ENFCO

EUROPEAN NETWORK FOR
COMPLIANCE OFFICERS

The evolving purpose, scope and success factors of Compliance: why Compliance must be independent from Legal function

Whitepaper
September 2025

Foreword

Lead working group Strategic positioning of Compliance and Representative Ethics & Compliance Switzerland

Dear Compliance Community,

The traditional view of Compliance as solely a guardian against legal pitfalls is outdated. Today, stakeholders – from regulators and investors to employees and consumers- demand more than just adherence to rules, they expect genuine ethical conduct and demonstrate corporate responsibility. As a result, the purpose and scope of Compliance changed from a risk mitigation function to a holistic commitment to organizational integrity and ethics.

The working paper articulates the critical success factors of the Compliance department, critically evaluates existing organizational models of Compliance department and provides a compelling argument for structural separation of Legal and Compliance function. The work paper also discusses how Compliance departments can use new technology to their advantage. Therefore, this working paper is intended for senior Boards, compliance officers and ethics leaders who are shaping the strategic role of compliance within their organization.

I would like to extend my heartfelt thanks to the members of the Working Group "Strategic Positioning of Compliance", Andrijana Bergant, Carlos M. Martins, Lucia Sanchez-Ocana Luyen and Radomir Dukov, for their dedication and invaluable contributions to this project. Their expertise and commitment have been instrumental in making this study a success.

Enjoy reading!

Patrick Wellens

Content

About ENFCO

ENFCO (European Network for Compliance Officers) is a network of not-for-profit associations for in-house compliance professionals across Europe. The organization facilitates the cooperation and communication between the participating associations and their incorporated professionals in the best spirit of a European community, according to the network's mission goals.

At the time of publication, the following Compliance Association (listed alphabetically) are members of ENFCO:

- AICOM (Associazione Italiana de Compliance) (Italy)
- ASCO (Association of Compliance Officers) (Greece)
- ASCOM (Asociacion Espanola de Compliance) (Spain)
- BAAFC experts (Bulgarian Association of Anti-Financial Crime Experts) (Bulgaria)
- BCM (Berufsverband der Compliance Manager) (Germany)
- Compliance Hub (Kazakhstan)
- Compliance Institute (Ireland)
- Compliance Pro (Belgium)
- Cumplen (Spain)
- Ethics and Compliance Switzerland (Switzerland)
- EICE (European Institute for Compliance and Ethics) (Slovenia)
- French Compliance Society (France)
- GACO (Gibraltar)
- GACO (Guernsey)
- Le Cercle de la Compliance (France)
- Nordic Business Ethics Initiative (Nordic Countries)
- ÖCOV (Austria)
- OPCR - Observatório Português de Compliance e Regulatório (Portugal)
- Slovak Compliance Association (Slovakia)
- VCO (Vereniging Compliance Officers) (Netherlands)

More information about ENFCO can be found on its website https://www.enfco.eu/

Management Summary

The purpose and scope of corporate compliance are undergoing a profound transformation, moving beyond mere risk mitigation to embrace a holistic commitment to organizational integrity and ethics. This evolution necessitates a critical re-evaluation of Compliance's structural placement within the corporate hierarchy, strongly advocating for its complete independence from the Legal function. Decoupling Compliance from Legal is not merely a structural adjustment but a strategic imperative that delivers significant advantages in today's complex regulatory and ethical landscape as this strategic paper will clearly highlight.

The traditional view of Compliance as solely a guardian against legal pitfalls is outdated. Today, stakeholders – from regulators and investors to employees and consumers – demand more than just adherence to rules; they expect genuine ethical conduct and demonstrable corporate responsibility. This shift emphasizes the "ethical premium," where a strong, independent Compliance function becomes a key driver of trust, reputation, and sustainable value.

For Compliance to effectively champion this expanded mandate, its independence is paramount. This requires:

- **Direct Access to the Board:** Unfiltered communication and accountability to the highest governance body are essential for strategic alignment and oversight.
- **Independent Decision-Making:** Autonomy in determining resource allocation and shaping crucial compliance initiatives, free from potential conflicts of interest inherent in a legal department.
- **Seat at the table:** Rather than be represented by the General/Division/Regional Counsel in Management meetings, the (Chief Compliance/Divisional/Regional) Compliance officer should be present in, actively engage with and inform Senior Management about compliance risks when strategic decisions on new business ventures, market expansion, mergers and acquisitions, or new product development *before* decisions are finalized.
- **Driving Organizational Values:** An independent Compliance function is uniquely positioned to embed and promote a culture of integrity, shaping employee behavior and decision-making from the ground up, rather than merely policing against legal violations.

The benefits of a distinct Compliance function, disconnected from Legal, are multifaceted. It fosters a proactive, rather than reactive, approach to ethical conduct, enhances transparency, and reduces the perception of potential conflicts where the same function advises on legal risk while simultaneously overseeing compliance with those very risks. This separation allows Legal to focus on its core advisory and litigation responsibilities, while Compliance can concentrate on fostering an ethical culture and ensuring systemic adherence to internal and external standards.

Various compliance models such as (de)central compliance teams, regional/divisional compliance officers, Compliance Champions, Compliance shared service centers or outsourcing compliance activities have certain advantages but also come with numerous disadvantages and not all are effective. Companies therefore need to critically evaluate the organization model for the Compliance function and for Compliance to thrive make sure that success factors such as independence, sufficient resources, empowerment, and seat at the table are met.

Looking ahead, new technologies, particularly Artificial Intelligence (AI), will reshape the industry. AI will undoubtedly absorb routine, rule-based compliance tasks, enhancing efficiency and accuracy. However, AI will not replace the Compliance function's ultimate role as the ethical compass and decision-maker on complex integrity matters. This technological shift, coupled with the expanding scope, necessitates a continuous investment in new skills and ongoing training for compliance professionals.

In conclusion, this document will evidence why establishing a robust, independent Compliance function is no longer a luxury but a strategic necessity. The implications for companies that decouple Compliance from Legal are highly advantageous, leading to stronger governance, enhanced ethical standing, increased stakeholder trust, and ultimately, a more resilient and sustainable enterprise in the modern business environment.

A. Purpose & Focus of this Paper

A.1. Objective and Aims

This paper aims to

1. analyze the evolving scope and purpose of Compliance within organizations
2. critically evaluate existing organizational models of Compliance departments
3. articulate the critical success factors for compliance function.
4. benefits that an effective compliance program brings to the business
5. Examining the distinct mandates and skill sets required for effective Compliance, this paper will provide a compelling argument for structural separation of the Legal and Compliance Function, ultimately enhancing organizational integrity and resilience across the European landscape.
6. Give an outlook on the future of compliance

A.2. Intended Audience

This white paper is intended for senior executives, Boards, compliance officers, legal professionals, integrity and ethics leaders, and governance stakeholders who are shaping or influencing the strategic role of compliance within their organizations. It offers insights into the evolving positioning of compliance—from a traditionally reactive, legal-driven function to a more proactive, integrity-focused approach—highlighting the implications for organizational culture, risk management, and long-term value creation.

B. Structure of this Paper

This white paper is structured to guide the reader through the evolving role and strategic positioning of compliance within organizations. It is organized as follows:

- **Chapter C** outlines the historical context of compliance, focusing on its traditional role as a reactive, legal-driven function and the shift towards a more proactive, integrity-based approach to compliance.
- **Chapter D** describes the purpose and scope of compliance today, the core pillars of compliance and the difference between legal advice and ethical guidance.
- **Chapter E** highlights the structural problems when Compliance is part of Legal function
- **Chapter F** lists the benefits of an independent Compliance function
- **Chapter G** describes the (dis) advantages of the various organizational models of Compliance
- **Chapter H** lists the success factors of Compliance
- **Chapter I** provides examples of how Management and the Board weakens the effectiveness of Compliance Programs
- **Chapter J** discusses new technologies such as Artificial Intelligence and the impact on Compliance
- **Chapter K** is an Outlook into the future and the skillset needed for Compliance officers

Together, these chapters provide a comprehensive view of the transformation of compliance from a legal safeguard to a strategic enabler of integrity and organizational resilience.

C. Introduction: The evolving role of Compliance

C.1. Historical Background- Compliance as a legal sub-function

The Watergate scandal of the early 1970s, which surfaced into public as former U.S. President Richard Nixon resigned, exposed not only domestic political misconduct but also a broader pattern of unethical financial practices by large corporations. Investigations revealed that high-level political espionage and campaign manipulation were supported by illegal corporate donations and money laundering. Some of which were also interfering with foreign politics, orchestrated by U.S. officials and business interests.

In the aftermath, public and governmental scrutiny intensified around the role of U.S. corporations in foreign affairs, particularly the use of bribery to secure business advantages abroad. Subsequent inquiries uncovered widespread corrupt payments made by American companies to foreign officials across various countries.

In response, the U.S. enacted the **Foreign Corrupt Practices Act (FCPA)** in 1977. This legislation prohibits the bribery of foreign public officials and mandates accurate record-keeping and internal controls for publicly traded companies. It marked a significant shift in international business regulation, setting a precedent for global anti-corruption frameworks.

It was not until 2008, when the FCPA enforcement expanded significantly. U.S. authorities in cooperation with other governments have pursued American and foreign multinational corporations for violations World-wide, often resulting in substantial financial penalties for foreign bribery, long-term compliance obligations, and reputational damage. This robust enforcement approach has made anti-bribery compliance a central concern for global business operations and corporate governance.

Inspired by the FCPA, other jurisdictions have adopted similar frameworks, most notably the **UK Bribery Act**, which further broadens the scope of corporate liability for corrupt practices.

It’s not surprising that corruption has become one of the central compliance risk-areas and main driver of an independent compliance function, globally.

The future of anti-bribery remains uncertain in light of recent political developments in the US. A 2025 executive order aimed at halting or limiting FCPA enforcement may signal a potential shift in the U.S. stance on international anti-corruption efforts. Whether this will diminish the further development of global compliance practices and standards is a question for ongoing observation and analysis.

The **development of the compliance function** globally has roots in several parallel developments beyond the FCPA and Watergate. Two especially important drivers were the **need for self-regulation in high-risk sectors**—notably the **energy** and **defense industries**—and the **response to public spending scandals** involving these sectors in the U.S. and other countries.

A brief summary of key historical and structural origins:

Defense Industry Scandals and Oversight Mechanisms

- **Massive US government contracts and classified budgets**, which increased vulnerability to fraud, waste, and abuse.

- **Scandals such as the 1980s "Pentagon procurement scandal"**, where whistleblowers and journalists exposed inflated prices (e.g., $600 toilet seats) and corrupt contracting practices.
- In response, the **U.S. Department of Defense (DoD)** initiated more stringent internal controls and oversight requirements. This included:
  - The **Defense Industry Initiative (DII)** (launched in 1986), a **voluntary self-regulation program** among major defense contractors aimed at promoting ethical conduct, business integrity, and corporate self-governance.
  - Establishment of **internal compliance programs** within companies like Lockheed Martin, Raytheon, and Northrop Grumman to avoid debarment and retain government contracts.

These efforts positioned **compliance officers** as essential figures in managing reputational and regulatory risks.

Energy Sector: Environmental, Safety, and Anti-Corruption Drivers

The **oil and gas industry**, particularly in the 1990s and early 2000s, faced growing scrutiny for:

- Operating in **high-corruption-risk regions**, especially in resource-rich developing countries.
- Exposure to **bribery cases**, environmental disasters, and human rights controversies (e.g., Shell in Nigeria, BP in the Gulf of Mexico).
- Investor and stakeholder pressure for **greater transparency and sustainability**.

  In response:

- Major energy companies developed **internal compliance, ethics, and sustainability units**.
- The **Extractive Industries Transparency Initiative (EITI)**, launched in 2003, promoted disclosure of payments between governments and energy companies.
- The **Sarbanes-Oxley Act (2002)**, although finance-focused, also required stronger internal controls, indirectly influencing compliance practices in energy multinationals listed in the U.S.

Public Spending and Government Contracting Reforms

In broader terms, **public procurement scandals** (both domestic and international) led to:

- Stricter **bid-rigging and fraud prevention rules**.
- Growth of **corporate integrity agreements (CIAs)** in the U.S., where companies avoid prosecution by agreeing to independent oversight.
- Integration of **ethics and compliance requirements into public tenders**, requiring vendors to demonstrate effective compliance programs (e.g., OECD Anti-Bribery Convention pressures since 1997).

In continental Europe, compliance functions started to really flourish with the rise of EU regulation governing the financial sector, after the last big financial crisis of 2008 onwards. The EU directives and regulator's guidelines in the sphere of governance of the financial sector required the compliance function to be obligatory and one of the key functions in the context of internal governance and the internal control system of financial organizations. This is perhaps the reason that in Europe, we have been more focused on regulatory compliance as opposed to an overall compliance management system with business ethics and integrity highlights. It's not surprising that most compliance officers in Europe are to be found within the financial sector and have a legal background.

In many organizations in continental Europe, compliance functions in practice developed as a legal sub-function. Compliance associations across Europe are still seeing compliance officers being organized within the legal department and having a direct reporting line to the head of legal.

Developments over the last 10 years show that today more compliance officers operate within independent departments and have direct reporting lines to senior management and the board (committees).

C.2. The shift from legal risk mitigation to integrity and ethics

In continental Europe the real shift from mostly legal compliance to more of an ethics and integrity Compliance function is beginning to take hold, though it’s not yet the norm everywhere. A major reason for highly regulated organizations to still be focused on legal/regulatory compliance is the ongoing hyper-production of EU and national regulations. Consequently, we are witnessing increasing regulatory compliance fatigue, unrelenting push-back from the business and burned-out compliance officers.

We believe that this situation is going to lead more organizations to lean into a smarter risk-based approach to compliance and focus more on the culture of integrity and ethics in business. Some empirical evidence for the shift towards a more “Integrity and Ethics” focused Compliance are:

Regulatory Actions and Guidance

Beyond the Letter of the Law: Regulators are increasingly looking beyond mere technical compliance with rules. They are focusing on the *spirit* of the law and whether companies have fostered a culture of integrity. This is evident in:

- **Deferred Prosecution Agreements (DPAs) and Non-Prosecution Agreements (NPAs):** When settling enforcement actions, authorities (like the U.S. Department of Justice or the UK's Serious Fraud Office) often demand not just financial penalties but also commitments to enhance ethics and compliance programs, including fostering a "culture of compliance." This isn't just about preventing future legal violations but about embedding ethical conduct.

- **Focus on Root Causes and Culture:** Investigations often delve into the root causes of misconduct, specifically examining corporate culture, leadership tone, and whether ethical lapses were tolerated or even encouraged.

- **New Regulations with Ethical Dimensions:** Emerging regulations in areas like AI ethics (e.g., EU AI Act) and ESG reporting inherently demand an ethical framework, not just a legal one. They require companies to consider societal impact, fairness, and transparency, which go beyond traditional legal compliance. For example, the EU AI Act includes requirements for human oversight, risk management, and data governance that are rooted in ethical principles.

- **Anti-Corruption Frameworks:** International guidelines and conventions (like the UN Convention Against Corruption, OECD Anti-Bribery Convention) increasingly emphasize robust ethics and compliance programs as the most effective long-term deterrent against corruption, not just reactive legal measures. The "An Anti-Corruption Ethics and Compliance Program for Business: A Practical Guide"[1] by the OECD, World Bank, and UNODC explicitly details this shift, noting that "companies that understand that countering corruption requires more than complying with domestic laws and avoiding negative consequences are increasingly encouraged to set themselves apart from their peers."

[1] https://www.unodc.org/documents/corruption/Publications/2013/13-84498_Ebook.pdf

Academic Research and Publications

Studies on Ethical Culture: A growing body of academic research demonstrates the direct correlation between a strong ethical culture and reduced misconduct, improved financial performance, and enhanced reputation.

- **"Ethical Business Regulation: Understanding the [2]Evidence" (Gov.uk):** This report highlights that "compliant behavior cannot be guaranteed by regulation alone, and that ethical culture in business is an essential component that should be promoted and not undermined." It also emphasizes that "businesses should demonstrate constant evidence of their commitment to fair and ethical behavior that will support the trust of regulators and enforcers."

- **"The Overview of Compliance Management" (HRMARS)[3]:** This paper notes that "the development trend of enterprise compliance management shows that the motivation shifts from external pressure to endogenous demand" and that "the compliance scope is expanded from traditional finance to the whole industry, the compliance content is expanded from special to comprehensive." It specifically includes ethics and corporate social responsibility as core components of a qualified compliance management system.

- **"Beyond Compliance: The Role of Integrity in Management and Leadership"[4] (ResearchGate):** This study explores the relationship between integrity, compliance, and organizational culture, arguing that "solid integrity serves organizational objectives as a specific internal immune system, which protects against external and internal compliance challenges." It also emphasizes that "without an appropriate compliance function, there is no organizational integrity."

- **Distinction between "Compliance" and "Ethics":** Academic papers often distinguish between the two, advocating for a holistic approach. For example, studies from Trust Community[5] highlight that "compliance refers to the adherence to laws, regulations, and internal policies, while ethics involves conducting business in a morally responsible manner." They stress that "ethical behavior goes beyond mere compliance, as it involves a deep-rooted commitment to doing what is right, fair, and responsible."

Investor and Stakeholder Demands

ESG Investing: The exponential growth of ESG (Environmental, Social, and Governance) investment is perhaps the strongest empirical evidence of this shift. Investors are actively seeking companies that demonstrate strong ethical governance, responsible social practices, and environmental stewardship.

- **Shareholder Activism:** Investors are increasingly using their power to push for ethical reforms, demanding transparency in supply chains, fair labor practices, and climate action. Non-compliance in these areas can lead to divestment or proxy battles.

- **Consumer Behavior:** Consumers are more informed and ethically conscious. They are willing to boycott companies involved in unethical practices, whether it's data misuse, environmental damage, or human rights abuses. This translates directly into market share and brand value.

[2] https://assets.publishing.service.gov.uk/media/5a800de040f0b62305b88e56/16-113-ethical-business-regulation.pdf
[3] https://hrmars.com/papers_submitted/23542/the-overview-of-the-compliance-management.pdf
[4] https://www.researchgate.net/publication/383747309_Beyond_ComplianceThe_Role_of_Integrity_in_Management_and_Leadership
[5] https://community.trustcloud.ai/docs/grc-launchpad/grc-101/compliance/compliance-vs-ethics-what-is-the-difference-and-why-it-matters/

- **Employee Attraction and Retention:** A strong ethical culture is a key differentiator in the talent market. Employees, particularly the younger generations, seek employers whose values align with their own. Reports often link employee engagement to management's commitment to ethical practices.

- **"Strategic Project Management: Navigating Regulatory Compliance and Stakeholder Expectations for Success" (WSP)[6]:** This article highlights that while official regulators impose penalties, "it is crucial not to underestimate the influence of stakeholders. They can hold protests, block access roads, initiate hearings, and undertake actions that incur costs and disrupt project timelines."

Corporate Practice and Reporting

- **Expanded Compliance Roles:** Many companies are broadening the scope of their compliance functions to include "Ethics & Compliance" or "Integrity & Compliance." This is reflected in job titles, department structures, and the responsibilities assigned to compliance officers.

- **Codes of Conduct and Ethics:** Companies are increasingly developing comprehensive Codes of Conduct that go beyond simply listing legal prohibitions to articulating core values, ethical principles, and expected behaviors. These are often accompanied by robust training programs.

- **ESG Reporting and Due Diligence:** The rise of mandatory and voluntary ESG reporting frameworks (e.g., TCFD, SASB, CSRD) forces companies to collect and disclose non-financial data related to their ethical and social performance. This systematic reporting provides empirical data on a company's commitment to these areas.

- **Third-Party Due Diligence:** Companies are extending their ethical scrutiny to their supply chains and third-party relationships, recognizing that their integrity can be compromised by the unethical actions of partners.

In essence, the empirical evidence points to a growing understanding that simply avoiding legal infractions is insufficient. A truly compliant organization must integrate a strong ethical foundation into its core operations, driven by regulatory expectations, stakeholder pressure, and the recognition that integrity is a fundamental driver of long-term value and resilience.

C.3. Growing regulatory scrutiny and stakeholder expectations

The growing regulatory scrutiny and increasing stakeholder expectations are fundamentally reshaping the compliance function. Compliance is no longer just about avoiding fines; it's a strategic imperative that directly impacts a company's reputation, market value, and ability to attract and retain talent and investors.

Here are the key points and issues to highlight and mention as worthwhile considering for the compliance function:

[6] https://www.wsp.com/en-gl/insights/strategic-project-management-navigating-regulatory-compliance-and-stakeholder-expectations

C.3.1. Heightened regulatory scrutiny and enforcement

1. **Proliferation and Divergence of Regulations**

   - **Global Reach, Local Nuances:** Companies, especially multinational ones, face a complex web of regulations that vary significantly across jurisdictions (e.g., EU's GDPR, US state privacy laws, new AI acts). Staying abreast of these changes and their specific requirements is a monumental task.

   - **Emerging Regulatory Areas:** Rapid legislative development in areas like AI governance (e.g., EU AI Act, US AI Executive Order), digital assets, environmental, social, and governance (ESG), and cybersecurity means continuous monitoring and adaptation are critical.

   - **Increased Enforcement Action:** Regulators globally are becoming more proactive and assertive, with larger fines, stricter penalties, and a greater willingness to pursue legal action for non-compliance. This includes personal liability for senior management in some cases.

2. **Focus on Data Privacy and Cybersecurity**

   - **Ubiquitous Data:** The sheer volume and sensitivity of data collected and processed by businesses make data privacy a top concern. Regulations like GDPR, CCPA, and upcoming privacy laws demand robust data governance frameworks, consent management, and data subject rights fulfillment.

   - **Evolving Cyber Threats:** The increasing sophistication of cyberattacks necessitates a strong alignment between cybersecurity and compliance. Data breaches not only lead to financial penalties but also significant reputational damage and loss of customer trust. Compliance functions must ensure adequate controls are in place to protect sensitive information.

3. **ESG as a Core Compliance Domain**

   - **Mandatory Reporting and Due Diligence:** What was once voluntary "greenwashing" is rapidly becoming mandatory. Regulations like the EU's Corporate Sustainability Reporting Directive (CSRD) and proposed SEC rules are requiring companies to disclose detailed ESG metrics, including Scope 1, 2, and in some cases, Scope 3 emissions, climate-related financial risks, and human rights due diligence in supply chains.

   - **Investor and Public Pressure:** Beyond regulation, investors, consumers, and employees are increasingly demanding demonstrable ESG performance. This scrutiny translates into a need for robust data collection, transparent reporting, and verifiable impact.

   - **Interconnected Risks:** ESG risks are often intertwined (e.g., poor labor practices linked to governance failures or environmental harm). Compliance needs to adopt a holistic approach to identify and mitigate these interconnected risks.

   - **Anti-Greenwashing Focus:** Regulators are cracking down on misleading ESG claims, leading to a need for rigorous data verification and clear communication

C.3.2. Evolving stakeholder expectations

4. **Demands for Transparency and Accountability**

   - **Investors:** Seek reliable, verifiable information on a company's compliance posture, risk management, and ESG performance to inform investment decisions and manage their own risk. They expect clear disclosures and proactive engagement.

- **Customers:** Expect their data to be handled responsibly and ethically. They are increasingly making purchasing decisions based on a company's ethical standing and commitment to social and environmental responsibility.
- **Employees:** A strong compliance culture and ethical conduct are crucial for attracting and retaining top talent. Employees want to work for organizations that align with their values and operate with integrity. Whistleblower protections and internal reporting mechanisms are increasingly important.
- **Public and NGOs:** Are more vocal and organized in demanding corporate accountability for environmental, social, and ethical impacts. Social media amplifies both successes and failures, leading to rapid reputational fallout.

5. **Reputational Risk and Brand Value**

- **Beyond Fines:** While financial penalties are significant, the damage to reputation, brand value, and customer trust resulting from compliance failures can be far more costly and long-lasting.
- **Social License to Operate:** Non-compliance, particularly in areas like data privacy or ESG, can jeopardize a company's "social license to operate," leading to boycotts, protests, and difficulties in market access.

6. Ethical Considerations and Conduct Risk

- **Broader Definition of Compliance:** Compliance is moving beyond strict legal adherence to encompass ethical conduct and responsible corporate citizenship. This includes managing conduct risk related to employee behavior, corporate culture, and decision-making.
- AI Ethics: The ethical implications of AI use (e.g., bias in algorithms, data privacy, accountability for AI-driven decisions) are a major focus for stakeholders and are rapidly becoming a regulatory concern.

D. Defining Compliance: Purpose and Scope today

D.1. What is the purpose and scope of compliance today?

A comprehensive definition of the purpose and scope of compliance for a company could be read as follows:

Purpose of Compliance

The fundamental purpose of compliance for a company is to **ensure that all its operations, activities, and conduct consistently adhere to applicable laws, regulations, industry standards, and internal policies and ethical principles.** This is not merely a legal obligation, but a strategic imperative that aims to:

1. **Mitigate Risks:** Proactively identify, assess, and manage legal, financial, operational, and reputational risks associated with non-compliance. This includes avoiding fines, penalties, lawsuits, sanctions, and business disruptions.
2. **Foster Ethical Conduct and Integrity:** Cultivate a strong ethical culture throughout the organization, promoting transparency, accountability, and responsible behavior among all employees, management, and third-party partners.
3. **Build and Maintain Trust:** Enhance credibility and trust with customers, investors, regulators, employees, and the wider public. This strengthens brand reputation, attracts talent, and can provide a competitive advantage.
4. **Enable Sustainable Growth and Business Continuity:** Ensure the company operates within a stable and legitimate framework, allowing for sustained growth, market access, and resilience against evolving regulatory landscapes and potential misconduct.
5. **Improve Operational Efficiency:** Streamline processes, reduce errors, and optimize resource allocation by establishing clear guidelines and controls, leading to more efficient and secure operations.

Scope of Compliance

The scope of compliance within a company is broad and pervasive, encompassing virtually every aspect of its operations. It can be broadly categorized into:

1. **Regulatory Compliance (External):** Adherence to laws, regulations, and guidelines imposed by external governmental bodies, industry regulators, and international agreements. This varies significantly by industry and jurisdiction but often includes:
   - **Financial Regulations:** Anti-Money Laundering (AML), Anti-Bribery and Corruption (ABC), financial reporting standards (e.g., GAAP, IFRS), tax laws, and sanctions.
   - **Data Protection & Privacy:** GDPR, CCPA, HIPAA, and other data privacy laws governing the collection, processing, storage, and transfer of personal data.
   - **Employment & Labor Laws:** Workplace safety, anti-discrimination, wages, working hours, benefits, and fair labor practices.
   - **Environmental Regulations:** Waste disposal, emissions control, and sustainable practices.
   - **Consumer Protection:** Product safety, advertising standards, and fair-trading practices.

    - **Industry-Specific Regulations:** Unique rules and standards applicable to sectors (e.g., healthcare, financial services, pharmaceuticals).

2. **Corporate/Internal Compliance (Internal):** Adherence to internal rules, policies, and procedures established by the company itself to govern its internal operations and employee conduct. This includes:
    - **Code of Conduct/Ethics:** Guiding principles for employee behavior, conflicts of interest, gifts and hospitality, and ethical decision-making.
    - **Internal Policies & Procedures:** Rules governing internal processes, such as IT security, data handling, financial controls, procurement, and whistleblowing.
    - **Governance Frameworks:** Structures and processes for oversight, risk management, and decision-making within the organization.
    - **Training & Awareness:** Ensuring employees are informed and trained on all relevant compliance obligations and internal policies.
    - **Monitoring & Auditing:** Regular internal checks and audits to assess compliance effectiveness and identify areas for improvement.
    - **Third-Party Due Diligence:** Ensuring that vendors, partners, and other third parties also comply with relevant standards and policies.

Or simply said in one sentence: compliance serves as the guardian of a company's legal standing, ethical integrity, and long-term viability, ensuring that the pursuit of business objectives aligns with responsible and lawful conduct across all fronts.

D.2. Core pillars of modern compliance

The core pillars of Compliance are:

- Compliance risk assessment
- Compliance obligations
- Scope of compliance management system
- Roles & responsibilities

D.2.1. Compliance Risk Assessment

This pillar is the foundational step, identifying and evaluating the potential for non-compliance within an organization. It's about understanding *where* things can go wrong and *how bad* the impact could be.

- **What it involves:**
    - **Identification of Risks:** This includes looking at all relevant laws, regulations, industry standards, internal policies, and contractual obligations. Risks can arise from operational processes (e.g., data handling, financial transactions), new products/services, changes in regulations, or even employee misconduct.
    - **Analysis of Likelihood and Impact:** For each identified risk, assess the probability of it occurring (likelihood) and the **severity of its consequences if it does (impact). Impact can be financial (fines, penalties), reputational (loss of trust, brand damage), operational (disruption of services), or legal (lawsuits, sanctions).**

    - **Risk Prioritization:** Not all risks are equal. Prioritize risks based on their likelihood and impact. High-likelihood, high-impact risks require immediate attention, while low-likelihood, low-impact risks might be monitored.
    - **Examples:**
        - **Financial Institution:** Risk of money laundering due to inadequate customer due diligence processes.
        - **Healthcare Provider:** Risk of HIPAA violation due to improper handling of patient data.
        - **Manufacturing Company:** Risk of environmental pollution due to non-compliance with waste disposal regulations.
- **Making it Concrete:** A tangible output of this process is often a "risk register" – a document listing identified risks, their assessment (likelihood, impact), and initial mitigation strategies. Regular reviews (e.g., annually or when significant changes occur) are crucial.

D.2.2. Compliance Obligations

This pillar focuses on understanding and cataloging the specific rules, laws, and internal policies an organization must adhere to. It's about knowing *what* needs to be done.

- **What it involves:**
    - **Identification of Applicable Laws and Regulations:** This requires a thorough scan of all external rules governing the organization's industry, geographic locations, and operations. This includes national and international laws (e.g., GDPR, SOX, industry-specific regulations like those from financial authorities or health ministries).
    - **Internal Policies and Procedures:** Beyond external laws, organizations also have their own internal rules designed to operationalize compliance and reflect their ethical stance (e.g., code of conduct, anti-bribery policy, data privacy policy).
    - **Contractual Commitments:** Obligations arising from agreements with customers, vendors, and partners (e.g., data protection clauses in service agreements).
    - **Keeping Up to Date:** Regulatory landscapes are constantly evolving. This pillar requires a robust system for monitoring changes in laws and regulations and updating obligations accordingly.
- **Making it Concrete:** A "compliance obligations register" or a similar system (often integrated into GRC software) is a practical tool here. It lists each obligation, its source, a summary of its requirements, and the specific departments or processes it applies to. For instance, a bank might have an obligation to report suspicious transactions, detailing the specific reporting format and deadline.

D.2.3. Scope of compliance management system

This pillar defines the boundaries of the compliance program within the organization. It's about knowing *who* and *what* the compliance efforts cover.

- **What it involves:**
    - **Organizational Scope:** Clearly define which entities, departments, business units, and geographical locations are covered by the CMS. Does it apply to all subsidiaries globally, or only specific regions?

    - **Process/Activity Scope:** Identifying which business processes, functions, and activities are subject to compliance oversight (e.g., sales, marketing, finance, human resources, IT, product development).
    - **Defining Inclusions and Exclusions:** Explicitly stating what is within the scope and, importantly, what might be deliberately excluded (with justification).
    - **Alignment with Business Objectives:** Ensuring the CMS scope is aligned with the organization's strategic goals and risk appetite.
- **Making it Concrete:** This is often documented in a "Compliance Policy" or a "CMS Charter" which outlines the program's objectives, its scope, and high-level principles. For a multinational corporation, the scope might explicitly state that the CMS covers all global operations, with specific local adaptations where required. A small business might define the scope as covering all employees and all customer-facing processes.

D.2.4. Roles and responsibilities

This pillar assigns accountability for compliance tasks and activities throughout the organization. It's about knowing *who does what*.

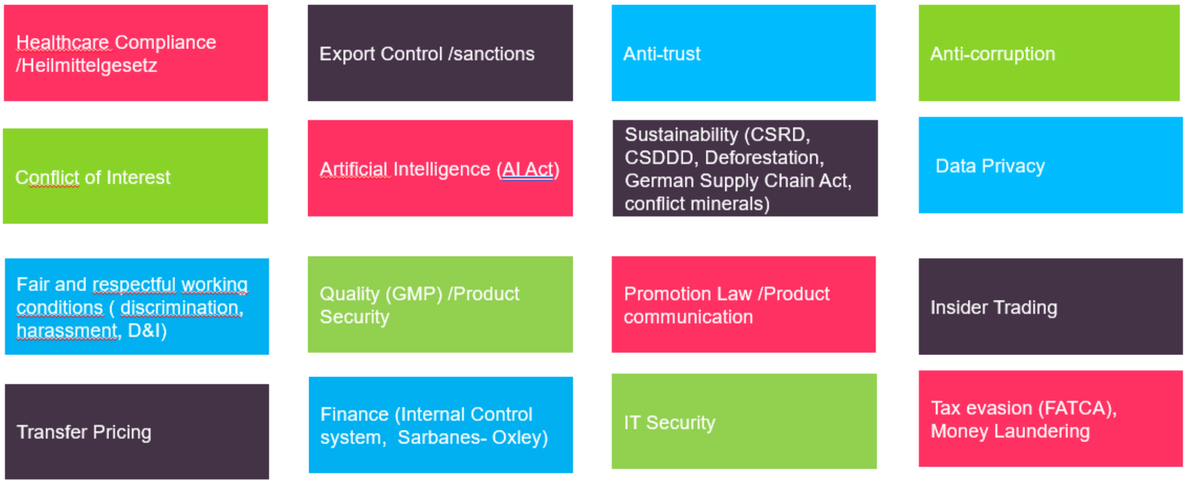
- **What it involves:**
    - **Clear Assignment of Duties:** Defining who is responsible for identifying, assessing, mitigating, and monitoring compliance risks and obligations. This extends from the board of directors down to individual employees.
    - **Leadership and Oversight:** Establishing clear roles for senior management and the board in overseeing the compliance program. This often includes a Chief Compliance Officer (CCO) or similar role.
    - **Operational Roles:** Detailing the responsibilities of various departments and individuals in implementing compliance controls (e.g., HR for employee training, IT for data security, legal for regulatory interpretation).
    - **Reporting Lines:** Establishing clear reporting structures for compliance issues, breaches, and performance.
    - **Training and Awareness:** Ensuring that all employees understand their individual compliance responsibilities and the importance of compliance.
- **Making it Concrete:** This is often outlined in job descriptions, an organizational chart for compliance, and specific policy documents. For example:
    - **Board of Directors:** Ultimate oversight of the compliance program, setting the tone from the top.
    - **Chief Compliance Officer:** Designs, implements, and monitors the overall compliance program.
    - **Department Heads:** Responsible for ensuring compliance within their respective departments and implementing specific controls.
    - **All Employees:** Expected to adhere to the code of conduct and report any suspected non-compliance.
    - **Internal Audit:** Provides independent assurance on the effectiveness of the CMS.

By concretely addressing each of these pillars, organizations can build a robust and effective compliance framework that not only helps avoid penalties but also fosters a culture of integrity and ethical conduct.

D.3. Compliance Function and Compliance Risks

Compliance has evolved enormously in the last 20 years. In its initial days the focus was on “legal compliance” where compliance departments were mostly run by lawyers, and the focus was on preventing (criminal) fines for companies. Much has happened since.

The scope and breadth of compliance departments, depending on industry, have expanded significantly since as can be seen in Figure 1 below.



Healthcare Compliance /Heilmittelgesetz	Export Control /sanctions	Anti-trust	Anti-corruption
Conflict of Interest	Artificial Intelligence (AI Act)	Sustainability (CSRD, CSDDD, Deforestation, German Supply Chain Act, conflict minerals)	Data Privacy
Fair and respectful working conditions (discrimination, harassment, D&I)	Quality (GMP) /Product Security	Promotion Law /Product communication	Insider Trading
Transfer Pricing	Finance (Internal Control system, Sarbanes- Oxley)	IT Security	Tax evasion (FATCA), Money Laundering

Figure 1: scope of Compliance Department

D.4. Distinction between legal advice and ethical guidance

In a compliance context, the distinction between legal advice and ethical guidance is crucial for a company's effective functioning and long-term sustainability. While often intertwined, they operate on different principles and address different facets of corporate conduct.

Here is a possible breakdown of the key distinctions that we could identify:

Legal Advice

- **Focus:** Primarily concerned with what the law *requires* or *prohibits*. It addresses the question: "Is this action legal?" or "What are the legal consequences of this action?"
- **Basis:** Rooted in codified laws, regulations, statutes, judicial precedents, and regulatory guidance issued by government bodies. It's about adherence to external, enforceable rules.
- **Nature:** Objective and prescriptive. It provides clear "do's and don'ts" based on legal interpretation.
- **Source:** Typically provided by qualified legal professionals (in-house counsel, external law firms) who are licensed to practice law. They represent the company's legal interests.
- **Consequences of Non-compliance:** Legal penalties, fines, lawsuits, criminal charges, regulatory sanctions, loss of licenses, and significant reputational damage.
- **Goal:** To ensure the company operates within the bounds of the law, minimizes legal risk, and avoids legal liability. It's the minimum standard of acceptable behavior.

Ethical Guidance

- **Focus:** Concerned with what is *right* or *wrong*, even when no law explicitly dictates it. It addresses the question: "Is this action ethical?" or "Does this align with our company's values and moral principles?"
- **Basis:** Derived from a company's internal code of conduct, values statement, industry best practices, societal norms, and moral principles. It often goes beyond the letter of the law.
- **Nature:** Subjective and aspirational. It encourages a higher standard of behavior and promotes a culture of integrity. It involves judgment and discretion.
- **Source:** Often provided by ethics and compliance officers, senior leadership, HR, or even through peer discussions and training. It's about shaping internal culture and behavior.

- **Consequences of Non-compliance:** Reputational damage, loss of trust from stakeholders (customers, employees, investors), decreased employee morale, reduced productivity, negative media attention, and potential long-term business impact (e.g., boycotts, difficulty attracting talent). While not always direct legal consequences, ethical failures can quickly lead to legal problems if they violate public trust or lead to new regulations.

- **Goal:** To cultivate a strong ethical culture, build trust, enhance reputation, foster a positive work environment, and ensure sustainable business practices that align with broader societal expectations. It's about "doing the right thing" even when not legally compelled.

Interplay and Overlap:

It's important to note that legal advice and ethical guidance are not mutually exclusive and often overlap. Many ethical principles are codified into law (e.g., anti-discrimination, anti-bribery). Conversely, legal compliance often sets the floor for ethical behavior; a company that is only legally compliant but not ethically sound may still face significant challenges.

- **Legal advice** often informs the development of ethical policies (e.g., a data privacy law will lead to a specific data handling policy, which is then reinforced by an ethical commitment to privacy).
- **Ethical guidance** can prompt a company to go beyond mere legal compliance, anticipating future regulatory trends or societal expectations (e.g., adopting sustainable practices before they are legally mandated).

In challenging situations, a decision might be **legally permissible but ethically questionable**. In such cases, ethical guidance helps the company navigate towards a more responsible and sustainable path.

Legal advice ensures a company stays within the boundaries of the law, while ethical guidance helps it define and uphold its values and reputation, striving for a higher standard of conduct that builds long-term trust and resilience. A robust compliance program integrates both, recognizing that true corporate responsibility requires adherence to both the letter and the spirit of the law.

D.5. Role of Compliance in driving ethical values

Compliance plays a pivotal and often underestimated role in driving organizational values. It acts as the **operationalization and reinforcement mechanism for a company's stated principles and ethical commitments.** Instead of being just a burden of rules, effective compliance transforms values from abstract statements into tangible behaviors and practices. Here's how compliance drives organizational values:

1. **Translate Values into Actionable Policies and Procedures:**

    - **From "Integrity" to "Anti-Bribery Policy":** A company might have "integrity" as a core value. Compliance translates this by developing and enforcing a strict anti-bribery and corruption policy, providing clear guidelines on gifts, entertainment, and third-party interactions. This shows employees *how* to embody integrity in their daily work.

    - **From "Respect" to "Anti-Harassment Training":** The value of "respect" is concretized through anti-harassment and diversity policies, along with mandatory training that educates employees on appropriate conduct and reporting mechanisms.

2. **Sets the Tone at the Top and Middle:**

    - **Leadership by Example:** When senior leaders actively champion compliance, not just as a legal necessity but as a reflection of the company's values, it sends a powerful message. Their commitment to adhering to policies and ethical standards encourages the entire organization to follow suit.

    - **Managerial Reinforcement:** Compliance programs empower managers to reinforce values in their teams. They become the "face" of compliance, demonstrating how ethical behavior is expected and rewarded, and how non-compliance has consequences.

3. **Fosters a Culture of Accountability and Responsibility:**

    - **Clear Expectations:** Compliance outlines clear expectations for employee conduct. When individuals understand what is expected of them in terms of values, and that there are consequences for failing to meet those expectations, it drives accountability.

    - **Reporting Mechanisms:** Whistleblower hotlines and clear reporting channels, often overseen by compliance, demonstrate a commitment to transparency and encourage employees to speak up about potential violations without fear of retaliation. This reinforces values like honesty and courage.

4. **Mitigates Risks to Values and Reputation:**

    - **Preventing Ethical Lapses:** By identifying and mitigating risks of misconduct, compliance directly protects the company's values from being compromised. A data breach, for example, not only has legal repercussions but also violates values of trust and privacy.

    - **Protecting Brand Image:** A company's reputation is intrinsically linked to its values. Strong compliance helps prevent incidents that could severely damage this reputation, thereby safeguarding the perceived embodiment of those values by the public and stakeholders.

5. **Promotes Consistent Decision-Making:**

    - **Standardized Behavior:** Compliance frameworks ensure that decisions across different departments and regions are made consistently and in line with the company's values. This prevents situations where different parts of the organization might act in ways that contradict the stated principles.

    - **Ethical Dilemma Resolution:** Compliance training often includes scenarios that help employees navigate ethical dilemmas, guiding them to make decisions that align with both legal requirements and organizational values.

6. **Enhances Employee Engagement and Trust:**

- **Proud to Work There:** Employees are more likely to be engaged and proud to work for a company that clearly articulates and consistently upholds its values through its compliance efforts. They feel secure knowing that their employer operates ethically.

- **Fairness and Equity:** Compliance with labor laws, anti-discrimination policies, and fair treatment principles reinforces values of fairness and equity within the workplace, leading to higher morale and retention.

Compliance acts as the **backbone and nervous system** of organizational values. It provides the structure, processes, and continuous monitoring necessary to ensure that a company's aspirational values are not just words on a wall but living principles that guide everyday actions and contribute to long-term success and trust.

E. Structural Problem: Compliance within Legal Department

Placing the compliance department inside the legal department of a company can create several structural problems and issues due to inherent differences in their primary functions and objectives. We will outline below why this is the case.

E.1. Overview of issues when Compliance is within Legal Department

E.1.1. Inherent conflict of interest

Legal's Role vs. Compliance's Role: The legal department's primary function is to represent and defend the company's interests, often focusing on minimizing legal liability after an issue arises. This can involve providing legal advice that aims to protect the company in litigation or regulatory enforcement actions. In contrast, the compliance department's main objective is to prevent violations of laws, regulations, and internal policies by proactively identifying risks, establishing controls, monitoring adherence, and fostering an ethical culture. When Compliance is part of Legal department then there is a risk that the focus becomes narrowly focused on **lawful vs. unlawful**, potentially overlooking ethical, cultural, or business-practical concerns.

Hiding vs. Disclosing: If compliance reports to legal, there's a risk that legal counsel might use their authority to "hide" or downplay potential violations to protect the company from legal repercussions, rather than fully disclosing and addressing them. Regulators, like US Department of Justice (“DOJ”) and Office of Inspector General (“OIG”), are particularly concerned about this conflict. Whistleblower reports or internal investigations may be **suppressed** or **under-addressed** to avoid legal exposure.

Investigation Bias: If the legal department is involved in or the subject of an investigation, and compliance reports to legal, it creates a perceived (and often real) conflict of interest. The compliance officer might feel pressure to protect the legal department or suppress findings that could be detrimental to them.

E.1.2. Lack of independence and Authority

Perceived Weakness: Regulators often view a compliance function reporting to legal as less effective and lacking true independence. They prefer a structure where the Chief Compliance Officer (CCO) reports directly to the CEO or the Board of Directors/Audit Committee. This signals that compliance is a top priority for the organization, not just a subset of legal concerns.

Limited Empowerment: A compliance officer placed too low in the organizational structure, such as under the General Counsel, may not have the necessary authority or influence to make meaningful changes, implement robust controls, or challenge senior management effectively when compliance issues arise.

Chilling Effect on Reporting: Employees may be less likely to report wrongdoing through compliance channels if they perceive that the information will be filtered or used primarily for legal defense rather than for internal remediation. The "Upjohn Warning" (where legal counsel must inform employees that they represent the company and not the individual) can further chill employees trust in speaking openly.

E.1.3. Different skillset and focus

Proactive vs. Reactive: Compliance is inherently proactive, focusing on building systems, training, and processes to prevent issues. Legal is often reactive, dealing with the consequences of issues that have already occurred.

Business Operations vs. Legal Interpretation: Compliance requires a deep understanding of business operations, risk assessment, data analysis, and building relationships with various departments and regulators. While legal provides essential interpretations of laws, it doesn't typically build the day-to-day compliance tools, processes, controls and relationships that are crucial for an effective compliance program. The legal department typically does not have the skillset to operationalize laws (e.g. GDPR, ESG reporting) and might lack the skills to monitor transactions in large datasets.

Cultural Differences: Legal departments often operate with a focus on privilege and confidentiality, which can hinder the transparency and open communication necessary for a strong compliance culture. Compliance needs to foster an environment where employees feel comfortable raising concerns and engaging in discussions about ethical conduct.

E.1.4. Undermining Compliance culture

"Check-the-Box" Mentality: When compliance is seen as merely an extension of legal, it can foster a "check-the-box" mentality rather than a genuine commitment to ethical behavior and regulatory adherence.

Less Proactive Risk Management: The focus might shift from proactive risk identification and mitigation to simply addressing legal risks as they emerge, potentially missing opportunities to prevent future violations.

E.1.5. Compliance gets deprioritized

Legal teams are often **overloaded** with contracts, litigation, M&A, IP issues. Consequently, Compliance may get less focus, fewer resources, or only “reactive” attention when something goes wrong.

E.1.6. Limited access to senior leadership and the Board

Filtered Information: When compliance reports to legal, the information reaching the CEO and Board of Directors is often filtered through the General Counsel (GC). The GC, whose primary role is legal risk mitigation and defense, might inadvertently or intentionally prioritize certain information, downplay compliance failures, or frame issues in a way that minimizes legal exposure rather than highlighting systemic compliance weaknesses. This can prevent the Board from getting a full and unfiltered picture of the company's compliance risks and the effectiveness of its compliance program.

Lack of Direct Influence: The Chief Compliance Officer (CCO) needs direct and unfettered access to the Board (or a designated committee, like the Audit Committee) to fulfill their oversight responsibilities effectively. This direct line of communication ensures that the Board receives critical compliance insights, emerging risks, and program performance updates directly from the source, without being influenced by other departmental agendas. Without this direct access, the CCO's ability to advocate for necessary resources, policy changes, or cultural shifts is severely diminished.

Regulatory Expectation: Regulators, particularly in highly regulated industries, increasingly expect the CCO to have direct access to the Board. This is viewed as a hallmark of an independent and empowered compliance function. If a company's CCO lacks this access, it can be seen by regulators as a sign of a weak compliance program and a lack of "tone at the top" regarding ethics and compliance. This can lead to increased scrutiny, larger fines, and more severe penalties in the event of a violation.

Undermined "Tone at the Top": The "tone at the top" is crucial for a strong compliance culture. If the Board and senior leadership are not regularly and directly engaging with the CCO, it sends a message throughout the organization that compliance is not a top priority, potentially undermining employee willingness to report concerns or adhering to policies.

E.1.7. Lack of control over budget and resources

Under-resourcing: If compliance is a subset of the legal department, its budget and resources are typically allocated by the General Counsel. The GC might prioritize legal defense and litigation needs over compliance needs, leading to the compliance function being under-resourced. This can manifest as insufficient staff, lack of necessary technology, inadequate training budgets, or limited funding for proactive monitoring and auditing activities.

Limited Autonomy: Without direct control over its budget, the compliance department lacks the autonomy to invest in critical areas, adapt to evolving regulatory landscapes, or implement necessary program enhancements without seeking approval from the legal department, which may have different priorities. This can hinder the compliance program's agility and effectiveness.

Impact on Program Effectiveness: A lack of resources directly impacts the compliance program's effectiveness. For example:

- **Insufficient Training:** Inadequate budget for training means employees may not receive the necessary education on compliance policies and risks, increasing the likelihood of violations.
- **Outdated Technology:** Without funds for modern compliance tools, the department might struggle with manual processes, data analysis, and efficient risk management.
- **Limited Monitoring and Auditing:** Insufficient resources can curtail the ability to conduct robust monitoring, internal investigations, and audits, leading to missed red flags and unresolved issues.

Accountability Challenges: It becomes difficult to hold the compliance function fully accountable for its effectiveness if it doesn't have the independent authority to control the resources necessary to achieve its objectives. The CCO can legitimately argue that their ability to meet compliance goals is constrained by the budget decisions of another department.

E.2. Summary

In summary, while legal counsel provides essential expertise in interpreting laws and regulations, the compliance function requires a degree of independence and a distinct operational focus to be truly effective in preventing misconduct and fostering a strong ethical culture within a company. The best practice, as advocated by many regulatory bodies, is to have a separate, independent compliance function with direct reporting lines to the highest levels of the organization.

Furthermore, an independent compliance function with direct access to the Board and control over its budget is vital for effective risk management and fostering a strong ethical culture. When these elements are compromised by being housed within the legal department, it creates significant vulnerabilities that regulators, employees, and external stakeholders are increasingly scrutinizing.

F.Benefits of an independent Compliance Function

An independent compliance function is a cornerstone of good corporate governance and effective risk management. Its independence ensures that the compliance program operates with integrity, objectivity, and sufficient authority to achieve its objectives.

F.1. Enhanced effectiveness, accountability and trust

- **Objectivity and Impartiality:**

  - Unbiased Assessment: An independent compliance function can objectively assess the company's adherence to laws, regulations, and internal policies without fear of reprisal or pressure from business units or even the legal department. This leads to more accurate risk identification and assessment.

  - Credibility: Its findings and recommendations are more credible to internal stakeholders (management, board, employees) and external parties (regulators, investors, public) because they are perceived as unbiased and not influenced by conflicting interests.

- **Enhanced Authority and Influence:**

  - Direct Reporting Lines: A truly independent compliance function typically reports directly to the CEO or, more commonly and preferably, to a committee of the Board of Directors (e.g., Audit Committee). This direct line ensures that critical compliance issues are escalated to the highest levels of the organization promptly and without filtering.

  - Empowerment: This reporting structure grants the Chief Compliance Officer (CCO) the necessary authority to challenge business practices, enforce policies, and implement corrective actions, even if they are unpopular or impact profitability in the short term.

- **Stronger "Tone at the Top" and Culture of Compliance:**

  - Clear Message: An independent compliance function sends a clear and unambiguous message throughout the organization that compliance is a top priority, supported by the highest levels of leadership.

  - Ethical Environment: It fosters a culture where ethical conduct is valued, employees feel safe to raise concerns without fear of retaliation (e.g., through robust whistleblowing programs), and compliance is seen as everyone's responsibility, not just a legal burden.

- **Proactive Risk Management and Prevention:**

  - Focus on Prevention: Unlike legal, which often focuses on reactive defense, an independent compliance function is inherently proactive. It focuses on identifying potential compliance gaps and risks before they lead to violations, implementing preventative controls, and continuously monitoring for effectiveness.

  - Better Resource Allocation: With control over its own budget and resources, the compliance department can strategically invest in areas that will yield the most effective risk mitigation, such as specialized training, advanced monitoring technology, and robust internal investigations capabilities.

- **Improved Regulatory Relationships and Reduced Penalties:**
  - Demonstrated Commitment: Regulators, such as the Department of Justice (DOJ) in the U.S. or the Financial Conduct Authority (FCA) in the UK, increasingly look for independent compliance functions as a key indicator of a company's genuine commitment to compliance.
  - Mitigation of Penalties: In the event of a violation, a demonstrably independent and effective compliance program can lead to more favorable treatment from regulators, including reduced fines, avoidance of criminal charges, or more lenient settlement terms. This is a significant benefit, as compliance failures can result in massive financial and reputational damage.
  - Trust and Transparency: An independent compliance function can build trust with regulators by providing transparent and honest assessments of the company's compliance posture.
- **Protection of Reputation and Brand Value:**
  - Avoidance of Scandals: By proactively preventing violations and fostering an ethical culture, an independent compliance function helps the company avoid costly scandals, litigation, and reputational damage that can erode public trust and stakeholder confidence.
  - Sustainable Growth: A strong reputation for integrity and compliance is a valuable asset that can attract and retain customers, investors, and talent, contributing to long-term sustainable growth.
- **Clear Accountability:**
  - Defined Roles: When compliance is separate, its responsibilities are clearly defined and distinct from those of legal or business operations. This clear delineation of roles enhances accountability for compliance outcomes.
  - Performance Measurement: It allows for clearer measurement of the compliance program's effectiveness, as its successes and failures are not conflated with those of other departments.

In essence, an independent compliance function is a strategic investment that enables a company to not only meet its regulatory obligations but also to build a resilient, ethical, and trustworthy organization capable of navigating complex business environments.

F.2. Better Alignment with International Standards ("DOJ" /OECD Guidelines and ISO 37301)

Numerous regulators provided guidance that the Head of Compliance must report either directly to the CEO with direct and independent access to the board or to the board directly.

The United States Department of Justice, Criminal Division, Fraud Section (the "Fraud Section") **deferred prosecution agreement** with companies typically contains the following wording "The Company will assign responsibility to one or more senior corporate executives of the Company for the implementation and oversight of the anti-corruption compliance code, policies and procedures. Such corporate officials shall have the authority to report directly to independent monitoring bodies, including internal audit, the Company's Board of Directors, or any appropriate committee of the Board of Directors, and shall have an adequate level of autonomy from management as well as sufficient resources, authority, and support from senior leadership to maintain such autonomy".[7]

[7] https://www.justice.gov/opa/press-release/file/1272151/dl

The International Standard Organization writes in their ISO 37301 standard on compliance management systems[8] that "the governance body and top management shall ensure that the following principles are implemented:

- Direct access of the compliance function to the governing body
- Independence of the compliance function
- Appropriate authority and competence of the compliance function"

The Office of Inspector general (OIG) of the US Department of Health and Human Services stated in their General Compliance Program Guidance[9] that the Compliance Officer must report either directly to the CEO with direct and independent access to the board or to the board directly. The compliance officer should not lead or report to the entity's legal or financial functions and should not provide the entity with legal or financial advice or supervise anyone who does.

Many of the Corporate Integrity Agreements issued by the Office of Inspector general (OIG) of the US Department of Health and Human Services contains the following wording " The Compliance Officer shall be an employee and a member of senior management of company X, shall report directly to the President of company X, and shall not be or be subordinate to the General Counsel or Chief Financial Officer or have any responsibilities that involve acting in any capacity as legal counsel or supervising legal counsel functions for company X.

F.3. Empowerment to challenge internal decisions and challenge concerns

Empowering employees to challenge internal decisions and escalate concerns is a critical aspect of a healthy, ethical, and resilient organization. In practical terms, it involves creating a systematic and cultural environment where employees feel safe, capable, and encouraged to speak up without fear of retaliation.

Here's how this empowerment would look like in practical terms, broken down into various facets:

1. Clear, Accessible Policies and Procedures:

- **Written Guidelines:** The organization would have clear, widely publicized policies outlining *how* employees can challenge decisions and escalate concerns. This includes:
    - **Decision Challenge Process:** A defined process for questioning a decision made by a manager or team, typically starting with direct conversation, then escalating to a higher-level manager, and potentially to a review committee.
    - **Escalation Matrix:** A visual or written guide detailing different types of concerns (e.g., ethical breaches, legal violations, operational inefficiencies, workplace disputes) and the appropriate escalation channels for each. This might include:
        - Immediate manager
        - Manager's manager
        - HR Business Partner
        - Compliance Officer
        - Legal Department
        - Internal Audit
        - Designated ethics hotline (internal or external)
        - Ombudsman (if applicable)

[8] https://www.iso.org/standard/75080.html

[9] https://oig.hhs.gov/documents/compliance-guidance/1135/HHS-OIG-GCPG-2023.pdf

  - **Whistleblower Protection Policy:** A robust policy explicitly stating non-retaliation for good-faith reporting, regardless of the outcome. This policy would explain how employees are protected and what to do if they experience or witness retaliation.

- **Easy Access:** These policies wouldn't be buried in an obscure HR manual. They would be readily available on the company intranet, in employee handbooks, and routinely discussed in training sessions.

2. Multiple, Secure, and Anonymous Reporting Channels:

- **Open-Door Policy (with structure):** While an "open door" is good, it needs structure. Managers are trained to actively listen, acknowledge, and commit to follow-up when concerns are raised directly.

- **Dedicated Ethics Hotline/Portal:** A confidential and, if desired, anonymous hotline or online portal managed by an independent third party or a designated internal compliance function. This is crucial for sensitive issues, especially those involving senior management.

- **Direct Access to Senior Leadership/HR/Compliance:** Employees should know they can bypass their direct manager if the concern involves that manager or if they feel uncomfortable. This means clear contact information for HR, Compliance, or a specific senior leader responsible for ethics.

- **Anonymous Suggestion Boxes (digital or physical):** For less severe but still important feedback or ideas for improvement that employees might hesitate to voice directly.

3. Training and Awareness Programs:

- **Regular Compliance Training:** Not just one-time onboarding, but recurring training that covers:
  - The company's Code of Conduct and values.
  - Specific compliance policies (e.g., anti-bribery, data privacy, workplace conduct).
  - **How to challenge decisions and escalate concerns:** Practical scenarios, role-playing, and clear explanations of the process.
  - **What constitutes a reportable concern:** Helping employees distinguish between minor disagreements and issues that require formal escalation.
  - **The non-retaliation policy:** Emphasizing its importance and the consequences for those who retaliate.

- **Leadership Training:** Managers are specifically trained on:
  - How to *receive* challenges and concerns constructively, without defensiveness.
  - How to investigate and address issues appropriately.
  - When and how to escalate issues themselves.
  - The importance of protecting those who speak up.

4. Visible Leadership Commitment and Role Modeling:

- **"Walk the Talk":** Senior leaders and managers visibly demonstrate that they value feedback, are open to being challenged, and take concerns seriously. This means:
  - Actively soliciting feedback.
  - Publicly acknowledging and acting on concerns raised.
  - Celebrating instances where speaking up led to positive changes (without revealing sensitive details).
  - Ensuring that no one raises a concern in good faith suffers negative career consequences.

- **Communication of Outcomes:** While individual case details remain confidential, the organization communicates general trends and the positive impact of raised concerns (e.g., "Thanks to employee feedback on X process, we've implemented Y improvement that saved Z amount").

5. Culture of Psychological Safety and Open Dialogue:

- **No Fear of Failure/Mistakes (within reason):** Employees feel comfortable proposing new ideas, admitting mistakes, or challenging inefficient processes without fear of severe punishment, as long as it's done constructively and with learning in mind.
- **Encouragement of Constructive Dissent:** Team meetings and discussions are facilitated in a way that encourages diverse perspectives and allows for respectful disagreement, rather than just groupthink.
- **Recognition for Speaking Up:** While not necessarily monetary, employees who proactively identify issues or respectfully challenge decisions are recognized for their contribution to the company's improvement and ethical culture.
- **Fair and Timely Investigation Processes:** When concerns are escalated, they are investigated promptly, impartially, and thoroughly, and the complainant is kept informed (where appropriate and without compromising confidentiality).

6. Feedback Loops and Continuous Improvement:

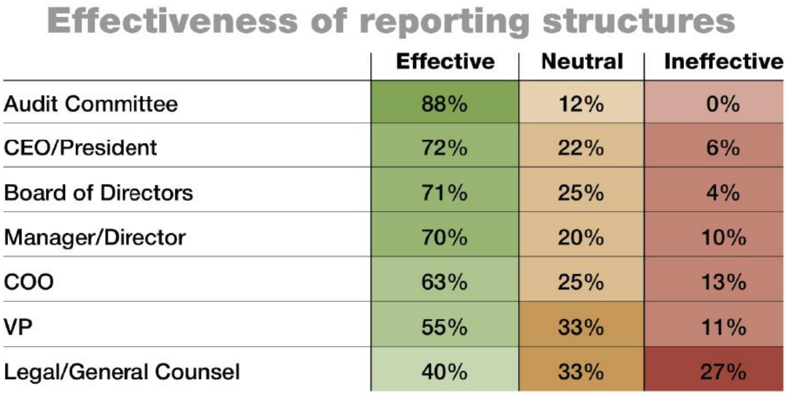
- **Metrics and Analysis:** The compliance function tracks the number and types of concerns raised, how they are resolved, and the time taken for resolution. This data helps identify systemic issues and areas for improvement in the compliance program itself.
- **"Lessons Learned" Culture:** After significant issues or challenges are addressed, the organization conducts a "lessons learned" review to understand root causes and implement preventive measures.
- **Employee Surveys and Pulse Checks:** Regular surveys gauge employee perceptions of psychological safety, confidence in reporting mechanisms, and fairness of processes.

An empowered environment for challenging decisions and escalating concerns isn't just about having a hotline; it's about embedding a deep-seated belief throughout the organization that speaking up is a valuable contribution, a sign of loyalty, and essential for the company's long-term health and success.

F.4. Mental Health: survey among Compliance officers

In the Corporate Compliance Insights 2025 study on “the Compliance Officer Working conditions, stress and mental health”[10] most of the compliance officers were satisfied with their reporting structure. Among the most common reporting structures, CEO/President and Board of Directors are rated as most effective, however Compliance Officers who report to the legal department or General Counsel were the most dissatisfied. A combined 27% of those reporting to the General Counsel rated that structure as ineffective.

[10] https://www.corporatecomplianceinsights.com/2025-mental-health-stress-cci/



Effectiveness of reporting structures

	Effective	Neutral	Ineffective
Audit Committee	88%	12%	0%
CEO/President	72%	22%	6%
Board of Directors	71%	25%	4%
Manager/Director	70%	20%	10%
COO	63%	25%	13%
VP	55%	33%	11%
Legal/General Counsel	40%	33%	27%

Figure 2: Reporting lines of Chief Compliance Officer

F.5. Ethical Premium

In a compliance context, an **ethical premium** refers to the **tangible and intangible benefits, advantages, and enhanced value a company gains by consistently operating at a standard of ethical conduct that surpasses mere legal compliance**.

It's the "extra" reward or positive outcome that accrues to an organization for "doing the right thing" not just because it's legally required, but because it aligns with its values and broader societal expectations.

Here is a possible breakdown of what that could look like in practical terms for companies:

Key Characteristics of an Ethical Premium:

1. **Beyond the Letter of the Law:** It's not about avoiding fines or staying out of jail; it's about proactively implementing practices that reflect high moral standards, even if there isn't a specific regulation mandating them. For example, a company might invest in truly sustainable supply chains or pay living wages globally, even if local laws allow for less.

2. **Reputational Advantage:**

    - **Enhanced Brand Image:** Companies with strong ethical reputations are often seen as more trustworthy and responsible, which can differentiate them in the market.
    - **Increased Customer Loyalty:** Consumers are increasingly willing to support and even pay more for products/services from companies they perceive as ethical. This is sometimes called an "ethical consumption premium."
    - **Reduced Brand Risk:** An ethical approach acts as a buffer against public backlash during times of crisis, as stakeholders are more likely to give the company the benefit of the doubt.

3. **Attraction and Retention of Talent:**

    - **Employer of Choice:** Talented individuals, especially younger generations, are often drawn to organizations with a clear purpose and strong ethical values.
    - **Higher Employee Morale and Productivity:** Employees who believe in their company's ethics are typically more engaged, motivated, and less likely to engage in misconduct. This can lead to lower turnover and higher productivity.

4. **Improved Investor Relations and Access to Capital:**

   - **ESG (Environmental, Social, Governance) Investing:** Many investors now prioritize ESG factors, viewing ethically sound companies as more sustainable and less risky in the long run. An ethical premium can attract this capital.
   - **Long-Term Resilience:** Ethical companies are often better positioned to adapt to evolving societal expectations and regulatory landscapes, leading to more stable and predictable performance.

5. **Stronger Stakeholder Relationships:**

   - **Favorable Regulatory Treatment:** While not a guarantee, regulators may view companies with a strong ethical culture more favorably in the event of minor transgressions or when considering new regulations.
   - **Trust with Partners and Suppliers:** Ethical practices build trust throughout the value chain, leading to stronger, more reliable partnerships.
   - **Positive Community Impact:** Being a good corporate citizen fosters goodwill and support from the communities in which the company operates.

6. **Innovation and Competitive Advantage:**

   - **Forward-Thinking:** An ethical mindset can drive innovation, as companies seek out more responsible and sustainable ways of doing business, potentially creating new market opportunities.
   - **Differentiation:** In crowded markets, a genuine commitment to ethics can be a powerful differentiator that resonates with value-driven consumers and partners.

The ethical premium is the return on investment (ROI) that an organization realizes from embedding ethical principles deeply into its culture and operations, going beyond mere legal ticking of boxes. It's the strategic advantage gained by viewing compliance not as a cost center, but as a driver of long-term value, trust, and sustainable success.

Ethisphere (consulting company) compares the financial performance of the publicly listed most ethical companies with a comparable group of peer companies to calculate the "ethics premium". The Ethics Premium[11] is 7.8% from January 2020 to January 2025, demonstrating a tangible ROI for doing the right thing.

[11] 2025 Ethics Premium - Ethisphere | Good. Smart. Business. Profit.®

G. (Dis)Advantages of various organizational models of Compliance

G.1. Factors impacting the organizational model of Compliance

The scope of a compliance program, the structure of an organization, the risk assessment and the tasks to be done by the compliance department are important considerations when designing the compliance department structure.

The **scope of the compliance department** can differ between industries and companies and can include some of the components below (not exhaustive list)

- AML (anti-money laundering)
- Anti-corruption
- Antitrust
- Conflict of interest
- Conflict Minerals
- Data Privacy
- ESG
- Export Controls & Sanctions
- Failure to prevent fraud
- Failure to prevent tax evasion
- Fair and Respectful working conditions (sexual harassment, mobbing etc.)
- Fraud prevention
- Healthcare laws
- Human rights (German Supply Chain, CSDDD, Uyghur Labor Prevention Act etc.)
- Insider Trading
- IT Security
- Money Laundering
- Pharma Industry Codes
- Promotion Laws
- Sustainability (CSRD, Deforestation, Reach, PFAS)

The **organizational structure** will also affect the compliance organization. Some organizations have headquarters and subsidiaries in a few countries. Other multinational organizations have subsidiaries in all countries and have a regional management structure whereby business units or subsidiaries are managed by EMEA, Asia Pacific and Americas Region. Other organizations have different divisions and each of the divisions have a management structure that manages the divisional operations globally.

The chief compliance officer, regional compliance or divisional compliance officer needs to be close to central Headquarter functions respectively regional or divisional management to support them achieving their strategic objectives in a compliant way.

Compliance resources also tend to be present at those locations where increased compliance risks exist. Countries with high enforcement activities by regulators, countries with high fines for non-compliance, emerging markets with higher risks etc. will warrant local compliance officers.

The compliance organizational model will also be affected by what tasks and activities can best be done central, decentral or a combination of both (see further).

G.2. Central versus Decentral Compliance Team

In a central compliance organizational model, the compliance department is based in Headquarters. The key advantage of being based in Headquarters is that the Compliance department has close vicinity with key stakeholders in headquarters.

This model is not appropriate for medium or large multinational companies with an international footprint. In large multinational organizations with different divisions, numerous business units, different operating models (distributors, sales agents, external sales force) and numerous commercial approaches in countries, compliance staff based at Headquarters tend to lack business understanding of local /regional business approaches and therefore can't manage effectively the related compliance risks.

Compliance risks exist where operations take place hence compliance staff need to be close to the business to advise and manage compliance risks. A central team will also struggle with keeping abreast of all local laws that a company needs to comply with.

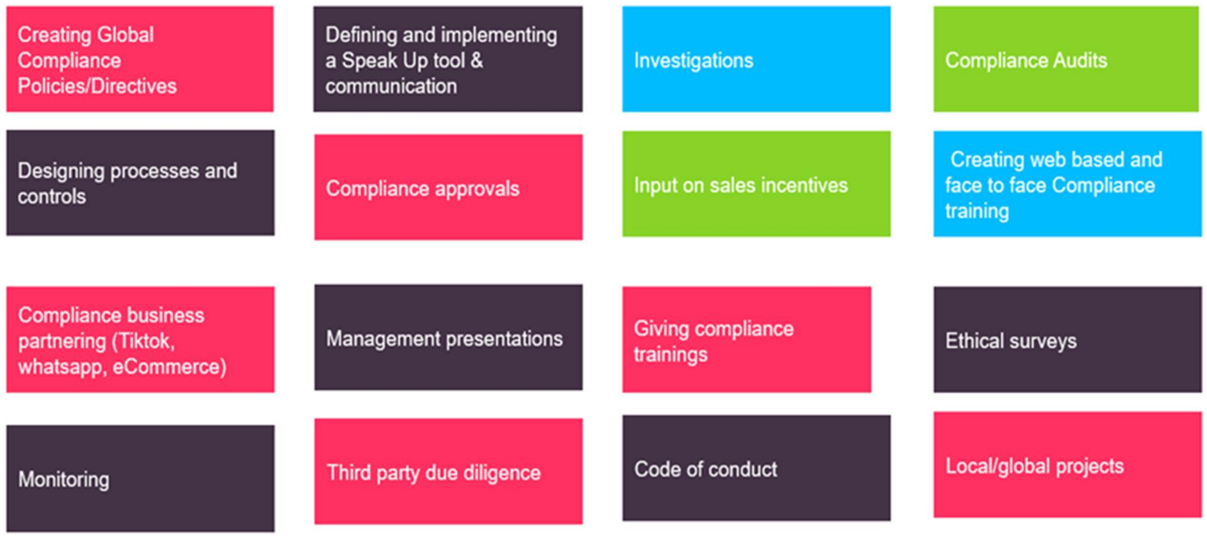
Companies therefore typically have a combined approach where certain key members of the compliance team are based at Headquarters, but other members of the team are based on the respective subsidiaries of the companies.

Different combinations can exist:

- Central team in Headquarters and several regional/divisional compliance officers
- Central team in Headquarters, several regional/divisional compliance officers and compliance officers in all major subsidiaries
- Central team in Headquarters and compliance officers in major subsidiaries (no regional compliance officers)
- Central team in Headquarters, compliance officers in major subsidiaries and "compliance champions "(see further) in other countries.
- Central team in Headquarters, compliance officers in subsidiaries and certain back office "competency centers" or "shared service centers" that conduct certain compliance tasks.

The compliant department must effectively manage compliance risks but at the same time needs to ensure that its compliance resources are used in an efficient way. Therefore, compliance departments should consider which of the compliance tasks and activities are best done central, decentral or a combination of both.

Regardless of industry or company size, most compliance departments must fulfill tasks listed in Figure 3. For some of the activities there might be certain efficiencies of scale doing them at a headquarter level, whereas other tasks e.g. providing training on specific local laws would be best done at a local level. Investigations might be centralized at Headquarters, might be centralized in dedicated "competency centers" within certain Regions or might be handled locally depending on the skillset of the investigators and the number of investigations to be handled.



Creating Global Compliance Policies/Directives

Defining and implementing a Speak Up tool & communication

Investigations

Compliance Audits

Designing processes and controls

Compliance approvals

Input on sales incentives

Creating web based and face to face Compliance training

Compliance business partnering (Tiktok, whatsapp, eCommerce)

Management presentations

Giving compliance trainings

Ethical surveys

Monitoring

Third party due diligence

Code of conduct

Local/global projects

Figure 3: Tasks and activities of Compliance Department

G.3. Divisional/Regional Compliance teams

Multinational companies with several divisions that operate in totally different industries and are impacted by totally different laws and regulations, often have a divisional management structure whereby divisional president is supported by a management team including the divisional head of commercial, divisional head of marketing, divisional head of IT, divisional CFO, divisional head of supply chain, divisional head of Legal and also a divisional head of Compliance.

The divisional head of Compliance has as objective the oversight and effective functioning of the compliance management system within the Division.

There are now two possibilities:

- The divisional head of Compliance has a direct reporting line to the CEO (is part of the business) and has a dotted reporting line to the global Head of Compliance

- The divisional head of Compliance has a direct reporting line to the global Head of compliance with a dotted reporting line to the Divisional President.

<u>Divisional Head of Compliance reporting to Divisional President</u>

Where the Divisional Head of Compliance directly reports to the CEO, the advantage is that the Divisional Head of Compliance is usually part of the leadership team and directly involved in all strategic decisions and projects within the Division. As such the Divisional Head of Compliance has strong connections to the various Divisional leaders, gets closely involved in the Divisional multi-year strategic plan, understands the business well and can proactively give input when major strategic decisions such as M&A deals, expansion into new markets, new business models, new incentive schemes etc. have to be taken by the leadership team.

A disadvantage is that the Divisional Head of Compliance is part of the Divisional leadership team, and his/her performance is closely connected with the Divisional performance. As such conflict of interests could occur between the Divisional Head of Compliance role to minimize compliance risks and the objective (as part of the Divisional Leadership team) to take certain business decisions (and increased compliance risks) to improve Divisional performance.

<u>Divisional Head of Compliance reporting to Global Head of Compliance</u>

Where the Divisional Head of Compliance directly reports to global head of compliance with a dotted reporting line to Divisional President, independence is guaranteed but the Divisional Head of Compliance might not be part of “the inner circle” of Divisional Management, might not be part of all Divisional Management team meetings as hence does not have the possibility to immediately provide input on strategic decisions.

Divisional President and/or his/her Divisional management team might be reluctant to share certain information with the Divisional Head of Compliance, as the Divisional Head of Compliance is often perceived as a representative from Headquarters “checking “Divisional Management.

G.4. Compliance Champions

Some organizations do not have compliance officers in every single subsidiary but rather have appointed people from the business such as country head of Human Resources, Country CFO etc. as compliance “champions” that promote ethical conduct and integrity within local subsidiaries.

Getting buy-in from the business is a useful way to promote ethics and compliance but the appointment of Compliance Champions also comes with certain challenges that can undermine the credibility and effectiveness of the compliance program.

Lack of subject matter expertise

Compliance Champions that do not have a formal compliance background or education might not have a detailed understanding of anti-corruption laws (FCPA, UK Bribery Act), antitrust regulations, data privacy and security laws (GDPR, NIS2), sanctions and export control legislation, insider trading etc. to name a few. As a result, these compliance champions might not be able to provide correct answers to employees requiring guidance on how to behave in certain situations which might lead to non-compliance, fines and reputational risks.

Employees may also not take compliance champions seriously if they lack recognized expertise. Without ongoing training important compliance issues may go unreported or be misunderstood.

Conflict of Interest

Compliance champions that are part of the business have an inherent conflict of interest. Such compliance champions might want to prioritize operational and commercial goals over compliance and cannot take “independent” decisions. There is a risk that Compliance is not lived as strictly as it should be but certain controls or monitoring are downplayed.

Resource constraints

Requesting a local head of Human Resources or local country CFO to be a compliance champion, might help to embed a compliant culture within the business, but if compliance champions have a full-time role then they might not have any time to take on compliance tasks or requests from the business. Compliance responsibilities might further be neglected or treated with low priority if the compliance champion is experiencing a busy project.

G.5. Shared Service Centers

Rather than having compliance officers occasionally doing a certain activity, there are certain economies of scale by building “competency centers” or “shared service centers” for certain tasks. This has the advantage that certain tasks are directed at individuals who are highly specialized and who have more detailed knowledge of a certain task than the average compliance officer. Examples could be a shared service center with dedicated employees that handle specific data privacy topics rather than having data privacy requests from the business handled by data privacy officers in each country.

To reduce compliance costs, shared service centers are often set-up in lower cost locations.

Shared service centers can offer cost and efficiency benefits, but when applied to **compliance functions**, there are **significant disadvantages** that can weaken the compliance framework and alienate business users. Below are the main **disadvantages**, with a compliance-specific lens:

Detachment from business reality

Shared Service Center compliance staff are often far removed—physically and operationally—from the day-to-day business. Hence, they often lack deep business insights to make nuanced compliance decisions.

Lack of Relationship and Trust

Business users often do not know compliance staff at the shared service center personally and might not trust their judgment or responsiveness. As a result, local employees might bypass compliance controls because they don't see compliance shared service staff as credible or helpful. Compliance risks becoming a box-ticking hurdle rather than a trusted partner in decision-making.

Impersonal, Ticket-Based Communication

Compliance shared service centers often work with a ticketing system to handle incoming compliance requests. If there are slow response times and the business believes that shared service centers do not act timely then they will not submit any requests to the shard service centers, potentially leading to non-compliance.

Inflexibility combined with junior staff

Shared service centers often follow a rigid Standard Operating Procedure (SOP) with little room for business judgment and/or exceptions. As a result, unique cases that require a slightly different approach are handled the same as any other compliance request. This is also because (compliance) shared service centers are often staffed by early-career professionals with limited compliance expertise. Standardized transactions can be learned by shared service center employees over time however it is not advisable to have shared service centers handle complex compliance requests.

Loss of Ownership by the Business

If compliance related activities are fully outsourced to shared service centers, then there is the risk that business leaders disengage from compliance assuming the shared service center will handle everything.

Lack of local legal requirements

Centralizing certain activities in a shared service center creates certain efficiencies, however often the centralized team is not aware of local legal requirements and changes in law. The local compliance teams would need to provide input to the shared service centers to update their SOPs.

G.6. Outsourced Compliance Function

Contrary to the assumption that Compliance is another cost center, numerous studies[12] have shown that the return on compliance is positive, i.e. Compliance contributes to business success. Therefore, staffing the Compliance Function makes sense.

Certain compliance-related activities can be outsourced to law firms or consultants, but the following factors should be considered:

- Whether activities or outsourced or not, the company remains responsible that its activities are done in a compliant way. Non-compliance cannot be delegated to the outsourced service provider. Therefore, the activities of the outsourced Compliance provider/consultant must be supervised.

[12] Return on Compliance: Success Factors of Compliance and Their Contribution to Corporate Value | SpringerLink

- If the company does not have many Investigations, then it could consider bringing in specialized resources to deal with these infrequent investigations. However, many core activities of compliance ("company values/integrity", "tone at the top" etc.) can not be delegated to third parties but should be done internally.

The US Department of Justice evaluates whether the compliance management system is effective and whether sufficient resources are provided to Compliance function.

H. Success Factors of Compliance Department

H.1. Empowerment

"Empowerment" is absolutely a crucial success factor for a compliance department, encompassing several key aspects. It's not just about the compliance team itself, but also about how compliance is empowered throughout the entire organization.

Here's a breakdown of what "empowerment" means for a successful compliance department:

1. **Empowerment of the Compliance Department/Chief Compliance Officer (CCO):**

   - **Independence and Authority:** This is paramount. The CCO must have the authority to act, investigate, and enforce compliance policies without undue influence or obstruction from business units or other departments (including legal). This means:
     - **Direct Reporting Line:** As discussed, reporting directly to the CEO or, ideally, an independent committee of the Board (like the Audit or Compliance Committee) signals that compliance is taken seriously at the highest level.
     - **Sufficiency of Resources:** The compliance department needs adequate budget, technology, and qualified personnel to carry out its functions effectively (e.g., training, monitoring, investigations, risk assessments). Empowerment includes having control over these resources rather than being dependent on another department's allocation.
     - **Access to Information:** The compliance department must have unfettered access to all relevant company data, systems, and personnel necessary for monitoring, investigations, and risk assessments.
     - **Right to Escalate:** The CCO must have the explicit right and ability to escalate compliance concerns, including potential violations or insufficient remediation, directly to senior leadership and the Board without fear of retaliation.
   - **Influence and Respect:** Empowerment means the compliance department is not just a "policeman" but a respected strategic partner to the business. This implies:
     - **Involvement in Strategic Decisions:** Compliance should be involved early in new business initiatives, product launches, or market expansions to proactively identify and mitigate compliance risks.
     - **Constructive Engagement:** Business units should view compliance as a helpful resource for navigating complex regulations and making sound ethical decisions, rather than a bureaucratic hurdle.

2. **Empowerment of Employees (Culture of Compliance):**

   - **"Speak Up" Culture:** Empowering employees means creating an environment where they feel comfortable and safe to raise concerns, report potential violations, or seek guidance without fear of retaliation. This includes:
     - **Robust Reporting Channels:** Establishing clear, accessible, and confidential (or anonymous, where appropriate) channels for reporting, such as hotlines or ethics helplines.

    - **Non-Retaliation Policy: A strong, clearly communicated policy against retaliation for good-faith reporting, coupled with visible enforcement of that policy.**
    - **Leadership Support:** Senior leaders must actively champion the "speak up" culture, leading by example and demonstrating their commitment to addressing reported issues.
- **Ownership and Accountability:** Empowering employees also means pushing compliance responsibility out into the business units, making it everyone's job:
    - **Clear Roles and Responsibilities:** Employees at all levels should understand their specific compliance obligations related to their roles and responsibilities.
    - **Targeted Training and Education:** Providing relevant, engaging, and ongoing training that equips employees with the knowledge and tools to comply with policies and identify risks.
    - **Decision-Making Authority (within compliance parameters):** Empowering employees to make day-to-day operational decisions that align with compliance requirements, rather than constantly seeking central compliance approval for every action. This requires trust and proper training.
    - **Accountability:** Holding individuals accountable for compliance performance, including through performance reviews and disciplinary actions for non-compliance.
- **Access to Resources:** Ensuring employees have easy access to compliance policies, procedures, and guidance materials that are clear, concise, and applicable to their roles.

Why is Empowerment a Success Factor?

- **Proactive Risk Mitigation:** Empowered compliance functions can identify and address risks before they become major problems, saving the company from fines, legal battles, and reputational damage.
- **Stronger Ethical Culture:** When compliance is truly empowered, it permeates the entire organization, leading to a stronger ethical foundation and more responsible business practices.
- **Regulatory Confidence:** Regulators view empowered compliance functions as a sign of a genuinely committed organization, which can lead to more favorable outcomes in the event of an issue.
- **Increased Efficiency:** When compliance is integrated and employees are empowered, it can lead to more efficient operations as compliance considerations are "baked in" rather than being afterthoughts.
- **Enhanced Reputation:** A company known for its strong ethical and compliance culture builds trust with customers, investors, and the public, enhancing its brand and market value.

In essence, "empowerment" transforms the compliance department from a reactive "cost center" into a proactive "value driver" that protects the company's assets, reputation, and long-term sustainability.

H.2. Independence

"Independence" is arguably the single most critical success factor for a compliance department. It underpins many of the other factors we've discussed, such as empowerment and objectivity. Without genuine independence, a compliance program is highly susceptible to compromise, rendering it less effective and potentially damaging to the company's integrity and standing with regulators.

Here's a detailed look at what "independence" means for a successful compliance department:

1. **Organizational Structure and Reporting Lines:**

   - **Direct Access to the Board/Audit Committee:** This is the gold standard for independence. The Chief Compliance Officer (CCO) should have a direct, unfiltered reporting line to an independent committee of the Board of Directors (e.g., Audit Committee, Compliance Committee). This ensures that the Board receives critical compliance information, concerns, and program updates directly, bypassing any potential filtering by management.

   - **Direct Access to Senior Leadership (CEO):** While Board access is primary, direct access to the CEO is also crucial. It signifies "tone at the top" and allows the CCO to directly influence strategic decisions and resource allocation concerning compliance.

   - **Separation from Legal Department:** As discussed in previous answers, housing compliance within legal creates inherent conflicts of interest and compromises independence. Regulators view this separation as vital for a truly effective compliance function. The compliance department focuses on prevention and proactive risk management, while legal focuses on reactive defense.

2. **Freedom from Undue Influence:**

   - **Protection from Business Pressure:** The CCO and compliance team must be free to make decisions, conduct investigations, and implement policies without pressure from business units to prioritize profit over compliance, or to overlook potential violations.

   - **No Conflicts of Interest:** The CCO should not hold other roles within the company that could create conflicts of interest (e.g., also serving as the General Counsel, or having direct revenue-generating responsibilities). This ensures their focus remains solely on compliance.

   - **Ability to Challenge:** Independence empowers the CCO to challenge decisions made by senior management or the Board if those decisions pose significant compliance risks or violate company policies.

3. **Control Over Resources and Budget:**

   - **Independent Budget Authority:** The compliance department should have its own dedicated budget, controlled by the CCO, rather than relying on allocations from another department (like legal or operations). This financial autonomy allows the CCO to invest in necessary technology, staffing, training, and external expertise without seeking approval from those who might have conflicting priorities.

   - **Adequate Staffing and Expertise:** Independence means the CCO has the authority to hire and manage a team with the necessary skills and experience to effectively implement and oversee the compliance program.

4. **Autonomy in Investigations and Corrective Actions:**

   - **Unfettered Investigation Powers:** The compliance department must have the authority and access to information (including systems, data, and personnel) to conduct thorough and impartial internal investigations into potential misconduct, regardless of who might be involved.

   - **Ability to Recommend and Enforce Remediation:** Independence allows the compliance department to recommend and push for necessary corrective actions, policy changes, and disciplinary measures, even when these are difficult or impact senior personnel.

5. **Perception of Independence:**

- **Internal and External Credibility:** Not only must the compliance function *be* independent, but it must also *be perceived* as independent by employees, management, the Board, regulators, investors, and the public. This perception is crucial for building trust, encouraging reporting, and demonstrating genuine commitment to ethical conduct.

- **"Tone at the Top":** The Board and senior leadership must visibly and consistently support the independence of the compliance function, demonstrating through their actions that the CCO has their full backing.

Why is Independence a Core Success Factor?

- **Foundation of Trust:** Independence builds trust – internally, it encourages employees to speak up; externally, it signals to regulators and the public that the company is serious about integrity.

- **Effective Risk Mitigation:** An independent compliance function is better positioned to identify, assess, and mitigate risks objectively, without internal pressures that might lead to underreporting or suppression of issues.

- **Regulatory Expectation:** Key regulatory bodies (like the DOJ, SEC, FCA, etc.) consistently emphasize independence as a critical component of an effective compliance program. Its absence can lead to more severe penalties during enforcement actions.

- **Promotes Accountability:** When compliance is independent, it can hold individuals and business units accountable for their actions, fostering a culture where compliance is truly valued.

- **Safeguards Reputation:** By ensuring integrity and proactively addressing issues, an independent compliance function acts as a critical safeguard against reputational damage stemming from misconduct.

In essence, independence empowers the compliance function to be the organization's ethical compass and early warning system, protecting its long-term viability and integrity.

Levels of **independence i**nclude

- Reporting Line
- Unfiltered Board access
- Employment agreement
- Prior Board approval to any changes in CCO employment terms
- Independent budget
- Adequate staff to properly manage the overall Compliance Program

H.3. Seat at the Table

Having a "seat at the table" and "access to the Board of Directors" are critical success factors for a compliance department, so much so that they are often considered synonymous with the "independence" and "empowerment" we've already discussed. However, they warrant specific attention because they represent the *tangible manifestation* of that independence and empowerment at the highest levels of the organization.

Here's a breakdown of why this access is so vital:

1. **Unfiltered Information Flow to the Top:**

   - **Direct Reporting:** The primary benefit is that the Chief Compliance Officer (CCO) can communicate directly and regularly with the Board (or a dedicated committee like the Audit or Compliance Committee) without information being filtered, delayed, or diluted by other senior executives (e.g., the General Counsel, CFO, or CEO, if they have conflicting interests).

   - **Comprehensive Risk Picture:** This direct access ensures the Board receives a complete, unvarnished picture of the company's compliance risks, the effectiveness of its compliance program, significant compliance incidents, and any internal resistance to compliance initiatives. This is crucial for the Board to fulfill its oversight duties.

2. **Strategic Alignment and Resource Allocation:**

   - **Influence on Strategic Decisions:** A CCO with a seat at the table can provide valuable input on compliance risks related to new business ventures, market expansions, mergers and acquisitions, or new product development *before* decisions are finalized. This proactive input allows the company to integrate compliance into its strategy from the outset, rather than trying to retrofit it later.

   - **Advocacy for Resources:** Direct access allows the CCO to directly advocate for the necessary budget, technology, and personnel resources to run an effective compliance program. They can explain the "why" behind these needs directly to those who control the purse strings, demonstrating the return on investment (e.g., risk mitigation, reduced fines).

3. **Demonstrating "Tone at the Top" and Culture of Compliance:**

   - **Visible Commitment:** When the Board actively engages with the CCO, it sends an unmistakable message throughout the entire organization that compliance is a top priority, not just a formality. This "tone at the top" is crucial for fostering an ethical culture where employees feel supported in doing the right thing.
   - **Building Trust:** Employees are more likely to report concerns through official channels if they perceive that compliance has the ear of senior leadership and that their concerns will be taken seriously and acted upon.

4. **Enhanced Regulatory Credibility and Mitigation of Penalties:**

   - **Regulatory Expectation:** Globally, leading regulatory bodies (like the US Department of Justice, the UK's Financial Conduct Authority, and others) explicitly look for and expect CCOs to have direct, regular, and unfettered access to the Board. This is considered a fundamental characteristic of an effective and mature compliance program.

   - **Evidence of Due Diligence:** In the event of a compliance failure, a company can demonstrate to regulators that its Board was actively engaged in oversight of the compliance program, received direct updates, and supported the CCO. This can significantly mitigate potential penalties. It shows the Board exercised its fiduciary duties regarding risk oversight.

5. **Effective Crisis Management:**

   - **Timely Information during Crises:** In a crisis (e.g., a major violation, regulatory investigation), the Board needs immediate, accurate, and direct information from the compliance function to make informed decisions about remediation, public statements, and legal strategy. A CCO with direct access can provide this swiftly.

What Does "Seat at the Table" Practically Mean?

- **Regular Meetings:** The CCO should have regularly scheduled meetings with the Board or relevant committee (e.g., quarterly).

- **Executive Sessions:** The CCO should have the opportunity to meet with the Board or committee in an executive session (without other members of management present) to discuss sensitive issues freely.

- **Presentation of Reports:** The CCO should regularly present formal reports to the Board on compliance risks, program effectiveness metrics, significant incidents, and remediation efforts.

- **Active Participation:** The CCO isn't just an attendee but an active participant in discussions related to risk, governance, and strategy.

In conclusion, a "seat at the table" and "access to the Board of Directors" are not merely symbolic gestures; they are fundamental operational requirements for an effective, empowered, and truly independent compliance department. They ensure that compliance insights are directly factored into strategic decisions and that the highest level of governance is fully informed and engaged in overseeing the company's ethical and regulatory adherence.

H.4. Unrestricted access to information and line of sight

Having "unrestricted access to information and line of sight" is another absolutely critical success factor for a compliance department. It's the operational fuel that enables the compliance function to perform its duties effectively, identify risks, investigate issues, and measure program effectiveness. Without it, even the most independent and empowered CCO would be operating blind.

Here's a breakdown of what this factor entails:

1. **Access to Data and Systems**

    - **Comprehensive Data Access:** The compliance department must have access to all data relevant to its mandate, regardless of where it resides within the company's systems. This includes, but is not limited to:

        - Financial transactions and accounting records.
        - Employee data (HR records, background checks, training completion).
        - Communications (email, messaging platforms, call logs – with appropriate privacy considerations).
        - Customer information and onboarding records.
        - Third-party vendor data (due diligence, contracts, payment records).
        - Operational data relevant to specific regulatory requirements (e.g., trading data in finance, patient records in healthcare, production logs in manufacturing).

    - **System Permissions:** This translates to having the necessary permissions and technical capabilities to pull, analyze, and interpret data from various IT systems (ERP systems, CRM, HRIS, communication platforms, specialized operational software, etc.).

    - **Audit Trails:** The ability to review audit trails and system logs to track actions, changes, and access is crucial for investigations and monitoring.

2. **Access to Personnel (Line of Sight to People)**

    - **Interviewing and Gathering Information:** The compliance team must have the authority to interview any employee at any level of the organization, including senior management, without undue restrictions or the requirement for legal counsel to be present unless legally necessary or specifically requested by the interviewee (and even then, this shouldn't be an automatic blanket requirement that impedes investigations).

- **Obtaining Documentation:** This includes the right to request and receive any documents, files, or records held by employees that are relevant to a compliance inquiry or investigation.
- **"Ground Level" Perspective:** Direct access to individuals on the front lines provides invaluable "line of sight" into how policies are implemented in practice, what challenges employees face, and where potential workarounds or risks might exist that aren't apparent from data alone.

3. **Visibility into Business Operations and Processes (Line of Sight to Processes)**

- **Understanding Workflows:** The compliance department needs to understand the day-to-day operations and workflows of every relevant business unit. This involves:
  - Participating in business process mapping.
  - Reviewing standard operating procedures (SOPs).
  - Attending key operational meetings.
  - Being consulted on new product development or service offerings.
- **Identifying Control Gaps:** This "line of sight" allows compliance to identify where controls might be weak, where compliance risks are concentrated, and how misconduct might occur within specific business processes.
- **Real-time Awareness:** It means being embedded enough to have a pulse on what's happening across the organization, rather than discovering issues only after they've become major problems.

4. **Access to Physical Locations**

- **On-site Reviews and Audits:** For certain industries or types of risks, compliance may need the ability to conduct physical inspections, site visits, or walk-throughs to verify adherence to policies or assess operational controls.

Why is Unrestricted Access and Line of Sight a Success Factor?

- **Effective Risk Identification:** You can't mitigate what you can't see. Without broad access, compliance risks will remain hidden, leading to potential blind spots that can result in significant violations.
- **Thorough Investigations:** Limited access cripples the ability to conduct complete and credible internal investigations. If the compliance team can't access all relevant evidence or interview key personnel, their findings will be incomplete, and remediation efforts may fail to address root causes.
- **Proactive Monitoring and Auditing:** Effective monitoring relies on the ability to collect and analyze vast amounts of data. Without unrestricted access, these crucial preventative activities are severely limited.
- **Accurate Compliance Assessments:** To assess the overall health and effectiveness of the compliance program, the compliance department needs a holistic view of the company's activities.
- **Credibility with Regulators:** Regulators expect the compliance function to have the tools and authority to monitor and enforce compliance throughout the organization. Demonstrating this broad access signals a robust and serious commitment. If a company can't show that its compliance team has real "eyes and ears" everywhere, regulators will be skeptical of the program's effectiveness.

- **Enabling Empowerment and Independence:** While "independence" grants the *authority* to access, "unrestricted access" provides the *means* to do so. They are two sides of the same coin: independence ensures the right, and access ensures the capability.

In essence, unrestricted access to information and line of sight are the vital sensory organs of the compliance department. They allow it to observe, detect, understand, and respond to the complex web of risks and activities within the organization, making it truly effective at fulfilling its protective and preventive mandate.

H.5. Adequate Resources

Without adequate resources, even the most independent and empowered compliance department with theoretically unrestricted access will struggle to be effective. It's like having a top-tier fire department (independent, empowered) with full access to a building (unrestricted access) but no water hoses, ladders, or sufficient personnel (inadequate resources).

Here's what "adequate resources" means for a successful compliance department:

1. **Sufficient and Qualified Personnel**

- **Right Headcount:** The compliance department needs enough staff to cover the breadth and depth of the organization's compliance risks. This isn't just about raw numbers but ensuring that the staffing levels are proportionate to the company's size, complexity, geographic spread, and regulatory environment.

- **Diverse Skillsets:** Beyond general compliance knowledge, staff need specialized skills. This could include:
  - **Legal Expertise:** Understanding specific regulations.
  - **Data Analytics:** To monitor transactions, identify anomalies, and conduct investigations.
  - **Technology/IT:** To understand systems, manage compliance software, and oversee data security.
  - **Forensic Accounting/Auditing:** For financial fraud and misconduct investigations.
  - **Training & Communications:** To effectively disseminate policies and build a compliance culture.
  - **Industry-Specific Knowledge:** Deep understanding of the business operations and unique risks of the company's sector.

- **Experience Level:** A mix of junior, mid-level, and senior professionals is vital, with sufficient experienced leaders to guide strategy and complex investigations.

2. **Appropriate Technology and Tools**

- **Compliance Management Software:** Systems for policy management, risk assessments, control frameworks, incident management, case tracking, and reporting.

- **Data Analytics & Monitoring Tools:** Software that can ingest, analyze, and visualize data from various sources to detect patterns, anomalies, and potential violations (e.g., transaction monitoring for AML, communication surveillance).

- **Third-Party Due Diligence Platforms:** Tools to vet vendors, agents, distributors, and other third parties for corruption, sanctions, or reputational risks.

- **Whistleblower Hotlines/Case Management Systems:** Secure and confidential platforms for receiving and managing reports of misconduct.

- **E-discovery and Forensic Tools:** For investigations, to collect and analyze digital evidence.
- **Learning Management Systems (LMS):** For delivering and tracking compliance training.

3. **Sufficient Budget**

- **Operating Expenses:** Covering salaries, training, software licenses, data subscriptions, travel for site visits, and general administrative costs.
- **External Expertise:** Budget for engaging external legal counsel for specialized advice, forensic accountants, independent auditors, or consultants for program reviews and remediation efforts.
- **Training Programs:** Adequate funds for developing and delivering comprehensive, engaging, and tailored training programs to all relevant employees.
- **Technology Upgrades:** Budget for continually updating and investing in new compliance technologies to keep pace with evolving risks and regulatory expectations.

4. **Time and Bandwidth**

- **Capacity for Proactive Work:** Beyond reacting to incidents, the compliance team needs the time and bandwidth to dedicate to proactive activities like risk assessments, policy development, control testing, continuous monitoring, and relationship building with business units.
- **Strategic Planning:** The CCO and senior compliance staff need time to engage in strategic planning, anticipate future regulatory changes, and evolve the compliance program accordingly.

Why is Adequate Resources a Critical Success Factor?

- **Operational Effectiveness:** Without sufficient resources, even the best-designed compliance program will remain theoretical. Staff will be overwhelmed, technology will be outdated, and critical tasks like monitoring, investigations, and training will be inadequately performed.
- **Credibility:** An under-resourced compliance department sends a message that the company isn't truly committed to compliance, which can be noted by employees, regulators, and external stakeholders.
- **Risk Blind Spots:** Inadequate resources can lead to critical risk areas being unaddressed, controls not being tested, and potential violations going undetected until it's too late.
- **Increased Workload and Burnout:** Overworked compliance teams are prone to mistakes, and high turnover due to burnout can further weaken the function.
- **Inability to Adapt:** Without resources to invest in new technology or specialized training, the compliance department will struggle to adapt to new regulatory requirements, emerging risks (e.g., AI ethics, ESG compliance), or changes in the business environment.
- **Regulatory Scrutiny and Penalties:** Regulators actively assess whether a company has adequately resourced its compliance function. An under-resourced compliance department is a red flag and can lead to harsher penalties in the event of a violation. The US DOJ's "Evaluation of Corporate Compliance Programs" guidance explicitly asks whether the compliance program has "adequate resources to effectively discharge its responsibilities."

In essence, adequate resources are the practical engine that powers an effective compliance department. They translate the abstract concepts of independence and empowerment into tangible capabilities, allowing the department to fulfill its vital role in protecting the company's integrity and value.

H.6. Other Considerations

Whilst the above mentioned five factors are the success pillars of any organization, to make a compliance program truly robust and sustainable, there are a few other highly relevant factors that complement these core pillars:

1. **Clear Scope and Mandate**

   - **Defined Responsibilities:** The compliance department needs a clearly articulated scope of responsibilities and a well-defined mandate. What risks are they primarily responsible for overseeing? What are the boundaries of their authority? This prevents overlap with other functions (like Legal or Internal Audit) and ensures all critical areas are covered.

   - **Written Policies and Procedures:** A successful compliance department develops, implements, and maintains comprehensive, clear, and user-friendly policies and procedures that translate regulatory requirements into practical guidance for employees. These must be regularly updated.

2. **Skilled and Knowledgeable Team (Beyond just "Adequate Resources")**

   - While "adequate resources" covers having *enough* people, this factor emphasizes the *quality* and *continuous development* of those people.

   - **Continuous Professional Development:** The regulatory landscape is constantly evolving. A successful compliance team invests in ongoing training, certifications, and knowledge-sharing to stay abreast of new laws, technologies, and best practices.

   - **Analytical and Problem-Solving Skills:** Beyond knowing the rules, the team needs strong analytical skills to identify root causes of issues, assess complex risks, and develop effective solutions.

3. **Integration with Business Operations ("Embeddedness")**

   - **Partnership Approach:** The compliance department shouldn't be seen as an isolated police force but as a business partner. This means working collaboratively with business units to embed compliance into day-to-day operations and decision-making, rather than being an afterthought.

   - **"Compliance by Design":** Ideally, compliance considerations are built into processes, systems, and new initiatives from the outset, rather than being bolted on later. This requires close collaboration and understanding of business needs.

   - **Regular Communication and Training:** Ongoing, tailored communication and training ensure that compliance knowledge is effectively transferred to the business lines.

4. **Effective Monitoring, Auditing, and Testing**

   - **Proactive Surveillance:** A successful compliance department doesn't just react to issues but actively monitors transactions, communications, and activities to detect potential red flags early.

   - **Regular Audits and Testing:** Beyond monitoring, periodic independent audits and systematic testing of controls are essential to verify that policies are being followed and that controls are effective.

   - **Data-Driven Insights:** Leveraging data analytics to move beyond anecdotal evidence and provide measurable insights into compliance performance and risk exposure.

5. **Robust Investigation and Remediation Processes**

- **Fair and Thorough Investigations:** A successful compliance department has well-defined, transparent, and fair processes for conducting internal investigations into alleged misconduct. Investigations must be thorough, objective, and timely.

- **Effective Remediation:** Beyond identifying problems, the department must ensure that appropriate and timely corrective actions are taken, including disciplinary measures, process improvements, and policy updates, to prevent recurrence. This closes the loop.

6. **Culture of Continuous Improvement**

- **Regular Program Assessment:** The compliance program should not be static. It needs to be regularly assessed against internal metrics, regulatory expectations, and industry best practices.

- **Learning from Mistakes:** A successful compliance department has mechanisms to learn from identified issues, near misses, and regulatory changes, using these insights to continuously enhance the program.

- **Adaptability:** The ability to adapt quickly to changes in the regulatory landscape, business environment, and emerging risks.

While the first set of five are the absolute non-negotiables, incorporating these additional factors transforms a merely compliant function into a truly excellent, value-adding, and resilient compliance department.

I. How Management and the Board weakens the effectiveness of Compliance Programs

I.1. Limiting the budget of the Compliance department

Depending on the scope of the compliance program, size and geographical footprint of the company, sufficient compliance resources should be available to instill a culture of integrity and prevent, detect and investigate misconduct. Management and the Board might hamper the effectiveness of the compliance program by limiting the budget of the compliance department. As a result:

- Experienced compliance professionals can't be recruited
- Not enough compliance staff is available to do the required compliance tasks
- The lack of sufficient budget for efficient and automated compliance tools and platforms (e.g. data analytics, monitoring, third party due diligence) will result in many tasks been conducted and completed manually
- (Regional /Divisional) compliance officers do not have sufficient travel budgets to regularly visit subsidiaries, speak at town halls, or attend Management meetings
- Compliance staff do not have sufficient time or budget to attend seminars or training events to keep their compliance knowledge up to date.

I.2. Not having a seat at the table

Towards Management it is important that there is a clear message from the Board that "Compliance Matters". By not inviting the (divisional/regional or chief compliance) officer to important strategy, budget or operational meetings or by not allowing the compliance officer to be part of leadership teams, not only can the (divisional/regional or chief) compliance officer not react timely on potentially risky business operations or decisions but also a perception might be created that "compliance is not a priority". Some of those examples are listed below:

- Compliance function is not involved in Mergers & Acquisition deals or large projects
- Compliance due diligence is not conducted at all when making major acquisitions or large projects
- The country compliance officer is not participating in country leadership team meetings
- The regional and/or divisional compliance officers are not part of regional/divisional leadership teams, team meetings or cross functional committees (e.g. go to market committee, digital excellence committee etc.);
- The heads of finance, HR, legal and business unit heads discuss the quarterly results or present the next 5-year strategy to the Board without the chief compliance officer present
- The chief compliance officer is not part of crisis management meetings

- The company (or company division) organizes an event with its top 100 executives, but the chief compliance officer is not invited or is not prominently on the agenda as a key speaker

- As a result, important information is withheld from the chief compliance officer or regional /divisional compliance officers

Not being involved in crucial meetings or information not only complicates the effectiveness of the compliance function, but it can also cause frustration.

I.3. Management philosophy on governance, risk and compliance

In today's volatile and complex world with a vast array of ever-changing laws and regulations, the average employee cannot be expected to know all these laws, directives and company policies. To prevent non-compliance, especially for high-risk transactions typically, the Compliance department has requested that such transactions be reviewed and approved by them so that they can help the business realize their strategic goals in a compliant way.

Some managers, especially those who see the compliance function as a complicated factor to do business, are in favor of increased autonomy and risk tolerance by business functions and do not like certain transactions or projects that need to be approved by the Compliance department. Therefore, they have suggested another approach to governance that weakens the Compliance function and increases compliance risks. Here are some examples:

- The elimination of managerial approvals (e.g. the elimination of managerial approval for the travel expense reports elimination of managerial approval on supplier invoices to an amount of 1,000€);

- Need to create purchase orders and obtain competitive bidding for any spend over 250,000 € is replaced by a single bid from a supplier to an amount of 1 million €;

- The replacement of a mandatory compliance approval to a system of "compliance on demand". Compliance is only contacted when needed, and business decisions (including the evaluation of compliance risks) are taken by commercial functions

- The replacement of a mandatory compliance approval to a system whereby the business asks compliance for advice, considers it but potentially overrides the compliance department decision

- In branch offices or smaller subsidiaries Management argues that not the same governance aspects and controls are needed as the rest of the company. Not surprisingly during audits at these branch offices and smaller subsidiaries later major deficiencies, frauds, conflicts of interest, single bank signatories etc. are found

- Company policies, directives and/or standard operating procedures are eliminated by Management with the motivation that the elimination of these bureaucratic policies will increase innovation, speed up the go to market, and allow for better decision making. What the proponents of this Management philosophy do not understand is that numerous guidance document such as ISO 37301 standard on "compliance management system", UK Bribery Act, the US Department of Justice "evaluation of a corporate compliance program" all contain minimum standards on compliance that companies should abide by. By eliminating policies, controls and governance, these Managers do not care or do not understand that they are not meeting the expectations of regulators

- The decision by the Board or Management to substantially reduce the number of internal audit personnel and audits carried out.

I.4. Cultural Failures

For a compliance management system to be effective there must be the “tone of top” by the Board and Senior Management clearly articulating the behavior(s) that are expected and what kind of behaviors that are not tolerated.

To reinforce the compliance management system, any allegations of violations must be investigated and confirmed allegations must be sanctioned to reinforce the company’s values, policies and compliance standards. Management and the Board are hampering the effectiveness of Compliance Management System by:

- Not serving as a role model themselves and lead by example
- Not sanctioning managers or executives for confirmed compliance violations
- Trying to downplay the sanctions that would normally be given to an employee /manager for similar conduct (by arguing that for instance there are too many Company Policies and Directives and therefore it cannot be expected that employees know all of these in great detail)
- Not considering Compliance and Integrity as a part of employee performance (promotion, bonus etc.)
- Excluding the Compliance department /Chief Compliance officer when changes are being made to company culture, performance criteria, incentive plans etc.
- Not creating a speak-up culture, but creating a culture where employees do not speak-up fearing retaliation
- Allowing toxic cultures where fair and respectful working conditions (no mobbing, no harassment) are not followed
- Not showing “tone from the top” by not attending mandatory compliance trainings, not taking compliance trainings and not following up with direct reports that compliance trainings were taken, not proactively promoting the importance of ethics and integrity in leadership videos.
- Management /Board members making derogatory remarks about compliance in townhalls.
- Management and the Board having each different and not aligned expectations on the role of compliance, e.g. Management is expecting Compliance to be a business partner/advisor whereas the Board expects Compliance to be a “policeman” giving assurance.

Granted, when Management ignores the advice of the Compliance Officer, this can be frustrating. The bigger problem arises when, as a result, the credibility of the compliance program is undermined by management decisions that are at odds with the compliance program.

I.5. Failures in the design of a Compliance Management System

Below are some failures in the design of a Compliance Management System.

Reporting Line

- Global Head of Compliance is reporting to the Chief Compliance Officer who is the General Counsel. General Counsel is reporting to the Board on Compliance matters without the Head of Compliance attending such Board meetings.

- General Counsel (=Chief Compliance Officer) who is also combining the role of Head of Compliance but does not have time to properly execute both functions.

- Chief Compliance officer is not appointed by a Board Circular (i.e. the whole Board approves the appointment and dismissal of CCO).

- Allowing compliance activities to be conducted by other departments that are not reporting to the Compliance department (e.g. having Procurement compliance staff, sustainability compliance staff etc.).

Other Design failures

- Limiting the scope of compliance program (e.g. anticorruption or antitrust only) where key other compliance risks (supply chain due diligence, cybersecurity, AI) are not managed at all

- The US Department of Justice states in its latest Guidance document that compliance departments should use data in their decisions to evaluate the effectiveness of a compliance management system. By not allowing compliance departments to include certain ethics and integrity questions in HR surveys or run separate ethical surveys, the compliance department does not have insight/data on the company culture.

- Replacing compliance monitoring by self-assessment questionnaires completed by the business themselves

- Not rolling out the compliance program to newly acquired businesses (i.e. Management believes that the “startup” mentality and innovation should be kept and not killed by the implementation of a compliance management program)

- Management not “owning” compliance and not verifying that minimum compliance processes and controls are working effectively

- Allowing certain types of investigations and their results not to be included in compliance case management statistics (e.g. HR conducts investigations on sexual harassment but these cases are not included in the case management reporting to the Board).

Wrong Incentives

- aggressive sales targets and “pressure” on business can induce inappropriate risk taking

- incentive systems that only consider the “what” (revenues, market share) and ignore the ‘how’ (i.e. playing by the rules).

- incentives without the corresponding check and balances to mitigate the increased risks coming from the incentive system

J.New Technologies and Compliance

J.1. New Technologies and Compliance

Technological advancements are fundamentally reshaping the compliance function. What was once seen as a reactive, manual, and cost-intensive area is rapidly transformed into a proactive, data-driven, and strategic business enabler. The integration of technologies such as artificial intelligence (AI), machine learning (ML), robotic process automation (RPA), blockchain, and advanced analytics is not only redefining the operational aspects of compliance, but also its purpose, skillset, and value to the organization. The strategic integration of cutting-edge technologies is critical for a modern Compliance function. These innovations are not just tools for efficiency; they are foundational pillars for a data-driven approach, empowering compliance professionals to operate with greater precision, scalability, and strategic insight.

Here's a breakdown of the key roles new technologies will play:

1. **Automation of Routine and Repetitive Tasks (RPA & AI)**

- **Reduced Manual Burden:** Robotic Process Automation (RPA) and AI will take over mundane, high-volume tasks such as data entry, document review, standard reporting, evidence collection for audits, and initial customer due diligence (KYC/AML checks).

- **Increased Efficiency and Accuracy:** Automation significantly reduces human error, speeds up processes, and frees up compliance professionals to focus on higher-value activities that require judgment, analysis, and strategic thinking. This can lead to substantial cost savings.

- **Examples:** Automating the collection of employee training records, flagging suspicious transaction patterns based on predefined rules, or generating routine compliance reports.

2. **Enhanced Monitoring, Surveillance, and Anomaly Detection (AI & Machine Learning)**

- **Leveraging Big Data for Real-time Insights:** This is where the data-driven nature of modern Compliance truly comes to the forefront. AI-powered tools, especially those leveraging Machine Learning, can process and monitor vast, diverse datasets – including transactional records, digital communications, and user behavioral patterns – in real-time. This capability enables the identification of subtle patterns, anomalies, and potential regulatory violations that would be virtually impossible for human review to uncover.

- **Reduced False Positives:** ML algorithms continuously learn from historical data, adapting and refining their risk assessment models. This iterative learning significantly reduces the incidence of "false positive" alerts, which traditionally consume considerable compliance staff time and resources. The result is a more precise and actionable risk identification process.

- **Predictive Analytics:** Moving beyond reactive detection, AI and ML can predict potential compliance issues before they escalate by analyzing trends and identifying early warning signs. This allows for proactive intervention strategies, transforming compliance from a reactive police force into a forward-looking risk intelligence unit.

- **Examples:** AI flagging unusual trading activity, suspicious communication between employees and third parties, or predicting which employees are at higher risk of non-compliance based on behavioral indicators.

3. **Intelligent Regulatory Intelligence and Impact Analysis (NLP & Generative AI)**

- **Automated Horizon Scanning:** Natural Language Processing (NLP) and Generative AI can continuously monitor global regulatory updates, legal changes, and industry guidance from a multitude of sources.

- **Impact Assessment:** These technologies can analyze new regulations, summarize key changes, identify their impact on existing policies and controls, and even suggest necessary adjustments.

- **Policy Generation & Updates:** Generative AI can assist in drafting, updating, and localizing compliance policies and procedures, ensuring they remain current and aligned with evolving requirements.

- **Examples:** AI identifying a new data privacy law impacting the company's European operations, summarizing its key requirements, and flagging relevant internal policies for update.

4. **Improved Investigation and Remediation (AI & Data Analytics)**

- **Expedited Discovery:** AI can rapidly sift through massive volumes of unstructured data (emails, chat logs, voice recordings) during investigations to identify relevant information and potential evidence.

- **Case Management & Prioritization:** AI can help prioritize investigation cases based on risk scores and identify potential connections between seemingly unrelated incidents.

- **Root Cause Analysis:** Advanced analytics can assist in identifying the underlying systemic issues that led to a compliance breach, allowing for more effective remediation.

- **Examples:** AI analyzing employee communications to detect potential collusion or fraud, or generating summaries of complex investigation findings for review.

5. **Enhanced Reporting and Visualization (Business Intelligence Tools)**

- **Dynamic Dashboards:** Interactive dashboards provide real-time visibility into compliance performance, risk exposure, control effectiveness, and progress on remediation efforts.

- **Automated Regulatory Reporting:** Technologies can automate the collection, validation, and submission of data for regulatory reports, ensuring accuracy and timeliness.

- **Data Storytelling:** Presenting complex compliance data in a clear, compelling, and actionable way to senior leadership and the Board.

6. **Immutable Record-Keeping and Transparency (Blockchain)**

- **Tamper-Proof Audit Trails:** Blockchain's distributed ledger technology can provide an immutable and transparent record of compliance activities, transactions, and approvals. This enhances auditability and reduces the risk of data manipulation.

- **Enhanced KYC/AML:** Blockchain-based digital identities could streamline customer onboarding and due diligence processes by providing secure and verifiable identity information.

- **Supply Chain Traceability:** For certain industries, blockchain can provide end-to-end visibility and traceability in supply chains, crucial for ESG, anti-slavery, and product safety compliance.

7. **Training and Awareness (AI & Gamification)**

    - **Personalized Training:** AI can tailor compliance training modules to individual employee roles, risk profiles, and knowledge gaps, making training more relevant and effective.
    - **Interactive Learning:** Gamification and immersive technologies can make compliance training more engaging and memorable.
    - **AI Chatbots for Queries:** AI-powered chatbots can provide instant answers to common compliance questions, freeing up compliance staff for more complex inquiries.

Overall Impact

The integration of these new technologies fundamentally redefines the role of the compliance professional. The function shifts from a primary focus on manual review and enforcement to that of a sophisticated data analyst, technological strategist, ethical advisor, and proactive risk manager. Modern Compliance departments will become inherently more agile, data-centric, and forward-looking, enabling organizations to navigate an increasingly complex and interconnected global regulatory landscape with enhanced confidence, greater efficiency, and a strengthened ethical foundation. The judicious adoption and strategic integration of these technologies are no longer optional but imperative for any company aiming to build a truly robust, future-ready, and strategically valuable compliance program. Compliance is no longer only about ticking regulatory boxes — it's about building resilient, forward-looking organizations capable of navigating complexity with integrity and agility. As technology continues to advance, the compliance function must lead, not follow, in shaping the future of responsible business.

K. Outlook

The field of compliance is undergoing a significant transformation, moving beyond its traditional "police" or "check-the-box" function to become a more strategic and integral part of business operations. Here is what we think is a reasonable outlook for where compliance is going:

K.1. Outlook: Where is Compliance Going?

1. **From Reactive to Proactive and Predictive**

   - **Anticipation is Key:** The focus will shift even more strongly towards anticipating regulatory changes and emerging risks rather than just reacting to them. This involves continuous regulatory intelligence gathering and horizon scanning.

   - **Data-Driven and Predictive Analytics:** Leveraging advanced analytics, AI, and machine learning to identify patterns, detect anomalies, predict potential compliance breaches, and proactively manage risks. This moves compliance from looking backward to looking forward.

2. **Increased Strategic Importance and Business Integration**

   - **Business Enabler:** Compliance will be seen less as a cost center or a blocker and more as a strategic enabler of sustainable growth, innovation, and competitive advantage. Companies that effectively manage compliance can build trust, attract ethical investors, and expand into new markets more smoothly.

   - **Embedded in the Business:** Compliance will become more deeply embedded in business processes and decision-making, with "compliance by design" becoming the norm. This means compliance teams will work closely with product development, sales, marketing, and IT from the outset of any new initiative.

   - **Interdisciplinary Collaboration:** CCOs will increasingly collaborate with other C-suite executives (CFO, CIO, CRO, CHRO) to ensure a holistic approach to risk management and corporate governance.

3. **Technological Transformation (RegTech and AI)**

   - **Automation of Routine Tasks:** AI and automation will handle more of the mundane, repetitive tasks like basic data monitoring, document review, and initial risk assessments, freeing up human compliance professionals for more complex, strategic, and judgment-based work.

   - **Enhanced Monitoring and Surveillance:** AI-powered tools will offer real-time monitoring of transactions, communications, and behaviors, significantly enhancing detection capabilities and reducing false positives.

   - **AI Governance:** Compliance will play a critical role in governing the ethical and compliant use of AI itself, addressing issues like algorithmic bias, data privacy in AI, explainability, and accountability.

   - **Regulatory Technology (RegTech):** Continued growth and adoption of RegTech solutions that streamline compliance processes, improve reporting accuracy, and provide dynamic compliance dashboards.

4. **Broader Scope of Responsibilities – Especially ESG**

- **ESG (Environmental, Social, and Governance):** ESG compliance is rapidly expanding beyond voluntary frameworks to mandatory reporting and due diligence requirements (e.g., EU's CSRD, CS3D). Compliance departments will be central to managing ESG risks, reporting, and anti-greenwashing efforts across the value chain.

- **Data Privacy and Cybersecurity:** As data continues to grow and cyber threats evolve, compliance will deepen its collaboration with IT and cybersecurity to ensure robust data governance, privacy protection (e.g., GDPR, CCPA, PIPL), and incident response.

- **Third-Party Risk Management:** Increased scrutiny on supply chains and third-party relationships will make robust due diligence and ongoing monitoring of vendors and partners a core compliance function.

5. **Focus on Culture and Behavioral Compliance**

- **"Tone from the Middle":** While "tone at the top" remains vital, there will be increased emphasis on ensuring ethical behavior and compliance values are cascaded and reinforced by middle management.

- **Behavioral Science:** Integrating insights from behavioral economics and psychology to design more effective compliance programs that influence employee behavior and decision-making positively.

- **Employee-Centric Compliance:** Designing compliance programs that are user-friendly, accessible, and provide clear guidance to employees, empowering them to make ethical choices.

Reasonable Outlook for Compliance Departments and the Compliance Function

- **Elevated Status of the CCO:** The Chief Compliance Officer will solidify their position as a key strategic advisor at the executive and Board levels, frequently participating in business strategy discussions.

- **Smaller, More Specialized Teams (Leveraging Tech):** Compliance departments might not necessarily grow massively in headcount but will likely become more specialized. They will require professionals with a blend of legal, technological, data analytics, and behavioral science skills.

- **"Hybrid" Compliance Professionals:** The ideal compliance professional will possess strong regulatory knowledge, business acumen, and an understanding of technology (AI, data analytics) to interpret complex data and drive tech-enabled compliance solutions.

- **Continuous Evolution:** The compliance function will need to be highly adaptable and agile, constantly re-evaluating its strategies and tools to keep pace with rapid technological advancements, evolving global regulations, and changing business models.

- **Compliance as a Competitive Differentiator:** Companies that proactively invest in and successfully integrate compliance into their DNA will gain a significant competitive advantage, attracting talent, investors, and customers who value integrity and responsible business practices.

In essence, compliance is moving from a reactive, cost-of-doing-business necessity to a proactive, strategic enabler of trust, innovation, and long-term value creation.

K.2. What skillset will be needed in the future

The compliance professional of the future will need a sophisticated blend of traditional and cutting-edge skills, moving beyond simply "knowing the rules." Here is a breakdown of the essential skill set we believe will be required going forward:

I. Core Foundational Skills (Still Essential, but Evolving)

1. **Deep Regulatory Knowledge & Legal Acumen**

- **Specialized Expertise:** While a broad understanding is important, many roles will require deep dives into specific regulatory domains (e.g., AML, sanctions, data privacy, ESG, consumer protection, competition law, industry-specific regulations like financial services, healthcare, or tech).
- **Global Perspective:** As businesses operate globally, understanding cross-border regulatory complexities and jurisdictional nuances will be crucial.
- **Legal Interpretation:** The ability to accurately interpret complex laws, regulations, and guidance, and translate them into practical, actionable policies and procedures for the business.

2. **Risk Assessment & Management**

- **Proactive Identification:** The ability to identify emerging risks, anticipate regulatory changes, and understand their potential impact on the business.
- **Holistic View:** Assessing risks across financial, operational, reputational, and strategic dimensions, not just legal.
- **Risk Mitigation Strategies:** Designing and implementing effective controls and mitigation plans tailored to specific risks.

3. **Communication & Influence**

- **Clarity and Simplicity:** Translating complex legal and technical jargon into clear, concise, and actionable language for diverse audiences (board, senior management, front-line employees).
- **Persuasion and Negotiation:** The ability to influence stakeholders, gain buy-in for compliance initiatives, and effectively resolve conflicts when business objectives clash with compliance requirements.
- **Active Listening:** Understanding the perspectives and challenges of business units to design pragmatic and effective compliance solutions.
- **Executive Presence:** The ability to present confidently and articulate complex issues to the Board and senior leadership.

4. **Integrity & Ethical Judgment**

- **Unwavering Ethics:** This remains the absolute bedrock. The compliance professional must embody the highest ethical standards and act with integrity, even under pressure.
- **Moral Compass:** The ability to make difficult decisions that prioritize ethical conduct and regulatory adherence over short-term gains, and to stand by those decisions.

5. **Critical Thinking & Problem Solving**

- **Analytical Acuity:** The capacity to break down complex issues, analyze root causes of non-compliance, and identify systemic weaknesses.

- **Strategic Thinking:** Moving beyond mere rule-following to connect compliance efforts with broader business strategy and organizational goals.

- **Solution-Oriented:** Developing practical, effective, and sustainable solutions to compliance challenges.

II. Emerging & Increasingly Crucial Skills (The "Future-Ready" Skills):

1. **Data Fluency & Analytics**

- **Data Sourcing & Cleaning:** Understanding where relevant data resides and how to ensure its quality and completeness.

- **Advanced Analytics Tools:** Proficiency in using data visualization tools, statistical software, and potentially basic coding (e.g., Python, R) to analyze large datasets, identify patterns, anomalies, and red flags.

- **Predictive Analytics:** The ability to leverage data to anticipate potential compliance risks and guide proactive interventions.

- **Metrics & Reporting:** Developing meaningful compliance metrics and dashboards to provide actionable insights to management and the Board.

2. **Technology Proficiency & RegTech Acumen**

- **Understanding AI/ML:** Not necessarily being a data scientist, but understanding how AI and machine learning work, their capabilities for compliance (e.g., transaction monitoring, communication surveillance, document analysis), and critically, their limitations and ethical implications (e.g., bias detection).

- **RegTech Implementation:** Familiarity with various RegTech solutions and the ability to evaluate, implement, and optimize these technologies for efficiency and effectiveness.

- **Cybersecurity & Data Privacy:** A strong understanding of cybersecurity best practices, data protection laws (GDPR, CCPA), and how they intersect with compliance, especially with increasing data volumes and cyber threats.

3. **Behavioral Science & Culture Building**

- **Understanding Human Behavior:** Applying insights from behavioral economics and psychology to design more effective compliance training, communication, and incentives that actually influence employee conduct.

- **Culture Assessment:** Tools and techniques to assess and measure the ethical culture of an organization, identifying areas for improvement.

- **Change Management:** Skills to drive cultural change and embed compliance thinking throughout the organization.

4. **Project Management & Program Design**

- **Strategic Program Development:** Ability to design, implement, and continuously improve a comprehensive, risk-based compliance program.

- **Project Execution:** Managing complex compliance initiatives, integrating technology, and ensuring timely delivery of objectives.

5. **Adaptability & Continuous Learning**

- **Agility:** The compliance landscape is dynamic. Professionals must be agile and able to quickly adapt to new regulations, technologies, and business models.
- **Growth Mindset:** A commitment to lifelong learning, staying updated with industry trends, emerging risks, and new compliance methodologies.

In summary, the compliance professional of the future will be a

- **Strategic Advisor:** Partnering with the business to enable compliant growth.
- **Technological Integrator:** Leveraging data and AI to enhance program efficiency and effectiveness.
- **Data Storyteller:** Translating complex data into actionable insights for decision-makers.
- **Culture Architect:** Fostering an ethical environment where compliance is naturally embedded.
- **Perpetual Learner:** Continuously evolving their skills to keep pace with an ever-changing world.

L. Disclaimer

1. General Information and Purpose: This strategic paper, "The evolving purpose, scope and success factors of Compliance: why Compliance must be independent from Legal function," (the "Paper") has been prepared by the European Network for Compliance Officers (ENFCO) for informational and discussion purposes only. It aims to stimulate dialogue, share perspectives, and contribute to the ongoing development of compliance practices within Europe and beyond. The views and opinions expressed herein are those of the authors and do not necessarily reflect the official policy or position of any organization, institution, or legal authority unless explicitly stated.

2. Not Legal Advice: The content of this Paper is not intended to constitute, and should not be relied upon as, legal, professional, financial, or any other form of advice. It is a strategic and conceptual document and does not address the specific circumstances of any individual, entity, or legal jurisdiction. Readers should consult with qualified legal and compliance professionals for advice pertaining to their specific situations and before making any decisions or taking any actions based on the information presented in this Paper.

3. Accuracy and Completeness of Information: While ENFCO has made every effort to ensure the accuracy and completeness of the information presented in this Paper as of the date of publication, we do not guarantee the same. The field of compliance, as well as relevant legal and regulatory frameworks, is dynamic and subject to continuous change. ENFCO and the authors disclaim all liability for any errors or omissions, or for the results obtained from the use of this information.

4. Forward-Looking Statements: This Paper may contain forward-looking statements or projections regarding future trends, developments, or outcomes in the field of compliance. These statements are based on the authors' current expectations and assumptions and involve known and unknown risks, uncertainties, and other factors that may cause actual results, performance, or achievements to differ materially from those expressed or implied by such forward-looking statements. ENFCO undertakes no obligation to update or revise any forward-looking statements to reflect new information, events, or circumstances.

5. Limitation of Liability: To the fullest extent permitted by law, ENFCO, its members, directors, officers, employees, agents, and the authors of this Paper shall not be liable for any direct, indirect, incidental, consequential, special, punitive, or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data, or other intangible losses (even if ENFCO has been advised of the possibility of such damages), resulting from: (i) the use or the inability to use the Paper; (ii) any content or information contained in the Paper; (iii) any reliance placed on the completeness, accuracy, or existence of any advertising, products, or other materials appearing in the Paper; or (iv) any other matter relating to the Paper.

6. Intellectual Property: This Paper, including all its content, is the intellectual property of ENFCO and/or the contributing authors and is protected by copyright and other intellectual property laws. Reproduction, distribution, modification, or transmission of any part of this Paper without the prior written consent of ENFCO is strictly prohibited, except for personal, non-commercial use, provided that all copyright and proprietary notices are retained.

M. Acknowledgement

We gratefully acknowledge the invaluable contributions of the following individuals, whose expertise, insights, and collaboration significantly enriched this white paper:

- **Andrijana Bergant**, President, EICE - European Institute for Compliance and Ethics, Slovenia
- **Carlos Martins**, Chairperson, Gibraltar Association of Compliance officers
- **Lucia Sanchez- Ocana Luyen,** First Vice President, ASCOM - Asociación Española de Compliance
- **Radomir Dukov**, Chairperson, Bulgarian Association of Anti- Financial Crime Experts
- **Patrick Wellens**, Chairperson, Ethics & Compliance Switzerland

Their diverse perspectives and dedication to advancing “The evolving purpose, scope and success factors of Compliance: why Compliance must be independent from Legal function” were critical to the quality and depth of this publication.

We also extend our thanks to the broader community of professionals and stakeholders who supported this initiative through feedback, dialogue, and peer review.

ENFCO

EUROPEAN NE ORK FOR
COMPLIANCE OFFICERS

European Network for Compliance Officers (ENFCO) at
Berufsverband der Compliance Manager (BCM) e. V.
Oberwallstraße 24 | 10117 Berlin | Germany
Tel. +49 (0) 30 / 84 85 93 20 | info@bvdcm.de | www.enfco.eu