



Serap Tutkun
is a senior manager at
KPMG Forensic Integrity
& Compliance.



Rebecca Kozlowski
is a manager at KPMG
Forensic Integrity &
Compliance.

The true cost of cutting corners: why regulatory compliance should be a priority



In today's complex regulatory environment, companies face increasing pressure to comply with a myriad of laws and regulations. This article explores the evolving landscape of compliance, highlighting recent regulatory changes and their implications for businesses. By examining enforcement actions and the costs of non-compliance, it underscores the importance of proactive compliance measures. Ultimately, investing in robust compliance programs not only mitigates risks but also fosters a strong ethical culture and supports sustainable business growth.

INTRODUCTION

Whether a company operates in the EU, the US or globally, in today's business world, the risk of non-compliance with existing and recently adopted regulations has become too costly to ignore. Companies in all industries must take preventive measures that assess and mitigate the key risks to address this (e.g., sanctions breach, corruption, money laundering, product compliance, export control violations). Depending on the risk exposure and the size of the company, ensuring the right measures are in place, including compliance framework, target operating model (TOM), internal controls and supportive technology. However, the effort and cost required to maintain compliance remain the smarter and more cost-effective investment compared to the potential penalties of non-compliance.

This article starts with an overview of various recent regulatory changes which will, or already do, impact organizations operating within different sectors globally. Furthermore, this article outlines the potential risks of non-compliance with regulatory requirements, citing examples from enforcement actions in the US and the EU in recent years. Finally, it is argued that investing in and prioritizing proactive approaches to compliance can help companies avoid potential financial and reputational penalties, while also fostering a strong ethical risk culture and supporting business growth.

INCREASING REGULATORY DEMANDS

The legal landscape of business conduct requirements has expanded rapidly in recent years. A decade ago, companies with a global footprint focused their regulatory compliance efforts on complying with Anti-Bribery and Corruption laws with extraterritorial reach – such as the US Foreign Corrupt Practices Act (FCPA), the UK Bribery Act (UKBA) – as well as on accounting compliance to address corporate fraud (Sarbanes-Oxley Act), privacy (EU General Data Protection Regulation, [Huij23]) and international and market laws for fair competition and consumer protection ([Spiv24]). In the meantime, the public debates around companies' responsibilities for personal data collection and processing, protection of consumers in the online environment, environmental impact and sustainable business practices have also changed the expectations of investors and customers. The requirement to operate with transparent and accountable governance has become a key component of responsible business conduct. When this is not adhered to, it increases the risk of negative media coverage and damages a company's reputation.

In recent years, many of these previously considered “good-to-have” requirements materialized into new laws and regulations. Below are a few recent (non-exhaustive) examples of the new and upcoming regulations in the Netherlands, EU and the US that establish new obligations for a wide range of companies operating within various industries.

One regulation driving the vast change in the Dutch compliance landscape is the introduction of the *Verklaring Omtrent Risicobeheersing (VOR) (statement on risk management [ed.]*). This amendment to the Dutch Corporate Governance Code in March 2025 (effective from 1 January 2025) requires management boards to provide a formal statement on their organization's overall risk management, internal control and compliance via demonstrable evidence (e.g., control execution, corrective actions, etc.). The VOR is also aligned with other regulatory developments in the EU ([KPMG25b]).

The EU has adopted several new acts and directives:¹

- the **Corporate Sustainability Reporting Directive (CSRD)**, which introduces requirements for large companies as well as listed small and medium-sized enterprises to report on a wide range of sustainability topics, and to collect information from their supply chain to analyze the risks associated with their business relationships (entered into force on 5 January 2023) ([EuCo]);
- the **Digital Services Act (DSA)**, which introduces obligations for companies and member states aimed at safeguarding consumer protection online (entered into force on 16 November 2022) ([EuCo24]; see also [Riet24] and the article about DSA in this edition);
- the **Digital Markets Act (DMA)**, which requires very large online platforms to act as gatekeepers for safeguarding online market competition (entered into force on 1 November 2022) ([EuCo23]).

Additionally, a few other regulations that have the potential to shape new industry requirements are currently undergoing the EU Digital Omnibus process:

- the **Corporate Sustainability Due Diligence Directive (CSDDD)**, which sets new obligations for large companies in terms of protection of the environment and human rights in the EU and globally, for instance by means of mandatory due diligence procedures (approved by the EU Parliament on 24 April 2024 and 16 December 2025 (Omnibus) and will now become effective on 26 July 2029) ([Vuch24]);

¹ These regulations are often also applicable to non-EU companies that have presence in the EU (e.g., parent companies registered or listed in the EU, subsidiaries registered and operating in the EU).

- the **EU Artificial Intelligence Act** (AI Act), which creates safeguards and requirements for companies to make inventory of the AI systems used and be prepared to adopt applicable governance structures (approved by the EU Parliament on 13 March 2024 and entered into force on 1 August 2024) ([EuPa24]).

Finally, the US authorities have clarified and expanded existing laws and regulations (non-exhaustive) on business conduct, with impact for the companies that have a US nexus.²

- the **US Foreign Extortion Prevention Act** (December 2023), which expands the definition of public official / person acting on behalf of government, thus expanding FCPA reach ([Gonz23]);
- the **DoJ and FTC Merger Guidelines** (December 2023), which expands and strengthens the US anti-trust enforcement ([Suns23]);
- the **FTC Non-Compete Clause Rule** (April 2024), which establishes significant restrictions for the non-compete clauses ([Suns23]).

These and other regulations set the bar high for business conduct requirements expected of companies to operate in the Netherlands, EU or US jurisdiction(s). Depending on the geography and nature of the company's operations, different obligations may apply. To comply, companies need to ensure that the right internal controls, policies and procedures are effectively and timely incorporated into their compliance framework. Moreover, in some cases they also need to undergo external compliance assurance audits to demonstrate that they are in control of their compliance processes. Later in this article, we will provide insights into the actions companies can take to ensure legal compliance. However, it is important to first outline the potential risks and costs associated with failing to comply with business conduct regulations.

THE COST OF NON-COMPLIANCE

Although meeting stakeholders' expectations and building trust are important reasons for companies to enhance their corporate governance, they are not the only ones. When it comes to non-compliance with regulations, most law enforcement bodies take a punitive approach. The laws and regulations, and subsequently the enforcement practices, demonstrate to companies that a failure

² Nexus refers to operating within US territory, including nationality of persons involved in a (business) transaction, geographic location of the (business) transaction or entities within the (business) transaction and currency of the (business) transaction. For information about federal US regulatory developments, see [Crew25].

to address the risks may also bring significant financial consequences. To illustrate this point, it is useful to investigate the recent enforcement actions of the US Securities and Exchange Commission (US SEC) and the approach on non-compliance taken by the EU when creating the abovementioned recent acts and directives.

Being one of the key US agencies regulating the securities industry and enforcing fairness and transparency in the financial markets, the US SEC has the power to investigate and prosecute individuals and companies for violating anti-corruption laws (inc. the FCPA), as well as insider trading, market manipulation and other types of fraud. On a yearly basis, the US SEC publishes an overview of enforcement actions in the past year, highlighting the main trends in terms of the types of violations investigated and penalties resulting from the cases. In 2023, the SEC settled a total amount of USD 4.9 billion in financial remedies for violations of various market regulations ([SEC23]), marking the second highest amount in SEC history, after 2022. The SEC also reported an 8% increase in stand-alone actions over the previous year. Apart from actions directed at companies, 133 individuals were barred from serving as officers and directors of public companies due to wrongdoing identified during the investigation, which was also the highest number of bars obtained in a decade ([SEC23]).

Almost USD 5 billion in financial remedies obtained by the SEC resulted from civil penalties, disgorgements, and prejudgment interest imposed due to market violations by publicly traded companies ([SEC23]). The 784 enforcement actions were directed at companies headquartered both in the US and other countries (incl. the EU) and related to a wide range of violations ([SEC23]): from bribery and corruption, cybersecurity and investment frauds to the increasingly important issues of ESG-related misstatements and crypto fraud. To name a few examples, a failure to establish or follow the existing policies, procedures and internal controls resulted in a USD 100 million settlement with a global chemicals company for allegedly using agents to pay bribes to obtain contracts in Vietnam, India, and Indonesia ([SEC23]). Another company, a medical equipment supplier, settled to pay more than USD 62 million for allegedly influencing government officials to draft favorable tender calls in China ([SEC23]). These examples illustrate that when it comes to non-compliance, the US enforcement practice stipulates considerable financial consequences for the companies in question, which should encourage them to proactively foster compliance culture instead.

Like the US, the EU also takes punishment for failing to comply with laws and regulations seriously. As such, a gatekeeper company that failed to comply with the

DMA obligations could be sentenced to a fine of up to 10% of its total worldwide turnover (or up to 20%, in case of repeated infringement) ([EuCo23]). For violations of the DSA obligations, companies with more than 45 million active users may get fines of up to 6% of their global turnover ([EC24]). For some regulations (e.g., CSRD) the implications will depend on how the specific member state country has enforced the EU law, which can also reach significant amounts in fines, as well as imprisonment for the responsible individuals.

Apart from the direct fines, settlement fees, disgorgements and other types of penalties that may result from violating business conduct laws and regulations, companies must also keep other risks in mind— such as loss of shareholder and client trust, bad publicity and overall reputational damage. To minimize the risks of non-compliance, companies therefore should proactively improve their compliance frameworks and practices.

INVESTING IN COMPLIANCE

Despite the established and growing penalties for non-compliance, many companies continue to inadequately invest in (regulatory) compliance. This may stem from the traditional perception that compliance programs are cost centers in a policing role. This perception and level of investment also differ per sector. The financial sector was effectively forced to invest in compliance across the board after the 2008 financial crisis resulted in swift and high-pressure regulatory changes. This has, on average, resulted in an estimated cost of USD 10,000 per employee to maintain compliance in large financial institutions ([Crew25]). The corporate sector was once freer to decide how robust or involved their compliance programs were, as regulatory oversight was largely based on operational jurisdictions and where the entities were stock listed. This is beginning to change with the rise of regulations mentioned in the previous section.

Irrespective of the sector, historical investment in compliance was often limited to the minimum actions required to meet regulatory obligations, typically with a short-term strategic focus. This approach was frequently adopted without a comprehensive understanding of the company's regulatory or operational risk landscape, or a clear objective to foster a preventative compliance culture.

The result is under-resourced compliance functions – both in terms of funding and expertise – leading to transparency gaps for management or supervisory boards, and an immature risk culture that enables non-compliance with laws and regulations, potentially

so severe that it materially impacts the company, as demonstrated above.

Luckily, a shift has begun across global markets over the last decades. More and more companies choose to proactively invest in a robust compliance program that is positioned with adequate authority to drive regulatory compliance, while also fostering a resilient and dynamic risk culture. The cost to maintain compliance, regardless of the size, regulatory landscape or maturity of a company generally includes the following (non-exhaustive):

- establishing a compliance function, including employees, a TOM, and a compliance framework.
- executing the compliance framework and compliance plan, including oversight of regulatory obligations, establishing a third-party risk management framework and overseeing third party compliance with the company's obligations/expectations, performing ad-hoc or event-driven activities (e.g., due diligence screening and reviews), and seeking independent external reviews of the program and framework;
- establishing and maintaining regulatory change management, including monitoring regulatory trends and changes, seeking external advice and costs related to implementation of regulation; and
- reviewing developed processes and procedures to consider implementation of technology (e.g., compliance management systems, regulatory compliance software) to further optimize and support compliance activities.

What's more, these companies have proven that the cost to maintain regulatory compliance far outweighs the potential financial, operational and reputational penalties of non-compliance. The Ponemon Institute in the US conducted a study of over 46 multinational organizations, finding the results shown in Figure 1 ([Poner1]).

The actual cost to maintain compliance will vary per sector and company. Nonetheless, the global regulatory landscape has steadily grown. In 2023, 87% of Chief Ethics and Compliance Officers surveyed globally by KPMG expect to face increasing regulatory expectations and scrutiny over the next two years, and 43% cited new regulatory requirements as the greatest challenge to compliance in this timeframe ([KPMG23]). In the Netherlands specifically, 2025 Chief Ethics and Compliance Officers continue to feel this pressure, with 87% expecting to face increasing regulatory expectations into 2026, and 38% citing regulatory requirements as the biggest compliance challenge moving forward ([KPMG25a]). This further supports the notion that investing in and maintaining sound compliance programs is no longer an option for most companies.

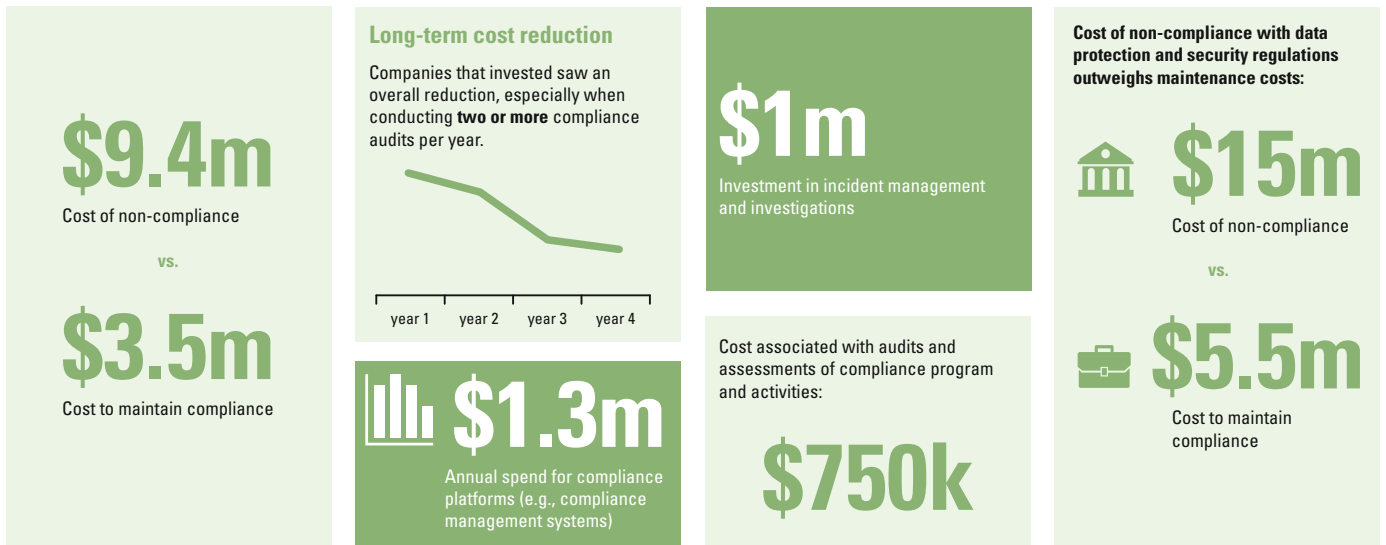


Figure 1. Cost of (non-)compliance according to the Ponemon Institute.

MANAGING COMPLIANCE COSTS THROUGH SOUND COMPLIANCE PROGRAMS

Investing in compliance is not a small feat. It requires a holistic approach supported by a comprehensive overview of risks and regulations. Companies seeking to (re)invest in compliance should take the following steps.

1. Perform a review of the existing compliance program and/or approach.
2. Perform a regulatory scan and develop an inventory of material compliance regulations, including associated risks (consider the applicability of obligations to the company based on (new) regulations, see the examples earlier in the article).
3. Consider a revision of the TOM is required to better support regulatory and operational compliance in design and effectiveness across the company.
4. Develop a roadmap to address the identified gaps within the existing approach and regulatory obligations.
5. Develop and implement an integrated and risk-based control framework.
6. Reinforce the TOM and governance structure to execute ongoing monitoring, testing and day-to-day support of the company.

Companies should ultimately determine the approach and steps that align best with their organization, industry, budget and regulatory landscape. For example, applying a risk-based approach by focusing on material regulations and key risks, assessing the most appropriate TOM, using technology, and considering outsourcing to fill expertise gaps and maintain independence.

SHORT-TERM DISRUPTION FOR LONG-TERM SUCCESS

Companies with global presence have experienced a steady increase in regulatory scrutiny and complexity across sectors. This has resulted in increased costs to maintain compliance and remediate incidents. However, companies that choose to invest in compliance – such as through the actions outlined in the previous part of this article – see their regulatory and operational burdens lessen in the long-term. Such companies are also better equipped to manage emerging trends and see their second line functions more dynamically collaborating with the business to achieve goals collectively.

Maintaining an effective and resilient compliance program requires a long-term vision that can adjust to both internal and external (un)foreseen factors. A sound compliance program goes beyond compliance with regulations and seeks to foster a strong ethical risk culture in every layer of the company. Achieving this requires a holistic assessment of the current and desired states of the compliance program and company, from a regulatory and operational compliance perspective.

Companies should act in a preventative manner to accommodate emerging compliance trends and upcoming regulations. This includes maintaining a comprehensive regulatory change management approach and prioritizing compliance. Compliance failings can occur in some instances, especially where new requirements are introduced (e.g., artificial intelligence) or where obligations impose additional administrative burdens (e.g., recordkeeping and retention). The penalties and costs to remediate failings also widely vary depending on the punitive nature of the jurisdiction and overall

situation. Therefore, companies must remain vigilant of regulations that may have a material impact, irrespective of the size of the regulation or the topic. They must additionally take measures to maintain adequate resources – including expertise, staffing and supportive tools – to meet regulatory obligations.

The starting point for most companies is reviewing the existing ways of working and obtaining an overview of their regulatory risk landscape. More mature companies may consider technology and external parties to collaborate and further optimize their compliance programs. Regardless of the maturity of your company, investing in compliance has become a necessity. Dedicating time and resources appropriately will ultimately

result in a compliance framework and program that grows with the business and supports it, rather than working against it.

References

- [Crew25] Crews, C.W. (2025). *Ten Thousand Commandments: An Annual Snapshot of the Federal Regulatory State*. Competitive Enterprise Institute. Retrieved from: <https://cei.org/studies/ten-thousand-commandments-2025/>
- [EC24] European Council & Council of the European Union (2024). *Digital Services Act*. Retrieved from: <https://www.consilium.europa.eu/en/policies/digital-services-act/#consequences>
- [EuCo] European Commission (n.d.). *Corporate sustainability reporting*. Retrieved from: https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en
- [EuCo23] European Commission (2023). *Questions and Answers: Digital Markets Act: Ensuring fair and open digital markets*. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2349
- [EuCo24] European Commission (2024, February 23). *Questions and answers on the Digital Services Act*. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348
- [EuPa24] European Parliament (2024). *Artificial Intelligence Act: MEPs adopt landmark law*. News European Parliament. Retrieved from: <https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law>
- [Gonz23] González Calvet, M., Raad, A.N., Rohlfen, R., Grishkan, Y.V., & King, J.M. (2023). *U.S. Congress Passes Law to Criminally Prosecute Corrupt Foreign Officials*. Ropes & Gray. Retrieved from: <https://www.ropesgray.com/en/insights/alerts/2023/12/us-congress-passes-law-to-criminally-prosecute-corrupt-foreign-officials>
- [Huij23] Huijts, L., Molenkamp, D. & Elbaz, M. (2023). Five years of GDPR supervision at a glance. *Compact* 2023/1. Retrieved from: <https://www.compact.nl/articles/five-years-of-gdpr-supervision-at-a-glance/>
- [KPMG23] KPMG Global (2023). *Stepping up to a new level of compliance: Chief Ethics and Compliance Officer Survey*. Retrieved from: <https://kpmg.com/us/en/articles/2023/cco-survey-2023-gated.html#Pressuresoncompliance>
- [KPMG25a] KPMG Netherlands (2025). *Matching the pace of compliance*. Retrieved from: <https://spo-global.kpmg.com/sites/nl-oi-intranet/SitePages/The-2025-Netherlands-Chief-Ethics-and-Compliance-Officer-Survey-results-are-in.aspx>
- [KPMG25b] KPMG Netherlands (2025). *Verklaring Omrent Risicobeheersing (VOR): Opportunities for continuous improvement on good governance and risk management*. Retrieved from: <https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/vor-opportunities-for-continuous-improvement-on-good-governance-and-risk-management.pdf>
- [Pone11] Ponemon Institute (2011). *The True Cost of Compliance: A Benchmark Study of Multinational Organizations*. Retrieved from: https://www.ponemon.org/local/upload/file/True_Cost_of_Compliance_Report_copy.pdf
- [Riet24] Rietschoten, M. van, Beemdelust, A. van, & Klein Tank, K. (2024). From Regulation to Reality: The DSA's early impact on Trust and Online Safety. *Compact* 2024/2. Retrieved from: <https://www.compact.nl/articles/from-regulation-to-reality-the-dsas-early-impact-on-trust-and-online-safety/>
- [SEC23] U.S. Securities and Exchange Commission (2023). *SEC Announces Enforcement Results for Fiscal Year 2023*. Retrieved from: <https://www.sec.gov/news/press-release/2023-234>
- [Spiv24] Spivack, P.S. & Costa Carvalho, I. (2024). *The Evolution of Compliance and here it is headed next*. Retrieved from: <https://latinlawyer.com/guide/the-guide-corporate-compliance/fifth-edition/article/the-evolution-of-compliance-and-where-it-headed-next>
- [Suns23] Sunshine, S.C. et al. (2023). *DOJ and FTC Release Final 2023 Merger Guidelines Formalizing Aggressive Merger Enforcement Playbook*. Skadden. Retrieved from: <https://www.skadden.com/insights/publications/2023/12/doj-and-ftc-release-final-2023-merger-guidelines>
- [Vuch24] Vuchot, A., Schmidtko, F., Spilker, M., Kuipers, P., & Wagemakers, S. (2024). *One step closer to a sustainable EU; the European Parliament adopts the revised CSDDD proposal*. Bird & Bird. Retrieved from: <https://www.twobirds.com/en/insights/2024/global/one-step-closer-to-a-sustainable-eu-the-european-parliament-adopts-the-revised-csddd-proposal>

About the authors

Serap Tutkun is a senior manager at KPMG Forensic Integrity & Compliance. She is an expert in supporting organizations in compliance and integrity, anti-bribery and corruption, third-party risk management, FCPA, due diligence, compliance frameworks, fraud risk management, and internal audits across various industries including construction, retail, manufacturing, and financial services.

Rebecca Kozlowski is a manager at KPMG Forensic Integrity & Compliance. She is a specialist in enhancing and maintaining compliance programs (including target operating models and risk/control frameworks). She specializes in regulatory and operational compliance in telecommunications, consumer goods, and healthcare sectors. She is also a KPMG Forensic ESG expert, driving value chain-wide change in organizations.