility of mitigation or exemption from criminal liability in case of criminal charges, or to prove certain internal rules to support disciplinary or employment consequences in cases of infringements (Antich, 2017; Matallín and Fernández, 2023; Sáiz, 2015; Vera, 2017; WCA, 2019).

According to Matallín and Fernández (2023; see also ISO 37301:2021; Antich, 2017; Engelhart, 2018; Enseñat, 2016; Pereira et al., 2022; Vera, 2017; WCA, 2019), the main criminal compliance risk controls are: Code of ethics or conduct; procedures, policies and other documents; complaints channel; criminal compliance training and awareness plan; audits; financial controls; non-financial controls; staff due diligence; and other management systems (for instance, following ISO 14000 family and particularly, ISO 14001 in the environmental field). Some of them have already been explained with the essential elements of a CCS (part III.1), so this section will only address the main ones.

Specifically regarding cyber risks, any policy or procedure must adapt those controls to the cyberworld, which entails the following measures: (a) Access controls, which is a security framework that determines who has access to which resources through previous authentication and authorization measures, for instance, by verifying login credentials (usernames, passwords, biometric scans)[51]. (b) Robust data security measures and privacy

incentives); and (c) detective (compliance monitoring; risk indicators; analysis of complaints; and complaints channel).

[49] As already explained, all these steps must be constantly reviewed and redone (at least, once or twice a year), but even more so when a change occurs (such as developing a new activity or operating in another location, or any legal modification).

[50] Like other authors, Antich (2017) discusses whether residual risk is acceptable from a criminal point of view, bearing in mind that the aim of the Compliance programme is precisely the elimination –or at least reduction– of risks: he concludes that, given that zero risk does not exist, residual risks must be documented for consideration and accreditation purposes, and may vary according to the risk accepted by the company –*risk appetite* (Enseñat, 2016; Matallín and Fernández, 2023); which is similar to *risk criteria* (ISO 31000).

[51] The three main types of access controls are (Brown, 2023): DAC (discretionary access control, which provides access rights depending upon the rules set by the owner or administrators –considering a single user account within a company–), RBAC (role-based access control, which gives access based on the

controls to protect sensitive information; for example, through encryption, access controls, data loss prevention, and regular security assessments. (c) Employee training on cyber hygiene and best practices. (d) Incident response plans, which must be comprehensive to effectively respond to cyberattacks and data breaches. (e) Reporting procedures in case of suspicious activity, which must be clear and confidential. (f) Supplier due diligence, which requires paying close attention to third-party vendors and partners who may access sensitive data or systems, and including cybersecurity requirements in contracts.

Furthermore, it is essential to continuously monitor the company's cybersecurity posture and threat landscape and regularly review and update the compliance programme to adapt to evolving threats and regulations, and in general, stay informed about emerging cybersecurity threats and vulnerabilities (all the more so in the cyberworld). To ensure effective and efficient compliance is also fundamental to invest in robust cybersecurity tools and technologies to protect the systems and data (besides promoting ethics).

2.2.1. Code of Ethics

One of the backbones of any Compliance programme (or plan) is the Code of ethics or conduct, since it defines the action line of the company and constitutes the documentary evidence of a Compliance model (Antich, 2017; Hermoso, 2018; Matallín and Fernández, 2023; Sáiz, 2015; Vera, 2017; WCA, 2019): for Hermoso (2018, p. 27), it serves as a sign of the company's "identity and a means of propagating the ethical principles and values that define the standards of behaviour of all members of the company as a social and economic organisation that interacts in the market" (Hermoso, 2018, p. 27). In fact, for Kaptein and Schwartz (2008, p. 113), when this document is developed by and for a given company, it should be called "code of *business*", which is "a distinct and formal document containing a set of prescriptions developed by and for a company to guide present and future behaviors on multiple issues of at least its managers and employees towards one another, the company, external stakeholders and/or society in general".

Regardless of the name, it is believed that it can motivate employees to pursue the recommended ethical behaviour by removing the existing ambiguity of rules and regulations (Jannat et al., 2022; Kaptein, 2015; Wong, 2013). However, empirical research demonstrates that its effectiveness is rather disputed and not unanimous: Màrquez (2022) –and Capdeferro et al. (2023) continuing this study–, after examining the empirical literature, finds out that 10 out 24 investigations obtain that Codes of ethics are effective and perceived as such (at least, short-term effects), specially when it is detailed and specific, without ambiguities. On the contrary, the other 14 investigations together with the one conducted by the author in question conclude that they are rather symbolic, since the ethical expectations declared are not enough to influence workers' attitudes, and that anticorruption tools work better when they are part of an integrity system. In this regard, Kaptein and Schwartz (2008, p. 122) states that "the process of developing and

organisational roles) and ABAC (attribute-based access control, which is a complex model that applies a multitude of attributes to both users and resources, offering more flexibility in the decision).

implementing the code is pivotal", since its effectiveness depend on "many mediating and moderating factors that may vary even within one organization".

Notwithstanding its effectiveness, it has a considerable binding effect, not only *ad intra* (within the organisation, for instance by integrating it into the worker's contract), but sometimes even *ad extra* (with third parties): for instance, Directive 2005/29/EC on unfair commercial practices (art. 6). Thus, codes of ethics must be clear –in an understandable, precise and pleasant language, with examples–, objective and pertinent to the company's reality, as well as publicized enough in order to fulfil its informative purpose and provide it with validity and efficacy (Hermoso 2018; Pereira et al., 2022; Vera, 2017; WCA, 2019).

In relation to its content, for Bacigalupo (2011, p. 106), even though it will vary depending on many factors (such as the size of the legal entity, its activity, location), the minimum content includes: (a) exclusion of conflicts of interest; (b) corruption, fraud, defrauding; (c) competition law; (d) human rights compliance; (e) ethics and protection against discrimination; (f) confidentiality and data protection; (g) correct accounting and invoicing and security of availability, integrity, authenticity and confidentiality of information; (h) compliance with environmental and health protection requirements; (i) regulation of internal complaints (whistleblowing).

Similarly, other authors (Antich, 2017; Sáiz, 2015; Vera, 2017; WCA, 2019) coincide that the main structure should distinguish: (a) *introduction* with the purpose and contextualisation of the Code; (b) *object and scope* to establish to whom it applies; (c) *general principles or values*, such as respect for legality, equality, integrity and responsibility, and the company commitment to employees, customers, suppliers (specially, with reference to the human rights observance); (d) *relational sphere*, both with employees (internal) and customers, shareholders, investors, suppliers, public institutions (external); with special focus on the prevention of corruption; (e) *treatment of information* (policies of confidentiality and use of information); (f) *corporate image and reputation*; (g) *respect for the environment*; (h) *use of corporate assets* (exclusively used for work purposes and during working hours); (i) *conflicts of interest* of employees and their family members (for example, regarding the prohibition on receiving gifts from clients), together with the regulation of unfair competition; (j) *compliance and disciplinary regime*; (k) *whistleblowing*, with the obligation to report possible risks and breaches to the body in charge of overseeing the operation and observance of the prevention model, and the establishment of the corresponding channel; (l) *identification of the Compliance Officer* (or Compliance Committee); (m) *Code update and availability* (with internal communications on any major changes); and (n) *approval and entry into force*. Which can be reduced to three different parts (Hermoso 2018; Nieto, 2006): values of the company (in connection with its addressees), rules of conduct, and responsibilities.

To sum it all up, Codes of ethics are an important tool to ensure compliance in the company and to establish and define its values, but for them to produce the expected effectiveness they must be accompanied by other elements and policies, such as a detailed implementation manual. And another core element is, as already explained, the leadership or ethical leader, who is the person of reference in this regard –most likely the Compliance

Officer– (Capdeferro et al., 2023; Jannat et al., 2022; Kar, 2014: Màrquez, 2022), and together with the managing bodies and figures must align and show commitment (*tone from the top*) and serve as role models (differential association and social learning theories[52]). Therefore, their training in ethics and compliance is essential.

2.2.2. Crime prevention manual

Crime prevention manual or Crime prevention organisation and management protocol is another key document in a CCS, whose main purpose is, on the one hand, to reflect the potentially dangerous and forbidden activities that make up the organisation's risk map (and taking into account the company's singularities), and, on the other hand, to integrate all the documents and internal control and monitoring rules that make up the Compliance model (Sáiz, 2015; Vera, 2017; WCA, 2019).

Its main content includes (Antich, 2017; Sáiz, 2015; Vera, 2017): (a) *general description* (essential characteristics and components; general structure of the company and duties and powers of the Compliance Officer or Committee, as well as the procedure for informing them of possible risks and non-compliance; and reference to the Code of ethics); (b) *criminal risk management process* (description, regulation and scope of the criminal liability of the legal entity; implementation of appropriate internal policies and procedures after having identified and described possible criminal risks; establishment of a disciplinary system; and periodic verification procedure, in the event of relevant breaches or when substantial changes occur in the organisation); and (c) *procedures or protocols of the Compliance model* (definition of the protocols or procedures for decision-making, adoption and execution of decisions in relation to the management of identified risks).

2.2.3. Corporate policies, protocols and other procedures

Dependent on the Crime prevention manual and complementing the Code of ethics, the policies, protocols or guidelines are a set of goals as well as obligations and prohibitions in relation to each of the risks identified in order to mitigate the likelihood of a crime being committed –and thus achieve exemption from criminal liability of the legal entity in case of offences– (Antich, 2017; Anwita, 2024; Hermoso, 2018; Vera, 2017; WCA, 2019). Namely, they help to establish adherence standards and serve as a guiding tool to implement and set a culture of security and accountability. It is important to highlight that they must be documented in writing, adjusted to the company's particularities and be subject to the principle of proportionality, that is, they must be designed in such a way that the company can comply with them (and avoid *compliance fatigue*) (Antich, 2017; Sáiz, 2015; WCA, 2019).

[52] Both criminological theories (differential association from Sutherland, 1983; and social learning from Akers, 1997; Bandura, 1987) stress the importance of communicative interaction with intimate groups and the role they play in the decision to commit a crime –in this case, to act in accordance with the company's ethics. In fact, Hassan et al. (2014) in their empirical research obtained that an ethical leader is likely to increase subordinates' willingness to report an ethical problem, increase organisational commitment (and reduce employee turnover), improve job performance and increase citizenship behaviour, and decrease absenteeism.

Furthermore, any compliance policy or procedure should address roles and responsibilities (with the affected areas), governing requirements, standard operating procedures for implementation (including relevant technology to meet those obligations and control monitoring), monitoring and reporting mechanisms (continuous audits and evaluation of its effectiveness), management reviews and communication of updates (Antich, 2017; Anwita, 2024; Sáiz, 2015).

For instance, is specially important in this case the composition of a cybersecurity analysis procedure in relation to the main cyber risks detected, in order to continuously study and identify vulnerabilities and security mistakes. Other policies and procedures could be in relation to the following topics (del Rocío, 2019; Matallín and Fernández, 2023; Vera, 2017; WCA, 2019): definition of the job positions, welcome pack (confidentiality agreement or non-disclosure agreement, risk prevention training and data protection clause), software audits and licence management, good management practices, management of financial resources (such as the double signature of approval on invoice endorsement), investigation of a complaint, gifts (whether they are possible, of what amount, in which situations), black list (websites whose access is prohibited).

2.3. Establishment

Once defined and planned, it is important to implement the compliance programme (by the people who designed it, namely, the Compliance Officer or Committee). With this aim and beforehand, an action plan should be established, which is a detailed estimation of the timings and concrete steps, roles, responsibilities and tasks, controls, possible obstacles and delays, among other appreciations that should be foreseen, specified and documented in writing (Antich, 2017; Pereira et al., 2022).

This phase –which should be entirely documented– should include the appointment and constitution of the compliance body (if not already in place –which is advisable, as its involvement from the planification stage is essential–; reference to part III.1, element 2), the implementation of the adequate resources, the communication and dissemination of the programme, the training of employees and the monitoring of actions (ISO 37301:2021; Antich, 2017; Pereira et al., 2022; Vera, 2017; WCA, 2019).

2.3.1. Appropriate financial resources

Indeed, for the implementation of the CCS and to accomplish its purpose, enough and adequate resources are fundamental, which, as established by ISO 37301, include not only financial and human resources, but access to external advice, organisational infrastructure and current reference material on compliance management and legal obligations. As reference has already been made to personal resources (mainly, the Compliance Officer), this section focuses on financial resources, which are assets that have some degree of liquidity (cash, loans, deposits in financial institutions) (WCA, 2019).

But as reminded by Antich (2017), it not only refers to the necessary and sufficient provision of resources, but also to the need to plan the management of these resources and record all related operations to prevent the commission of crimes, which is linked to the principle of transparency (so as to provide reliable information to a third party). Moreover, the company's economic and financial information must reflect the economic, financial and asset reality in accordance with accounting principles (Matallín and Fernández, 2023; WCA, 2019). For instance, some measures to reduce cyber risks in this field could be the implementation of controls in IT systems to prevent leakage of confidential information, or the implementation of passwords and access controls to IT systems and documentary archives (Enseñat, 2016).

2.3.2. Communication and dissemination of the programme

An essential aspect to ensure compliance is the effective and evidenced communication to all parties involved (including employees, suppliers, stakeholders and anyone else interested), which is why all the implementation process should be documented since the beginning. And this written communication will not only serve as consciousness-raising but also as evidentiary purpose of due diligence (WCA, 2019).

To this end, employees can be physically provided with a copy of these documents and asked to sign a clause stating this in duplicate (one for themselves and one for the company), or it can be done by e-mail, intranet or other digital media where evidence is kept that they have read and understood the content (Vera, 2017).

2.3.3. Training and raising awareness

As repeatedly mentioned, the success of a compliance programme depends, to a large extent, on the degree of awareness-raising and sensitivity of the members of the company, since only when the organisation is aware of its responsibilities within the framework of criminal liability will it be possible to aspire to a culture of compliance and continuous improvement (Antich, 2017; Casanovas, 2013; Hermoso, 2018; Matallín and Fernández, 2023; Nieto, 2015; Pereira et al., 2022; WCA, 2019)[53]. In fact, for WCA (2019), the ultimate goal is: learning, awareness raising, sensitivity (teaching by thinking), engagement (inspire leaders to commitment), culture of compliance and continuous improvement (since training is a continuous process that advances as the corporate culture of compliance improves).

According to Matallín and Fernández (2023), training plans serve in two ways: on the one hand, staff learn the importance of their contribution to the success of the programme; and, on the other hand, they understand the risks they are exposed to according to their role and the consequences of non-compliance or inobservance. This is particularly relevant in cyberworld, as people are often less aware of the risks they entail and specially

[53] Nevertheless, for Casanovas (2013) training cannot be considered a control in the strict sense, although it is a recommendable measure to avoid non-compliance.

of its aftermath; for example, the possibility of obtaining some of the required certifications in this field could act as an incentive to learn.

Training can be face-to-face or e-learning, but, in any case, must be easy, attractive and in writing[54]; it should take place during working hours and, if possible, at the place of work (Antich, 2017; Hermoso, 2018). It should be entrusted to corporate compliance experts as well as defined for each business organisation and adapted to the job and the risks of each employee (Antich, 2017; Casanovas, 2013; Matallín and Fernández, 2023; Nieto, 2015; WCA, 2019). Regarding its frequency, organisational and regulatory changes, new hires, etc. will have to be taken into account, which in turn will lead to changes in the compliance programme (Antich, 2017; Casanovas, 2013). Finally, this training requires a double evaluation (Antich, 2017; Nieto, 2015): one, by the employees; another, by the programme managers in relation to the degree of knowledge acquired by employees (for example, through a test).

For all that, a (good) training actually constitutes a double burden, since it is not only a cost the company has to bear, but also a one-time loss of performance that will result in a reduction in profits (Antich, 2017).

2.3.4. Investigation and complaints channel: whistleblowing

In order for any compliance model to be considered effective beyond prevention, it must make it possible to detect criminal conduct; hence, both investigative measures and channels for reporting internal breaches and non-compliance are key elements (Antich, 2017; Engelhart, 2018; Hermoso, 2018; Matallín and Fernández, 2023; Pereira et al., 2022; Vera, 2017; WCA, 2019). That is, they involve a double aspect: investigation process, as part of the right of defence; and ethical or whistleblowing channels. “Investigative measures are useful control instruments to prevent, detect, and interrupt improper behaviour[, since] preventive measures remain useless when possible breaches of rules are not investigated.” (Engelhart, 2018, p. 18). Whereas “these channels must be open both to the internal public (the company's employees) and to the external public (customers and suppliers), with the sole purpose of identifying fraudulent actions, erroneous and suspicious procedures, as well as to propose internal solutions in order to avoid future losses, consequent indemnification and/or lawsuits.” (Pereira et al., 2022, p. 34; see also Antich, 2017; Ragués, 2013; WCA, 2019).

However, these control mechanisms must be implemented without undermining “a productive, innovative, and law-abiding corporate environment[, since] a culture of distrust is not only economically counterproductive but also carries the risk of false accusations and fosters secret circumvention strategies” (Engelhart, 2018, p. 18).

Ragués (2013) takes a similar line, expressing his reservations about the effectiveness of these ethical channels and about the obligation of all citizen to report when there is no

[54] Antich (2017) lists all the details that should be recorded: when and for how long the training took place, its content, its attendees, who delivered the training and how (face-to-face or online), if there were questions, if clear examples were given beyond the explanation of the rule, if there was evaluation, etc.

longer any legal asset that can be saved. Similarly and following the criminological social labelling theory (Becker, 2012; Redondo y Garrido, 2013), Silva and Montaner (2014) highlights his worry towards the complainant in regard to the stigmatization and exclusion effects. Gómez (2014, p. 146) warns of the risk of falling "into a kind of corporate Gestapo". Thus and to my mind, these mechanisms can only be established as an additional but non-mandatory channel that –if at all– must be carefully constructed and implemented.

In this way, some of the essential requirements are the following (Antich, 2017; Hermoso, 2018; Matallín and Fernández, 2023; Vera, 2017; WCA, 2019): they must guarantee free access to the channel and the confidentiality and safety of communication and neutralise the risk of reprisals for reporting (to avoid the stigmatisation), and, if possible, the anonymity[55]. Both the channel and the inquiry procedure must also respect guaranties and the fundamental rights of the individuals concerned as well as data protection laws (which, it should be noted, differ according to the country in which the company operates) and, particularly, ISO 37002:2021 (on whistleblowing management systems).

Other issues (such as the content of the complaint, how to ensure respect for all guarantees or the limits of the inquiry) should be addressed to comply with requirements, but for reasons of space and time, this paper will only focus succinctly on the person responsible for managing the inquiry and ethics channel: Big companies have their own legal compliance department with internal complaint channels, whereas small and medium-sized enterprises (SMEs), due to their size, usually have only a Compliance Officer, so that it is common to outsource the management of the ethical channel (Antich, 2017; Hermoso, 2018; WCA, 2019): internal channels are characterised by a greater risk of loss of anonymity and leaks about the matter and the parties involved, as well as by greater immediacy in communication and a lower economic cost in its creation; while external channels are characterised by a greater risk of interception of communications, although they enjoy greater professionalism, independence and objectivity. In my opinion, the best option is to opt for a whistleblowing channel created by the company but managed externally by a multidisciplinary team, in which, on the one hand, the complaints committee would be the external collegiate body responsible for ensuring compliance with the guarantees and managing the complaints channel, supervising the decisions taken by the instructor; and, on the other, the Compliance Officer would be the internal manager of the company responsible for managing the investigation of the reported facts.

In any case, if well-implemented, these control mechanisms serve as a twofold purpose (Sáiz, 2015; Vera, 2017; WCA, 2019): on the one hand, it is a reactive system, since it allows the company to respond to the knowledge of certain irregular or illegal acts already committed; and, on the other hand, it can act as a preventive measure, given that the implementation of this channel can help to inhibit a person from carrying out some irregular behaviour that, without the existence of this channel, he/she might be tempted

[55] For example, for Vera (2017), it is fundamental that the identity of the whistleblower is kept confidential from anyone outside the Compliance Committee or, as the case may be, the Internal Whistleblowing Committee. But guaranteed, it is preferable that the complaint is recorded as evidence for possible criminal or civil proceedings, stating the identity of the complainant, in the context of the criminal defence right, in which anonymous complaints are not usually allowed.

to carry out (in line with the general negative or intimidation prevention theory or deterrence theory: von Hirsch et al., 1999; Roxin, 1997).

2.3.5. Disciplinary and incentive system

To ensure observance of the CCS and legal certainty, certain coercive measures (such as oral reprimands or formal written warnings) should be foreseen and effectively implemented, which in turn serve to verify that the programme is actually carried out (Antich, 2017; Engelhart, 2018; Matallín and Fernández, 2023). In fact, the employer's disciplinary authority derives from its powers of control and supervision, which, in the context of the Compliance programme, are integrated into the duty to prevent offences (Hermoso, 2018; WCA, 2019).

Hence, the company is empowered to apply sanctions and corrective measures for non-compliance by persons subject to the CCS in this area. Notwithstanding it, and as Goñi (2014) reminds, this punitive system is part of Soft law, since these measures lack the implicit enforceability of a legal rule, although they do in fact deploy a *vis compulsiva*[56] capable of achieving the effectiveness of a legal rule.

In accordance with the principles of legality and typicality of the Punitive law, the above presupposes the existence of a Code of conduct which clearly sets out the obligations of management, employees, self-employed and subcontractors, and clearly delimits actions constituting offences –and, in the most serious cases and in accordance with the respective criminal code, criminal offences– as well as its corresponding sanctions and the procedures for enforcing them (del Rocío, 2019; Hermoso, 2018; Matallín and Fernández, 2023; Nieto, 2015). Indeed, both the sanctions in relation to their infringements and the sanctions in relation to each other must be proportionate (Antich, 2017; del Rocío, 2019; Enseñat, 2016; Hermoso, 2018; WCA, 2019), as well as applied with due certainty and celerity (deterrence theory: von Hirsch et al., 1999), which Enseñat (2016) calls in due time and manner. At the same time, all provisions must comply with all applicable regulations and laws of other legal systems, such as labour law (Antich, 2017; WCA, 2019).

To my mind, the purpose of the disciplinary system is not –or should not be– retributive, since this would only create a climate of mutual suspicion that would be detrimental to performance and ethical climate and would have no impact on ensuring future compliance with the CCS (as repeatedly proven by criminal penalties, such as prison or life imprisonment); but to act as a deterrence effect (deterrence theory), showing what is not admissible. That is, the reprimand of an infraction should only serve, on the one hand, to detect the failures and lacunas of the CCS in order to improve it (for it is a process that requires constant evaluations); and, on the other hand, to make sure that all employees understand that the infraction committed is not accepted and must not be repeated. With this aim, in my opinion, is essential to accompany this process with a new training in which the specific infraction is detailly addressed. In this regard, is very suitable Nieto's

[56] It is a Latin expression referred to moral force or violence resulting from intimidation and used to make the person concerned do something against his or her will.

(2015) proposal to focus on re-education: he suggests a kind of suspension of the sanction or probation, in order to make it clear to the offender what is expected of him/her and how and within what period of time he/she should improve his/her behaviour. He also argues in favour of the use of mediation before resorting to disciplinary proceedings.

Furthermore and from my point of view, more effective than the disciplinary system is the provision and application of incentives whenever someone carries out a "particularly ethical" action that can be publicly praised or privately congratulated (for example, with a bonus), to promote not only compliance, but mostly the willingness and commitment of all members of the company to comply (namely, awareness-raising and sensitisation).

2.4. Supervision and monitoring, and revision and improvement

Following the Deming cycle or PDCA model and ISO 37301:2021, is key to continuously evaluate and check the effectiveness of the controls implemented, to introduce the required improvements (Antich, 2017; del Rocío, 2019; Grijalvo et al., 2002; Matallín and Fernández, 2023; Vera, 2017; WCA, 2019), starting the whole process all over again. Self-assessment (by the Compliance Officer or Committee) means the organisation itself must assess its own capacity for the effective implementation of the Compliance system, as well as the quality of the work carried out through the compliance programme (WCA, 2019).

Even though, and to my mind, they are so directly related that they can be addressed in the same section, some authors divide this stage into two or even three steps (Pereira et al., 2022; WCA, 2019): (1) *check* (for ISO 37301:2021, *performance evaluation*), which, at the same time, can be divided into (1a) monitor the operation of each of the compliance programme's actions to ensure its effectiveness and efficiency, and (1b) evaluate, revise and conduct audits to compare results; and (2) *act* (for ISO 37301:2021, *improvement*), that is, continually introduce improvements based on the lessons learned and experiences gained, and restart the cycle again. Similarly, Enseñat (2016) divides it into (a) the *monitoring plan*, understood as a structured document defining and documenting the monitoring tasks to be performed by the Compliance Officer, focused on risks[57]; and (b) the *Compliance revisions*, which are the main tool of the Compliance Officer in exercising his or her supervisory functions[58].

Regarding surveillance, for Hermoso (2018) it materialises in two ways: on the one hand, through a continuous communication plan, to periodically inform employees and persons bound by the Compliance Manual with the aim of maintaining a culture of compliance; on the other hand, through a continuous compliance plan consisting of follow-up actions in order to adopt supervisory measures to detect irregularities[59], such as forensic readiness

[57] In it needs to be developed: factors to consider in risk analysis, the areas to be monitored, the structure of the monitoring plan, the process for approval of the monitoring plan, periodic reviews of the monitoring plan and modifications to the monitoring plan.

[58] According to the author, the process is divided into: planning, fieldwork, conclusions, reporting, follow-up, and closure and archiving.

[59] Goñi (2014) stresses the importance for the Compliance Officer to manage the investigation activity in accordance to the nature, scope and purpose of the control measure, avoiding unrestricted and unlimited access by the employer to employees' personal data.

plan in regard of IT resources[60]. In this sense, one of the most frequent controls (for example, ISO 37301:2021) is audits, both internal and external. According to Matallín and Fernández (2023), an audit is a process of the CCS that verifies whether the system is well implemented and whether it is effective, as well as identifies opportunities for improvement of the system.

Be that as it may, the CCS must be periodically reviewed, for instance, annually or when a new opportunity is detected –proactive evaluation–; but, in any case, when certain circumstances arise, such as the existence of relevant compliance breaches (detected through supervisory measures), legislative developments requiring adaptation or when there are changes in the organisation, control structure or business activity –reactive evaluation– (Antich, 2017; del Rocío, 2019; Hermoso, 2018; Matallín and Fernández, 2023; Vera, 2017; WCA, 2019). This is particularly relevant in the field of cybersecurity, as changes are even more frequent, since software upgrades or new licensing or other cybersecurity requirements entail changes to the entire CCS design (specially risk identification and assessment, which affects the entire programme and requires more training and new measures and controls).

There are numerous review techniques, such as interviews, surveys, statistical information, review of complaints or key risks indicators, monitoring software, among others. These results, continuing with the need for written records, will be collected in a final verification report, which includes the objectives and type of the review (and, if applicable, the cause of non-compliance), the evaluation actions carried out, and, if applicable, the corrective or improvement actions taken to address non-compliances and the review of its effectiveness (Aguilera, 2022; del Rocío, 2019; Enseñat, 2016; WCA, 2019).

3. Challenges of the Compliance process

Compliance management, and specially in cybersecurity, is an arduous process that requires strategic planning and robust systems. The following describes some of the main challenges and difficulties that may arise during the compliance process and that should be taken into account in its design and implementation.

(1) **Regulatory proliferation and complexity**: this is one of the foremost difficulties, since, on the one hand, companies must contend with a growing body of regulations (specially difficult to track them all when operating across multiple jurisdictions and sectors), and, on the other hand, these numerous laws, rules and standards across different regions and industries force organisations to thoroughly understand and adhere to a tangle of regulations and requirements that often overlap or contradict each other, and differ depending on the location, sector of activity, among other factors.

[60] Forensic readiness is a key element of a company's information risk management strategy that can ensure the ability to respond effectively in case of an incident ad reduce the impact of a data breach, as well as maximise the potential to use digital evidence whilst minimising the cost of an investigation (Sachowski, 2019).

(2) **Keeping up with changes, mostly in the ever-changing world of cyberspace**: regulations and standards are constantly being revised, developed and replaced by others (as seen in the legal framework) as new threats –specially cyber threats– emerge and technologies advance. Keeping up to date with these changes that directly affect the CCS demands ongoing vigilance and adaptation, which can strain internal resources.

(3) **Raising awareness and ethical culture**: a lack of process awareness and ethical culture or failure to understand business processes often lead to errors and incompetence that can hinder companies to stay compliant and result in inefficient or redundant processes, which not only cost organisations time and money, but also make it harder to track output efficiently to detect and correct errors to meet regulatory compliance. This is why it is so important to train all members involved and to provide enough incentives to motivate and raise awareness of their importance, as well as to have adequately and sufficiently trained and experienced professionals (specially, the Compliance Officer).

(4) **Cross-departmental coordination and accurate data**: compliance integrates and affects all parts of a company. Hence, effective communication and coordination between departments are critical, although it can be complicated when they differ priorities or understandings regarding data security protocols. This can result in inaccurate data, which facilitates the emergence of errors and inefficiencies and makes it difficult to make decisions that comply with regulatory standards.

(5) **Adequate and sufficient resource allocation**: organisations must invest financially and allocate the right human capital to manage and execute compliance-related tasks effectively, which is a substantial challenge in compliance management.

(6) **Critical self-assessment**: compliance is a self-regulated and self-managed sector, which requires a hard work of self-criticism, honesty and rigour to detect and correct failures, which in the long run will ensure greater effectiveness and efficiency and may lead to exemption from criminal liability in the event of a criminal offence being committed. In this respect, it is essential that managers themselves show commitment and address this issue as a priority (*tone from the top*).

(7) **Integration with existing systems**: implementing new compliance controls often involves integrating them within established systems without disrupting ongoing operations, which is a task that requires careful planning and execution.

Despite their difficulty and the effort required, effectively addressing these challenges is crucial for maintaining robust cybersecurity defences and upholding an organisation’s reputation in today’s stringent regulatory environment.

IV. Conclusions

Compliance is increasingly gaining relevance in organisations and, beyond a legal requirement, it is becoming a necessary condition for governance and ethical integrity, business competitiveness and sustainability, which requires a transversal and multidisciplinary study (beyond the legal and economic sphere), as it is an interdisciplinary issue with multiple dimensions (legal, economic-business, ethical, criminological). Therefore, while the cornerstone of the compliance function is crime prevention, compliance encompasses much more, such as compliance with data protection regulations, prevention of money laundering or competition law; closely associated with ethics, good corporate governance, accountability and corporate risk management.

As repeatedly stated in this work, the world of criminal compliance is dynamic, iterative, in continuous feedback and evaluation and it must be adapted to each organisation's particularities. As technology and science advances, regulatory frameworks evolve and criminal landscapes shift –specially in the cybersecurity landscape–, so too must compliance programmes. Thus, some of the key elements to consider within a forward-thinking compliance approach are the following:

On the one hand, a CCS (for, in line with ISO standards, it is better to refer to a Compliance system or Compliance management system, rather than Compliance programme) is not a set of "set-and-forget" initiatives, but rather a continuous improvement and flexible process. Thus, organisations must continuously review, update and refine their programmes and policies to remain effective in the face of evolving threats, mostly in the cybercrime landscape, which is constantly changing, with new threats and vulnerabilities emerging at an alarming rate.

Strictly related to the above, incorporating ongoing threat assessments and the latest security measures to address evolving risks becomes fundamental: new technologies, such as artificial intelligence and machine learning have the potential to revolutionize compliance efforts by automating tasks, enhancing risk assessments and facilitating data analysis that should be further explored. However, ethical considerations and integration challenges need careful consideration.

Furthermore, organisations operating in a globalized environment face a complex web of international regulations and standards that are too constantly being modified, which make it difficult for companies –specially, small and medium-sized enterprises– to keep up with all of them, mainly if they operate in different jurisdictions, each with its own set of laws and rules. Therefore and as a proposal *de lege ferenda*, harmonization of compliance standards across jurisdictions becomes crucial for streamlined and efficient compliance practices (beyond ISO standards).

On the other hand, developing a strong culture of ethics and compliance within companies remains cornerstone to preventing criminal activity. While the adoption of a code of ethics is one of the main elements, the establishment of a genuine compliance culture in the company goes much further and requires ongoing communication, training programmes and leadership commitment to ethical behaviour throughout all levels of the organisation. And regarding cybersecurity, is even more important building a strong culture of cybersecurity awareness through ongoing training and education programmes by all employees that equip them with the knowledge and skills to identify suspicious activity, report potential security breaches, and follow secure practices, since they are often the first line of defence against cyber threats.

In fact, effective CCS have a two-pronged character, since, on the one hand, they constitute a system of risk management and obligations of the legal person, delimited and concrete, capable of exempting it from criminal liability; but, on the other hand, their correct design and implementation are indicators of a culture of compliance of the legal person, reflected in the content of the compliance programme and policies.

Moreover, and even though control measures such as investigations and the provision of a disciplinary system are often important to ensure the effectiveness of the CCS, they should only be applied sparingly and where strictly necessary, and, in any case, subject to the Punitive law principles: not only the principles of legality and typicity, but also of proportionality, in order to prevent the sanctions provided for from having a counterproductive effect by discouraging compliance for fear of disproportionate sanctions. Much better is, though, to opt for incentives, which foster a culture of trust and awareness so that members of the company are intrinsically motivated to comply.

Whistleblowing channels are also a controversial element of a CCS and must thus be well defined and in accordance with laws and human rights and ensure the impartiality of the inspector –Compliance Officer– as well as the confidentiality –and, if possible, anonymity– of the complainant without risk of reprisal, to foster the reporting by employees of suspected non-compliance with the Compliance programme and policies.

Another important issue is robust data security and privacy measures, since organisations collect and use increasing amounts of data and since data breaches and cyberattacks continue to plague organisations, exposing sensitive information and potentially leading to financial and reputational damage. Hence, CCS must comply with data protection laws such as GDPR and prioritize data security best practices and ethical data management, including encryption, access controls and incident response plans.

Along the same lines, in today's interconnected environment, organisations rely heavily on third-party vendors and partners who may access sensitive data or systems, in a way that rigorous due diligence, contractual requirements for compliance with security standards and ongoing monitoring of third-party security posture are crucial for minimizing vulnerabilities.

In light of the above, the future of effective criminal compliance in the IT security sector hinges on a proactive and adaptable approach: organisations that embrace continuous improvement, leverage technological advancements responsibly, nurture ethical cultures and raise cybersecurity awareness, prioritize data security and privacy and navigate the complexities of global compliance will be best positioned to mitigate criminal risks and thrive in an ever-changing landscape while maintaining trust with stakeholders, and contributing to a more secure digital environment. By prioritizing robust and adaptable criminal compliance, companies can not only protect themselves from legal and reputational damage, but also play a vital role in mitigating the global threat of cybercrime and foster a more ethical and trustworthy business environment for all.

References

Afsharipour, Afra, & Rana, Shruti. (2014). The Emergence of New Corporate Social Responsibility in China and India. *U.C. Davis Business Law Journal*, *14*, 175-230.

Aguilera, R. (2022). *Manual de Compliance Penal en España: Régimen de responsabilidad penal de las personas jurídicas. Fundamentación analítica de base estratégica. Requisitos del Compliance Program* (2nd Ed.). Aranzadi

Akers, R. L. (1997). *Criminological theories*. Roxbury Publishing Company.

Andreoli, N., & Lefkowitz, J. (2009). Individual and organizational antecedents of misconduct in organizations. *Journal of Business Ethics*, *85*(3), 309-332.

Antich, Jaume. (2017). Compliance Program Penal y sus efectos en la exención y atenuación de la responsabilidad penal de la persona jurídica [Doctoral Thesis in Public Law and Political Legal Philosophy]. Universitat Autònoma de Barcelona, Spain. https://ddd.uab.cat/record/188083

Anwita. (2024, January 03). A Quick Overview of Compliance Framework. *Sprinto*. https://sprinto.com/blog/compliance-framework/

Ariely, D., & Mann, H. (2013). A bird's eye view of unethical behavior: Commentary on Trautmann et al. (2013). *Perspectives on Psychological Science, 8,* 498-500.

Arocena, Gustavo, (2017). Acerca del denominado criminal compliance. *Revista Crítica Penal y Poder*, (13), 128-145. https://revistes.ub.edu/index.php/CriticaPenalPoder/article/view/19320

Artaza, O. (2013). *La empresa como sujeto de imputación de responsabilidad penal: Fundamentos y límites* (pp. 118 ff.). Marcial Pons.

Askew, O. A., Beisler, J. M., & Keel, J. (2015). Current trends of unethical behavior within organizations. *International Journal of Management & Information Systems*, *19*(3),107-114.

Australian National University. (2023, June 27). *Policy: Information technology security*. https://policies.anu.edu.au/ppl/document/ANUP_000421

Bacigalupo, Enrique. (2011). *Cumplimiento y Derecho Penal*. Aranzadi.

Bandura, A. (1982). *Teoría del Aprendizaje Social*. Alianza.

Beccaria, Cesare (1957). *On Crimes and Punishments*. Clarendon Press. (Original work published in 1764)

Becker, Gary S. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy*, *76*(2), 169-217.

Becker, H. (2012). *Outsiders: Hacia una sociología de la desviación* (2nd reimp.). Siglo XXI Editores. (Original work published in 1963)

Bentham, Jeremy. (1789). *An Introduction to the Principles of Morals and Legislation*. Clarendon Press.

Blackwell, Barry. (1992). Compliance. *Psycotherapy and psychosomatics, 58*, 161-169.

Bleker, Sylvie, & Hortensius, Dick. (2014). ISO 19600: The development of a global standard on compliance management. *Business Compliance, 2014*(2), 3-5. http://www.nen.nl/web/file?uuid=81d60dcf-dd04-4820-8ccb-bb685a0786fc&owner=ccdd2a27-7f28-43b1-a3cb-d01e2bf2a56a&contentid=171861

Bondarenko, Peter. (2024, January 4). Enron scandal: United States history. *Britannica: History & Society*. https://www.britannica.com/event/Enron-scandal

Brown, Schuyler. (2023, May 23). 3 Types of Access Control: IT Security Models Explained. StrongDM. https://www.strongdm.com/

Capdeferro, Òscar. (dir.), Cerrillo, Agustí, Màrquez, Sandra, Obregon, Isidre, & Ponce, Juli. (2023). La governança del Codi ètic del servei públic de Catalunya: Fonaments i proposta. *Estudis de Recerca Digitals, 20*. School of Public Administration of Catalonia. https://shorturl.at/sIJOQ

Carrau, Rafael. (2016). *Compliance para PYMEs*. Tirant lo Blanch.

Casanovas, Alain. (2013). *Legal Compliance: Principios de cumplimiento generalmente aceptados*. Difusión Jurídica.

Cassidy, D., Goldstein, L., Johnson, S. L., Mattie, J. A., & James Jr. (2001). *Developing a strategy to manage enterprisewide risk in higher education*. NACUBO and PricewaterhouseCoopers. https://www.cuny.edu/wp-content/uploads/sites/4/page-assets/about/administration/offices/ehsrm/risk/nacubo_rm.pdf

Chalfin, Aaron, & Justin McCrary. (2017). Criminal Deterrence: A Review of the Literature. *Journal of Economic Literature, 55*(1), 5-48. https://doi.org/10.1257/jel.20141147

Chartered Financial Analyst (CFA) Institute. (2017). *Environmental, Social and Governance (ESG) Survey*. https://www.cfainstitute.org/-/media/documents/survey/esg-survey-report-2017.ashx

Chaturvedi, T., Wali, O. P., & Kesharwani, A. (2019). Enhancing Competitiveness through Compliance: Case of Technology Compliance. *Theoretical Economics Letters, 9*, 2397-2417. https://doi.org/10.4236/tel.2019.97152

Check Point Research (CPR) Team. (2023). *Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks.*

https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *South African Journal of Information Management, 23*(1). http://dx.doi.org/10.4102/sajim.v23i1.1277

Clark, M. A., & Leonard, S. L. (1998). Can Corporate Codes of Ethics Influence Behavior? *Journal of Business Ethics, 17*(6), 619-630.

CMS Law-Now (2021, May). *The CEE guide to the criminal liability of corporate entities*. https://cms.law/en/media/local/cms-cmno/files/publications/publications/the-cee-guide-to-criminal-liability-of-corporate-entities-cms?v=2

Committee of Sponsoring Organizations (COSO). (2023). *Home*. COSO. https://www.coso.org/about-us

Cosker, Glynn. (2023, February 05). *What Is Information Technology? A Beginner's Guide to the World of IT.* Rasmussen University. https://www.rasmussen.edu/degrees/technology/blog/what-is-information-technology/

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap Risk Insur Issues Pract, 47*, 698-736. https://doi.org/10.1057/s41288-022-00266-6

Criminal Division of the U.S. Department of Justice and the Enforcement Division of the U.S. Securities and Exchange Commission. (2020, July). *FCPA: A Resource Guide to the U.S. Foreign Corrupt Practices Act* (2nd Ed.). FCPA guide. https://www.justice.gov/criminal/criminal-fraud/file/1292051/dl?inline

Deci, E. L., Koestner, R., & Ryan, R. M. (1999). A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological Bulletin, 125*(6), 627-668. https://doi.org/10.1037/0033-2909.125.6.627

Del Rocío, María. (2019). Estudio sobre Compliance, antecedentes y perspectivas de futuro: Caso aplicado a empresas de publicidad. [Bachelor's Degree Final Project in Law and Business Administration and Management]. Universidad de Sevilla, Spain. https://idus.us.es/handle/11441/104744

Directive 2004/39/EC. *Directive (EU) 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC* (MiFID I). European Parliament and Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0039

Directive 2005/29/EC. *Directive (EU) 2005/29 of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance).* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32005L0029

Directive 2014/65/EU. *Directive (EU) 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast) Text with EEA relevance* (MiFID II). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32014L0065

Directive 2022/2555/EC. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2022/2555

Dubber, Markus D., & Hörnle, Tatjana. (eds.). (2014). *The Oxford Handbook of Criminal Law*. Oxford.

Dutton, Julia. (2021, August 23). *What is an Information Security Management System (ISMS)?* IT Governance USA. https://www.itgovernanceusa.com/blog/what-exactly-is-an-information-security-management-system-isms-2

EALDE, Bussines school. (2020). *Gestión de riesgos: Qué es la norma ISO 31000 y para qué sirve*. EALDE. https://www.ealde.es/iso-31000-para-que-sirve/

Elías, G., & Muñoz. (2023, November 21). *Criminal compliance: What is it?* G. Elías & Muñoz abogados. https://www.eliasymunozabogados.com/en/blog/criminal-compliance-what-it

Engelhart, Marc. (2018). *The nature and basic problems of compliance regimes*. Beiträge zum Sicherheitsrecht (in ArchiS, Architecture of Security Law), Max-Planck-Institut für ausländisches und internationales Strafrecht. https://pure.mpg.de/rest/items/item_2643714_7/component/file_3007899/content

Enseñat, Sylvia. (2016). *Manual de compliance officer: Guía práctica para los responsables de Compliance de habla hispana*. Aranzadi.

Escudero, Marta. (2015). Diagnóstico y mapa de riesgos de *Compliance*. In *Compliance: Cómo Gestionar los Riesgos Normativos en la Empresa* (Block III, Chapter 2), Aranzadi.

Franco, M. F., Künzler, F., von der Assen J., Feng, C., & Stiller, B. (2024). RCVaR: An economic approach to estimate cyberattacks costs using data from industry reports. *Computers & Security*, *139*(103737), 1-13. https://doi.org/10.1016/j.cose.2024.103737

Generalitat de Catalunya (2023, January 25). *Codi ètic del servei públic de Catalunya*: *Acord GOV/164/2021, de 26 d'octubre, d'adopció del Codi ètic del servei públic de Catalunya per part del Govern de la Generalitat i l'Administració de la Generalitat i les entitats del seu sector públic*. Govern obert, Generalitat de Catalunya. https://governobert.gencat.cat/ca/integritat-publica/codi-etic-del-servei-public-de-catalunya/

Gneezy, Uri, & Rustichini, Aldo. (2000). A Fine is a Price. *The Journal of Legal Studies*, *29*(1), 1-17. https://doi.org/10.1086/468061

Gómez, Víctor. (2013). Parte III: Compliance y derechos del trabajador, especialmente derecho a la protección de datos y whistleblowing. In Lothar Kuhlen, Juan Pablo Montiel & Íñigo Ortiz (Ed.), *Compliance y teoría del derecho penal* (pp. 125-146). Marcial Pons.

Goñi, José Luis. (2014). Programas de cumplimiento empresarial ("compliance programs"): Aspectos laborales. In Santiago Mir, Mirentxu Corcoy (dir.) & Víctor Gómez (dir.), Juan Carlos Hortal & Vicente Valiente (coord.), *Responsabilidad de la empresa y compliance: Programas de prevención, detección y reacción penal* (pp. 367-420). Edisofer.

Grant, R. M., & Visconti, M. (2006). The strategic background to corporate accounting scandals. *Long Range Planning*, *39*, 361-383.

Griffiths, Charles. (2024). *The Latest 2024 Cyber Crime Statistics (updated February 2024)*. AAG: Security. https://aag-it.com/the-latest-cyber-crime-statistics/

Grijalvo M., Prida B., & Martín-Romo, C. (2002). La gestión por procesos y la mejora continua. Nuevas expectativas abiertas por la ISO 9000 (Versión 2000). *Dirección y organización: Revista de dirección, organización y administración de empresas*, *28*, 5-11.

Hassan, S., Wright, E., & Yukl, G. (2014). Does ethical leadership matter in government? Effects on organizational commitment, absenteeism, and willingness to report ethical problems. *Public Administration Review*, *74*(3), 333-343. https://doi.org/10.1111/puar.12216

Hermoso de Mendoza, Javier. (2018). *Legal compliance: El manual de prevención de riesgos penales* [Master's Degree Final Project in legal sciences]. Universidad Pública de Navarra, Spain. https://academica-e.unavarra.es/xmlui/handle/2454/27435

Hodges, Christopher, & Steinholtz, Ruth. (2017). *Ethical business practice and regulation: A behavioural and ethical values-based approach to compliance and enforcement*. Hart Publishing.

Hofeditz, M., Nienaber, A. M., Dysvik, A., & Schewe, G. (2015). "Want to" versus "Have to": Intrinsic and extrinsic motivators as predictors of compliance behavior intention. *Human Resource Management, 56*, 25-49.

Homann, Moritz. (2022, October 25). *How GRC, Compliance and CSR Work Together*. EQS Group AG. https://shorturl.at/jpCH9

Hoseah, E. G. (2014). Corruption as a global hindrance to promoting ethics, integrity, and sustainable development in Tanzania: The role of the anti-corruption agency. *Journal of Global Ethics, 10*, 384-392.

International Business Machines Corporation (IBM). (2023). *What is IT security?* https://www.ibm.com/topics/it-security

International Business Machines Corporation (IBM). *Cost of a Data Breach Report 2023*. https://www.ibm.com/reports/data-breach

International Labour Organization (ILO). (2019). *Monitoring Compliance with International Labour Standards: The key role of the ILO Committee of Experts on the Application of Conventions and Recommendations*. International Labour Office. https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---normes/documents/publication/wcms_730866.pdf

International Organization for Standardization & DIS (Draft International Standard). (under development). Anti-bribery management systems–Requirements with guidance for use (ISO/DIS Standard No. 37001). https://www.iso.org/standard/85816.html

International Organization for Standardization & International Electrotechnical Commission. (2018). Information technology: Security techniques–Information security management systems: Overview and vocabulary (ISO Standard No. 27000:2018). https://www.iso.org/standard/73906.html

International Organization for Standardization & International Electrotechnical Commission. (2019). Security techniques: Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management–Requirements and guidelines (ISO Standard No. 27701:2019). https://www.iso.org/standard/71670.html

International Organization for Standardization & International Electrotechnical Commission. (2011). Information technology: Security techniques–Guidelines for information and communication technology readiness for business continuity (ISO/IEC Standard No. 27031:2011). https://www.iso.org/standard/44374.html

International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection–Information security controls (ISO/IEC Standard No. 27002:2022). https://www.iso.org/standard/75652.html

International Organization for Standardization & International Electrotechnical Commission. (2013). Information technology: Security techniques–Code of practice for information security controls (ISO/IEC Standard No. 27002:2013, withdrawn and revised by ISO/IEC 27002:2022). https://www.iso.org/standard/75652.html

International Organization for Standardization & International Electrotechnical Commission. (2022). Information security, cybersecurity and privacy protection–Information security management systems: Requirements (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

International Organization for Standardization & International Electrotechnical Commission. (2013). Information technology: Security techniques–Information security management systems: Requirements (ISO/IEC Standard No. 27001:2013, withdrawn and revised by ISO/IEC 27001:2022). https://www.iso.org/contents/data/standard/05/45/54534.html

International Organization for Standardization & International Electrotechnical Commission. (2023). Information technology–Information security incident management–Part 2: Principles and process (ISO/IEC Standard No. 27035-1:2023). https://www.iso.org/standard/78973.html

International Organization for Standardization & International Electrotechnical Commission. (2023). Information technology–Information security incident management–Part 2: Guidelines to plan and prepare for incident response (ISO/IEC Standard No. 27035-2:2023). https://www.iso.org/standard/78974.html

International Organization for Standardization & International Electrotechnical Commission. (2011). Information technology: Security techniques–Information security incident management (ISO/IEC Standard No. 27035:2011, withdrawn and revised by ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016). https://www.iso.org/standard/44379.html

International Organization for Standardization. (2016). Anti-bribery management systems–Requirements with guidance for use (ISO Standard No. 37001:2016). https://www.iso.org/standard/65034.html

International Organization for Standardization. (2018). Risk management–Guidelines (ISO Standard No. 31000:2018). https://www.iso.org/standard/65694.html

International Organization for Standardization. (2019). Risk management–Risk assessment techniques (ISO Standard No. 31010:2019). https://www.iso.org/standard/72140.html

International Organization for Standardization. (2021). Compliance management systems–Requirements with guidance for use (ISO Standard No. 37301:2021). https://www.iso.org/standard/75080.html

International Organization for Standardization. (2021). Whistleblowing management systems–Guidelines (ISO Standard No. 37002:2021). https://www.iso.org/standard/65035.html

Jain, S. (2024). *160 Cybersecurity Statistics 2024*. Astra: Security Audit. https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=Cybersecurity%20statistics%20indicate%20that%20there,cost%20%248%20trillion%20by%202023

Jannat, T., Alam, S. S., Ho, Y.-H., Omar, N. A., & Lin, C.-Y. (2022). Can Corporate Ethics Programs Reduce Unethical Behavior?: Threat Appraisal or Coping Appraisal. *Journal of Business Ethics, 176*, 37-53. https://doi.org/10.1007/s10551-020-04726-8

Jimenez, Araceli. (2019). *Ethics in the Public Sector: Analyzing the ethical behavior of public sector employees* [Master's Degree Final Project in Public Administration, Public Sector Management and Leadership]. California State University, Northridge. https://scholarworks.calstate.edu/downloads/c247dw060

Jimenez, Gustavo A. (2019). Corporate Criminal Liability: Toward a Compliance-Orientated Approach. *Indiana Journal of Global Legal Studies, 26*(1), 353-379. https://www.repository.law.indiana.edu/ijgls/vol26/iss1/12

Johnson, Ben. (2019). *Do Criminal Laws Deter Crime? Deterrence Theory in Criminal Justice Policy: A Primer*. MN House Reaserch. https://www.house.mn.gov/hrd/pubs/deterrence.pdf

Kaptein, M. (2015). The effectiveness of ethics programs: The role of scope, composition, and sequence. *Journal of Business Ethics, 132*, 415-431.

Kaptein, M., & Schwartz, M. S. (2008). The effectiveness of business codes: A critical examination of existing studies and the development of an integrated research model. *Journal of Business Ethics, 77*(2), 111-127.

Kar, S. (2014). Ethical leadership: Best practice for success. *Journal of Business and Management*, 112-116. https://www.semanticscholar.org/paper/Ethical-Leadership-%3A-Best-Practicefor-Success-Kar/08a921d1f8b4185425cde44229216640904a91f2

Knight, Frank H. (1921). *Risk, Uncertainty and Profit* (1921). Houghton Mifflin Company.

Kotlán, P., Ondrúš, M., Kozlová, A., Kotlán, I., Petr, P., & Kalabis, R. (2023). Criminal compliance program as a tool for criminal liability exculpation of legal persons in the Czech Republic. *Laws, 12*(2), 1-15. https://doi.org/10.3390/laws12020020

Koza, Erfan, & Öztürk, Asiye. (2023). How can ISO/IEC 27001:2013 be associated with ISO/IEC 27001:2022, ISO/IEC 27002:2022, and 27019:2018 using the mapping table? *The 33rd European Safety and Reliability Conference (ESREL 2023)*, 3228-3235. https://www.rpsonline.com.sg/proceedings/esrel2023/html/P144.html

Lerma, Agustín. (2012). ISO 31000:2009: Gestión estratégica del riesgo. Forum calidad, 24(235), 26-31.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Màrquez Postigo, Sandra. (2022). Poden servir els codis ètics per prevenir la corrupció?: estudi exploratori de la percepció d'efectivitat del codi ètic del servei públic de Catalunya (2021) [Master's Degree Final Project in Criminology and Criminal Justice System]. Universitat Pompeu Fabra, Barcelona, Spain. http://hdl.handle.net/10230/53582

Matallín, Ángela & Fernández, Antonio (dir.). (2023). *Criminal compliance programs y mapas de riesgos*. Tirant lo Blanch.

McDonald, G., & Nijhof, A. (1999). Beyond Codes of Ethics: An Integrated Framework for Stimulating Morally Responsible Behaviour in Organisations. *Leadership and Organization Development Journal, 20*(3), 133-146.

Moscariello, N., Pizzo, M., Ricciardi, G., Mallardo, G., and Fattorusso, P. (2022). The anti-corruption compliance models in a multinational company: A single case study. *Business Strategy and the Environment*, *33*(1), 70-80. https://doi.org/10.1002/bse.3331

Nieto, Adán. (2006). *Manual de derecho penal económico y de empresa: Parte general y parte especial*. Tirant lo Blanch.

Nieto, Adán. (2015). *Manual de cumplimiento penal en la empresa*. Tirant lo Blanch.

Organisation for Economic Cooperation and Development (OECD) (2024, February 22). *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct*. OECD. https://mneguidelines.oecd.org/mneguidelines/

Organisation for Economic Cooperation and Development (OECD). (2022). *Translating a risk-based due diligence approach into law: Background note on Regulatory Developments concerning Due Diligence for Responsible Business Conduct*. https://mneguidelines.oecd.org/translating-a-risk-based-due-diligence-approach-into-law.pdf

Pereira, A. N., Machado, F. G., Bon, F., & de Carvalho, S. (coord..). (2022). *Compliance dialogues* (ed. 1). Instituto Ibero-americano de Compliance. https://isal.pt/wp-content/uploads/2023/01/e-book_compliance_dialogues_isbn_isal.pdf#page=14

Petrosyan, A. (2023, October 23). *Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023*. Statista: Cyber Crime & Security. https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

Pollman, Elizabeth. (2021). Corporate Social Responsibility, ESG, and Compliance. *Faculty Scholarship at Penn Carey Law, 2568*, 1-20. https://scholarship.law.upenn.edu/faculty_scholarship/2568

PricewaterhouseCoopers (PwC). (2022) *PwC's Global Economic Crime and Fraud Survey 2022: Protecting the perimeter: A new frontier of platform fraud*. PricewaterhouseCoopers. https://www.pwc.com/gx/en/forensics/gecsm-2022/PwC-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

PricewaterhouseCoopers (PwC). (2024, January 15). *PwC's 27th Annual Global CEO Survey: Thriving in an age of continuous reinvention*. PricewaterhouseCoopers. https://www.pwc.com/gx/en/issues/c-suite-insights/ceo-survey.html

Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act). European Parliament and Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

Quinn, J. M., Rich, S., Bureau of National Affairs (Arlington, V.) & Bloomberg Law. Corporate compliance: Building a world-class borderless ethics compliance program. *Corporate Practice Portfolio Series 103*.

Ragués, Ramon. (2013). *Whistleblowing: Una aproximación desde el Derecho Penal*. Marcial Pons.

Redondo, S., & Garrido, V. (2013). *Principios de Criminología: La nueva edición* (4th ed.). Tirant lo Blanch.

Regulation 2016/679/EC. *Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. European Parliament and Council. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504

Regulation 2019/881/EC. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*. European Parliament and Council. https://eur-lex.europa.eu/eli/reg/2019/881/oj

Rimkus, Ron. (2016, November 29). Parmalat. *Chartered Financial Analyst (CFA) Institute: Financial Scandals, Scoundrels & Crises*. https://www.econcrises.org/2016/11/29/parmalat/

Root, Veronica. (2019). The Compliance Process. *Indiana Law Journal*, *94*(1), 203-251. https://www.repository.law.indiana.edu/ilj/vol94/iss1/5

Roxin, C. (1997). *Derecho penal. Parte general, tomo I: Fundamentos. La estructura de la teoría del delito* (2ª ed.). Translation and notes by Luzón, D. M., Díaz, M., & Vicente, J. Civitas.

Sachowski, Jason. (2019). *Implementing Digital Forensic Readiness: From Reactive to Proactive Process* (2nd Ed.). CRC Press.

Sáiz, Carlos Alberto. (2015). *Compliance: Cómo Gestionar los Riesgos Normativos en la Empresa*. Aranzadi.

Sarker, Sudipa. (2018). The Paradox of Risk Management: A Supply Management Practice Perspective. In *Revisiting Supply Chain Risk*, Vol. 7 (pp. 421-437), Springer. https://doi.org/10.1007/978-3-030-03813-7_24

Serafín, Aníbal, & Bello, Nohemí. (2023). Normativa ISO en la aplicación del Criminal Compliance en México. *Revista Misión Jurídica*, *16*(24), 193-214. https://doi.org/10.25058/1794600X.2213

Sieber, Ulrich. (2013). Programas de "compliance" en el Derecho penal de la empresa: Una nueva concepción para controlar la criminalidad económica. In Luis Arroyo Zapatero & Adán Nieto (dir.), *El derecho penal económico en la era de la compliance* (pp. 63-110). Tirant lo Blanch.

Silva, Jesús-María (dir.), & Montaner, Raquel (coord.). (2014). *Criminalidad de empresa y Compliance: Prevención y reacciones corporativas* (pp. 168-169). Atelier.

Sobers, Rob. (2024). 161 *Cybersecurity Statistics and Trends [updated 2023]*. Varonis: Data Security. https://www.varonis.com/blog/cybersecurity-statistics#attack

Stessens, Guy. (1994). Corporate criminal liability: A comparative perspective. *The International and Comparative Law Quarterly*, *43*(3), 493-520.

Sutherland, E. H. (1983). *White collar crime: The uncut version*. Yale University Press.

Teichmann, Fabian, & Wittmann, Chiara. (2024). Compliance cultures and the role of financial incentives. *Journal of Financial Crime*, *31*(1), 226-232. https://www.emerald.com/insight/content/doi/10.1108/JFC-06-2022-0135/full/html

Teichmann, Fabian, Wittmann, Chiara, & Boticiu, Sonia. (2023). Compliance as a form of defense against corporate criminal liability. Journal of Economic Criminology, 1 (100004), 1-4. https://doi.org/10.1016/j.jeconc.2023.100004

Tiedemann, Klaus. (1972). Welche strafrechtlichen Mittel empfehlen sich für eine wirksamere Bekämpfung der Wirtschaftskriminalität. In *Verhandlungen des 49. Deutschen Juristentages*, Vol. I, Part C (pp. 21 ff.). Beck.

United Nations (UN). (2021). *UN Global Compact Strategy 2021-2023*. United Nations Global Compact. https://unglobalcompact.org/library/5869

Vera, Carlos. (2017). Implementación de un modelo de compliance. [Master's Degree Final Project in Law]. Universidad de Zaragoza, Spain. https://zaguan.unizar.es/record/64567

Von Hirsch, A., Bottoms, A. E., Burney, E., & Wikström, P.-O. (1999). *Criminal Deterrence and Sentence Severity: An Analysis of Recent Research*. Bloomsbury 3PL.

Von Lampe, Klaus. (2002). Assessing Organized Crime: The Case of Germany. *ECPR Standing Group eNewsletter Organised Crime*. http://www.organized-crime.de/kvlECPRNL0309.pdf

Wong, Ken K.-K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin, 24*, 1-32.

World Compliance Association (WCA). (2019, May). *Guía de implementación de compliance para pymes: "Manual práctico de implementación"*. WCA. https://www.worldcomplianceassociation.com/documentacion/Guia_Compliance_web_v.02.pdf

World Compliance Association (WCA). (2024). Compliance: ¿Qué es? *WCA*. https://www.worldcomplianceassociation.com/index.php?language=es

World Economic Forum. (2022). *The Global Risks Report 2022: 17th Edition*. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

World Economic Forum. (2023, January). *Global Cybersecurity Outlook 2023*. https://www.weforum.org/publications/global-cybersecurity-outlook-2023/

WorldCom Files for Largest Bankruptcy in U.S. History (July 22, 2002). *PBS: Economy*. https://www.pbs.org/newshour/economy/business-july-dec02-worldcom_07-22