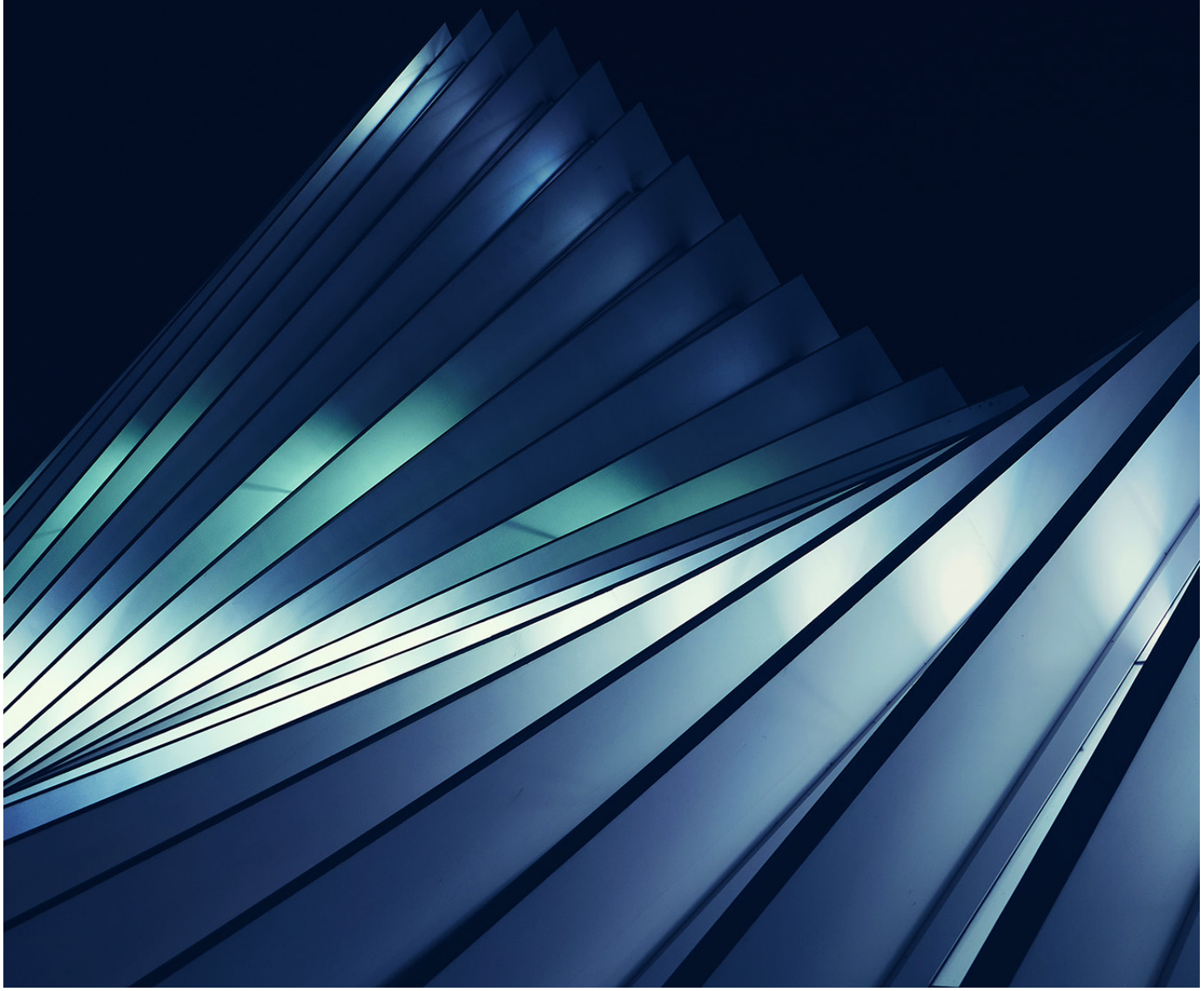
CROSS-BORDER INVESTIGATIONS

A new era of regulatory enforcement



Contributors

Boston Consulting Group GmbH

Dr. Bernhard Gehra
Managing Director & Senior Partner

Dr. Katharina Hefter
Managing Director & Partner

Dr. Georg Lienke
Associate Director

Jannik Leiendecker
Associate Director

Dmytro Golovatyi
Consultant

Freshfields Bruckhaus Deringer Rechtsanwälte Steuerberater PartG mbB

Dr. Moritz Pellmann
LL.M. (London), Partner

Dr. Philipp Redeker
Partner

Dr. Daniel Travers
Counsel

Dr. Christoph Werkmeister
LL.M. (Cambridge), Principal Associate

Holger Roos
Principal Associate

Dr. Vera Ibes
Associate

BCG BOSTON CONSULTING GROUP

Freshfields Bruckhaus Deringer

Amid a proliferation of conduct scandals and increasing awareness around corporate behaviour in relation to the environment and human rights, society's trust in business is fraying. Moreover, as calls for accountability grow louder, regulatory agencies are ramping up their efforts to ensure corporations obey the rules — and imposing heavy penalties on those that fail to deliver.

Supported by cross-border collaboration, compliance-related enforcement is no longer restricted to national jurisdictions. In fact, international investigations are the norm. For global businesses, this means two things: risk is rife and it is global. Based on our analysis of the current risk landscape, this paper focuses on two of the biggest potential pitfalls - anti-money laundering (AML) and cybercrime. Deep dives on these topics describe the shifting regulatory playing field and discuss ways in which corporations can assess their exposures and respond.

While there are few "quick wins" in effective risk and compliance management, there are relatively simple actions that businesses can take. Business leaders need to put in place systems to ensure they track the shifting regulatory framework, and are ready to implement changes as they happen. A key priority should be to build a dedicated target operating model (TOM). This will provide the structures and processes necessary for effective planning and action. If a money laundering or cyber incident does occur, businesses must also mobilise response teams and get ready for potential investigations. That means being ready to assemble task forces, gather necessary data, and manage external communications. Through these actions, they can embed the principles required to support effective risk management in increasingly uncertain and demanding times.

Because the financial industry has been under much more regulatory scrutiny over the last years the solutions developed to deliver sustainable effective risk management often have been driven predominantly by the banking sector, particularly in the field of AML. However, the general messages and key takeaways of this paper are tailored to financial and non-financial institutions alike (=corporations) and should inspire both industries to rethink their current approach to non-financial risk management.

A

Corporations Must Tackle Challenges on Multiple Fronts

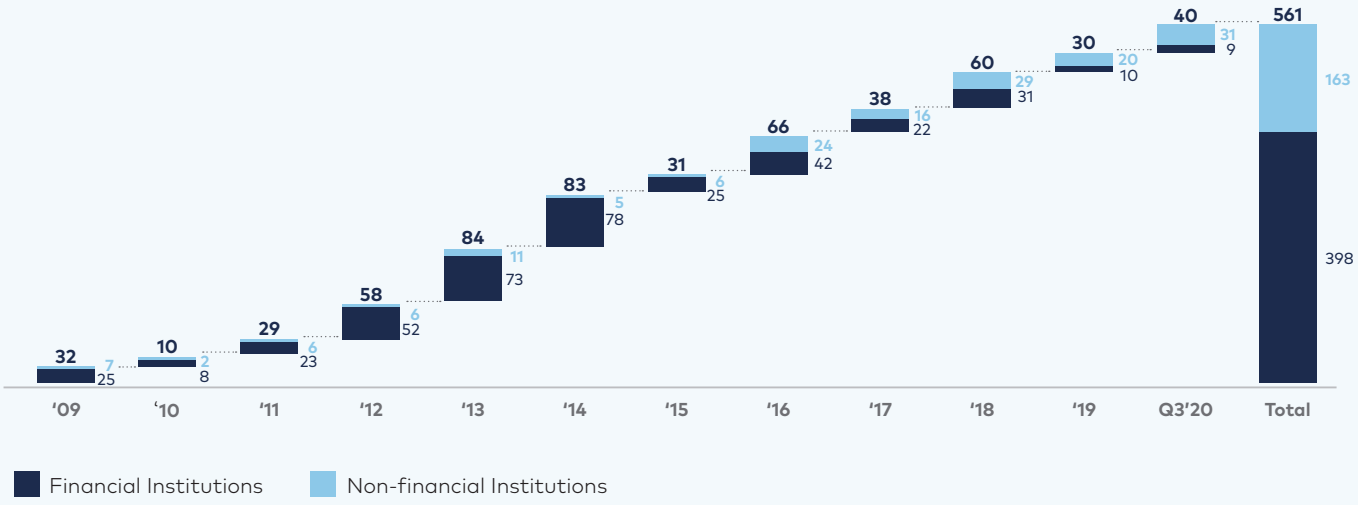
Risk is a daily part of conducting business, and decision makers are usually experts in assessing the risks they face, and might face. However, recent dynamics highlight three challenges that tend to apply to almost every business and which are rising up the strategic agenda. These are constantly high levels of financial penalties for any type of corporate misconduct, increasingly demanding regulatory regimes, and more effective cross-border enforcement.

The high price of corporate misconduct

Substantial financial penalties have become the norm over the last decade and are continuing to put pressure on corporates to get their game right. Across the financial and non-financial sectors, regulators and law enforcement agencies handed out just over $560 billion in fines for non-compliance between January 2009 and September 2020[1] (See Exhibit 1).

EXHIBIT 1 | More than $500 billion in fines for non-compliance

Major penalties for non-FI EURO STOXX 50, Dax, NASDAQ 100 & DJIA companies and major FI companies in Europe and North America (in B$)



Enforcement activity is also becoming more geographically dispersed, and regulatory actions are on the rise in Asia, Latin America, and Africa. High-growth countries such as China and India are stepping up their activities, imposing significantly higher penalties for misconduct. China's pharmaceutical sector, for example, is under considerable scrutiny, with several investigations under way. In June 2019, the Ministry of Finance announced that 77 major pharmaceutical companies would undergo an audit, including the local branches of global players.

1. Major penalties for non-FI EURO STOXX 50, Dax, NASDAQ 100 & DJIA companies and major FI companies in Europe and North America. "Major" meaning fines equal to or greater than $10M for non-FI companies and $20M for FI companies.

Legal and regulatory regimes are tightening

On top of an already high level of financial penalties comes a trend putting additional pressure on corporates. Law enforcement agencies across the globe have significantly accelerated their activities over the past decade, frequently turning to criminal law to hold companies liable for alleged misconduct. In addition, lawmakers across the globe are tightening the reins on corporate misconduct. Not only are corporations being prosecuted more frequently, but new laws are being introduced and existing rules strengthened - all with the aim of bringing companies to account. A recent example of this trend is the Anti-Money Laundering Act of 2020 (AMLA), passed by U.S. Congress on January 1, 2021. Among other amendments, it significantly expands the U.S. government's authority to obtain information from foreign financial institutions. The U.S. Treasury Department and the U.S. Department of Justice (DOJ) are entitled under the new law to subpoena foreign banks that maintain a correspondent account in the U.S. and request records relating to that account and any other account at the bank, as long as the records are deemed relevant. If a bank fails to cooperate, the AMLA can authorise the DOJ to require the U.S. correspondent bank to end its relationship with the foreign bank.

Against this increasingly stringent regulatory backdrop, compliance has become much more than a box-ticking exercise. Indeed, companies require a systematic approach, - one that can provide both defence against possible incidences and remediation where they do happen. Given high levels of personal responsibility in many jurisdictions, this is as important for individuals as it is for corporate entities. In Germany, for example, delayed disclosure of tax compliance breaches can constitute a criminal offence by any director, even if that person is not directly involved in tax affairs. The focus on individuals was recently illustrated by the prosecution of senior executives, including former board members, when a global car company was found to have mis-stated its diesel emissions.

The key to reducing these risks is to ensure adequate compliance mechanisms are in place. These will not only play a significant role in avoiding and reducing penalties; they will also lay the foundation for a more sustainable business model, which reflects the values and priorities of many of today's consumers.

Increasing international cooperation puts firms under pressure

Cooperation between prosecutors and other law enforcement authorities across borders is becoming the norm. In Europe, for example, the EU Agency for Law Enforcement Cooperation (Europol) collaborates with its member states' public prosecutor and regulatory offices (and their counterparts globally), using mutual legal assistance, as well as less formal arrangements.

Countries are also increasingly cooperating to combat what they consider to be harmful tax practices. For example, the most recent amendment to the EU-Directive on Administrative Cooperation (DAC6) introduces new tax disclosure rules and an automatic-exchange of information for cross-border transactions. On the other hand, companies understand they are operating on an uneven playing field in terms of tax laws, tax compliance requirements, and investigatory powers. As such, corporate structures and tax compliance systems must be adequately matched to each jurisdiction in which companies operate, and sometimes beyond.

Cross-border cooperation has become a fixture of global bribery, money-laundering, and tax fraud investigations. The U.S. Securities and Exchange Commission (SEC) and the DOJ officially acknowledged assistance from 40 authorities in 18 countries in 2020. By contrast, eight years earlier, in 2012, the SEC and the DOJ reported only two cases in which it received assistance by foreign agencies.[2]

In particular, there have been a rising number of initiatives aimed at money laundering. The Financial Crimes Enforcement Network (FinCEN), based in the U.S., aims to bring together law enforcement agencies and financial institutions from across the globe to share information and disrupt financial crimes. The Joint Money Laundering Intelligence Taskforce, based in the U.K., is a similar initiative. Given the current trend, these kinds of bodies are likely to become more common over the next few years.

Similarly, in the cyber realm, regulators increasingly talk to each other and more sophisticated cooperation mechanisms are proliferating, for example, data protection authorities in the EU have set up an international reporting and collaboration system to facilitate joint investigations. Such cooperation may lead to more intense scrutiny by multiple regulators across the globe with regard to deficiencies in technical and organisational measures so that the victim of a cyber attack may quickly turn into an offender. However, companies can also leverage one-stop-shop mechanisms to centralize proceedings in one jurisdiction instead of dealing with various regulators, ultimately mitigating the risk of multiple penalties and making outcomes more predictable.

This paper examines the impact of these shifting dynamics in two compliance-specific contexts – the conduct of AML activities and the battle against cybercrime, both of which yield specific and broad learnings.

2. Source: US Securities and Exchange Commission (www.sec.gov)

B

AML investigations amidst increasing regulatory scrutiny[3]

Money laundering high on the C-Suite agenda

Money laundering continues to present substantial risk to corporations, mainly due to the unpredictability of events, the volume of underlying allegations, and the potential intensity of corresponding regulatory responses. This holds particularly true for financial institutions. One reason that regulatory scrutiny has intensified in recent years is that money laundering can have such a significantly detrimental effect on the real economy. There is therefore pressure on compliance officers to be on top of the game and find an operating model that reduces risk to a minimum. Where regulators launch investigations, the pressure is ramped up even further. The best way to avoid these eventualities is to get ahead of the curve.

That means monitoring regulatory changes, building state-of-the-art target operating models, and putting in place the capabilities to respond should an investigation occur.

3. AML= Anti-Money Laundering

Staying ahea of regulatory changes

The AML regulatory framework is changing at pace and is likely to be shaped by two factors over the coming year.

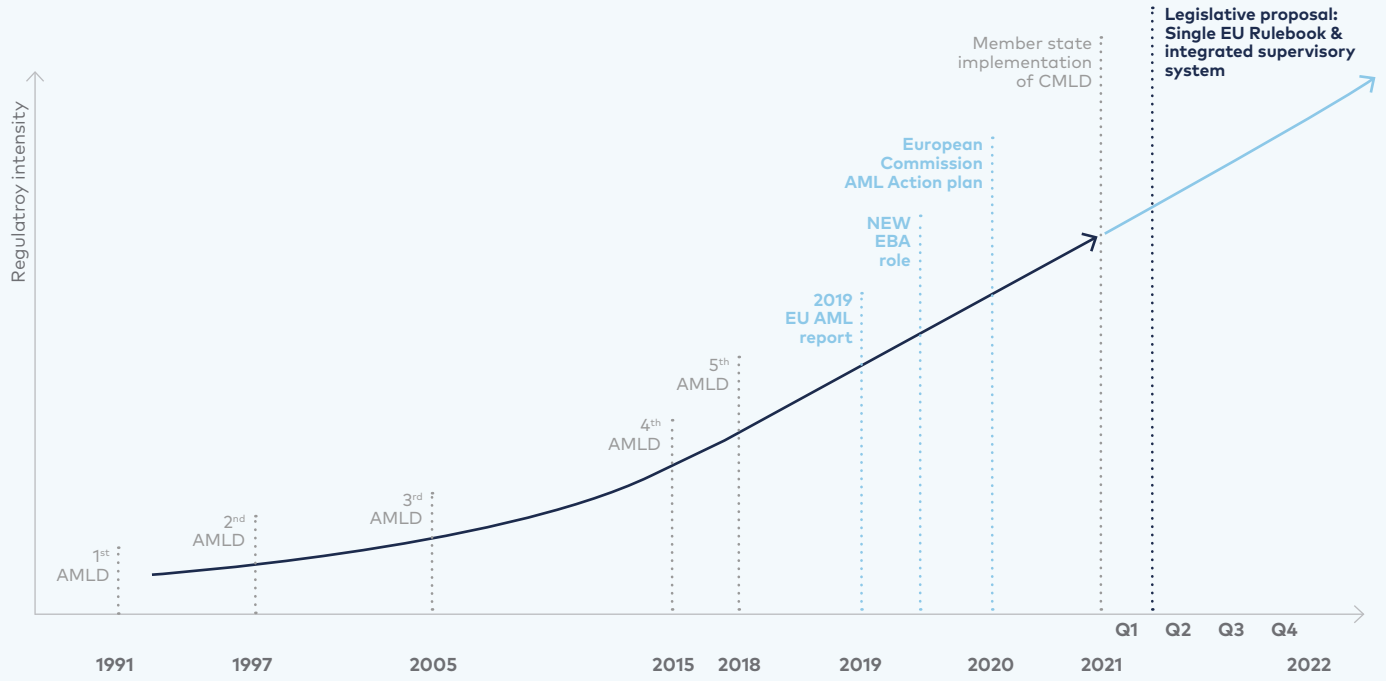
The EU Directive on Criminalisation of Money Laundering (CMLD)[4]

The transposition of the CMLD into national legal frameworks will substantially expand the scope of predicate offences that qualify as money laundering. These will include environmental crime, insider trading and market manipulation, cybercrime, and all crimes with a minimum prison sentence of six months or maximum sentence of more than one year. Some countries, such as Germany, will go further, encompassing proceeds from any crime, including petty offenses (the so-called "all crimes approach"). As a result, there will be a dramatic increase in the share of money within EU economies considered to be in scope.

The European Commission AML Action Plan

In May 2019, the European Commission (EC) announced a comprehensive AML Action plan, aiming to fundamentally reform the region's AML regulatory framework – both for financial and non-financial institutions (See Exhibit 2). The EC has since announced a legislative proposal for March 2021 and is pushing for the revised framework to take effect as early as October 2022.

EXHIBIT 2 | Game change in EU AML regulation currently in implementation



AMLD: Anti-Money Laundering Directive

4. Directive (EU) 2018/1673 of the European Parliament and of the Council of October 2018 on combating money laundering by criminal law

Under the revised framework, corporations should anticipate the following changes:

A single EU AML rulebook

The Single EU AML Rulebook is a step towards a harmonised regulatory regime. Under the changes, critical parts of the current directive-based framework will be transcribed into an EU Regulation, which will be directly applicable in all member states. Based on recommendations by the European Banking Authority (EBA), corporations should anticipate the following:

- Specific CDD requirements
- Stricter requirements for AML controls
- Enhanced transparency on cross-border AML data-sharing procedures
- SREP assessments.[5] Going forward prudential supervisors will increasingly focus on money laundering risk

An integrated EU AML supervisory system

EU AML supervision is currently in the hands of each of the 27 member states. However, given that human and financial resources, skills, and priorities vary widely across the EU, supervision can be uneven.

The EBA has a strong preference for EU-wide direct supervision of high-risk financial institutions, with indirect supervision of other obliged entities under the joint responsibility of national supervisors. Whether the mandate for EU Direct supervision will be allocated to EBA, or to a separate EU agency, is still subject to negotiation.

CASE STUDY • **Finding yourself in the eye of the storm**

A network of investigative journalists publishes reports and extensive raw data on a complex and extensive money laundering system dating back years. Several financial institutions immediately start evaluating and checking the data against their customers, while law enforcement authorities in multiple jurisdictions start investigating cash flows.

Any bank used in the money laundering scheme faces the challenge that its SAR (Suspicious Activity Report) filing going forward must keep up with findings of law enforcement agencies and further press reports. At the same time, it must prepare for regulatory AML investigations and defend itself against potential subsequent enforcement actions by prosecutors.

Essential actions for AML investigation success

Regulators initiate AML investigations to check allegations of potential misconduct and identify relevant evidence. A successful defence usually depends on being able to demonstrate that an institution has identified its individual risk profile, maintained a functioning AML framework, and reacted swiftly and forcefully to any suspicion of money laundering. In that regard, two success factors stand out:

An AML Target Operating Model

To structure their risk management activities, financial institutions must design and implement an AML Target Operating Model (TOM). BCG's AML TOM has five major building blocks: AML strategy, governance & organisation, risk management, data & IT, and culture of integrity (See Exhibit 3).

EXHIBIT 3 | **Anti-money laundering target operating model – selected elements**

01	AML Strategy	• Financial crime risk appetite incl. quantitative thresholds (e.g. maximum number of high risk customers) • AML Plan including key AML priorities and optimisation measures for the next 12 to 24 months
02	Governance & Organisation	• Three Lines of Defence incl. risk ownership of 1st LoD[6] and defined mandates for 1st, 2nd and 3rd LoD • Global Functional Lead defining AML standards and implementing these across the organisation
03	Risk Management	• Regulatory Change Management incl. adaptation of internal policies and procedures • Risk assessment to identify risk inherent to business activities and adequate controls
04	Data & IT	• Event driven calculation of Customer Risk Rating based on high quality data feeds • Establishment of IT platform as single KYC data source; workflow solution to support KYC activities
05	Culture of Integrity	• Leadership communication on need of Client and Risk ownership in 1st LoD (Tone from the top) • Awareness campaigns and subsequent belief audits to measure effectiveness

Equally, non-financial institutions should consider developing and implementing an AML TOM, tailored specifically to their business and operating model and individual risk exposure to money laundering.

5. Supervisory Review and Evaluation Process (SREP)
6. LoD = Line of Defence

Investigation readiness: Prepare for the worst

Once money laundering allegations are in the public domain, corporations must turn their attention towards preparing for a potential investigation by regulators and prosecutors.

It should be noted that regulators expect corporations to be prepared for investigations and to have action plans, emergency processes and stakeholder lists at hand that adequately reflect their business and operating model. It is therefore mandatory to think through the following items in advance to be prepared when times get rough.

Understand the allegations, and your own involvement

Based on a thorough understanding of the allegations, corporations should speedily assess their possible involvement. Depending on the jurisdiction of the prosecutor or regulator, and the geographical focus, this may require close collaboration with local branches or subsidiaries.

Identify internal and external stakeholders

Unless directly involved, stakeholders should be selected based on either their responsibility for activities subject to the allegations, or their ability to support the investigation. In addition to the above, and where required, external legal counsel should be involved.

Identify and gather data

Financial institutions should identify and gather data to assess the number of underlying client relationships, products, or transactions linked to the alleged misconduct. This will help them to either substantiate or invalidate the allegations. Relevant data can be scattered across IT systems and geographies, and may take time to collect, consolidate, and assess.

Establish a clear message

It is vital to develop a clear message for external communications. We recommend aligning any communication or publication with senior management stakeholders, the central task force, and the institution's press office.

Ensure a single line of communication with the prosecutor and/or regulator

A central task force should be set up to orchestrate activities. It should be responsible for the following key functions:

- A central point of contact to the prosecutor/regulator
- Coordination of internal efforts
- Involving relevant departments
- Checking data transferred to the prosecutor/regulator for quality, comprehensiveness, and consistency

C Cybercrime: A Risk Too Significant to Ignore

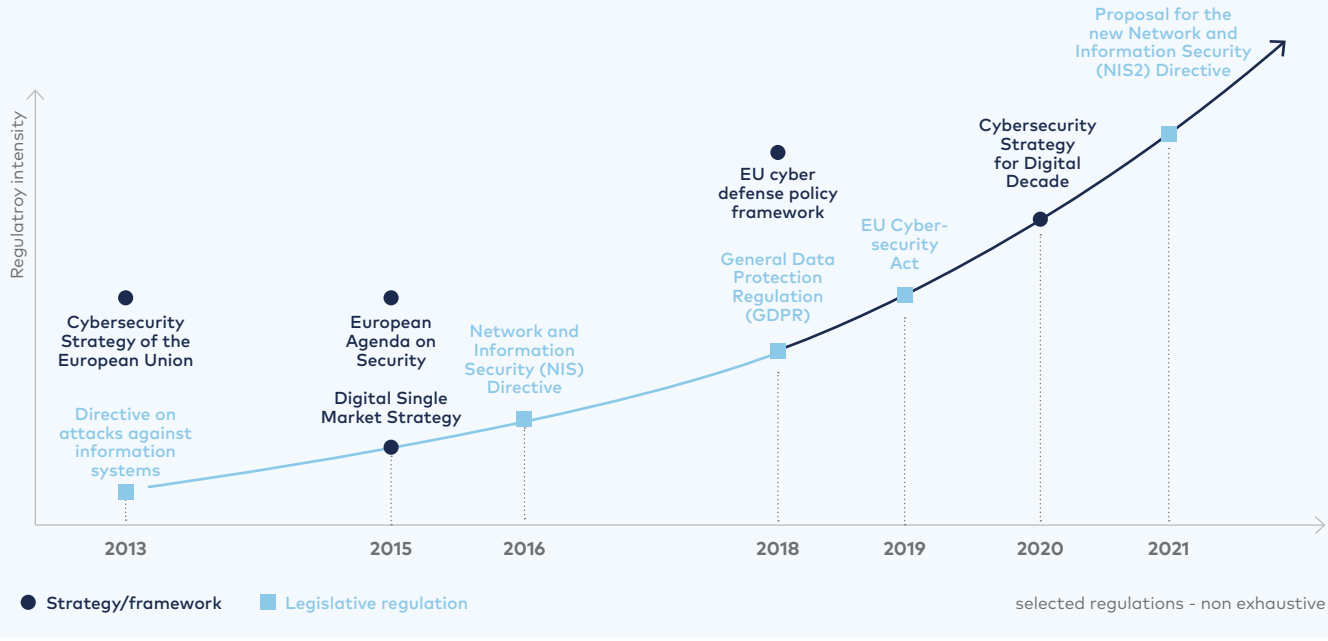
Evolving risk in a digital world

Corporations across the globe are being targeted by cybercriminals at an alarming rate. In 2019 there were ~32,000 corporate cyber security incidents worldwide.[7] Given these figures, it is easy to see why cybercrime is broadly viewed as the single biggest threat to companies worldwide.

A data breach can cause long-term legal and economic consequences. Not only can cyber criminals obtain comprehensive access to personal or financial data, business secrets, and other confidential information; cyber incidents can easily disable entire systems, leading to massive operational disruption. In addition, incidents often lead to reputational damage and affected customers are increasingly litigious.

Many countries, particularly in Europe, have recently tightened data protection rules – resulting in stricter enforcement. Under the EU General Data Protection Regulation (GDPR), companies that process personal data must implement technical and organisational measures to ensure a level of security appropriate to the risk (See Exhibit 4). A dereliction of this duty often triggers significant fines and claims for damages. Corporations are usually also obliged to notify supervisory authorities and individual data subjects. As a result, cybercrime incidents often lead to massive data loss, expensive lawsuits from aggrieved customers, and heavy regulatory fines.

EXHIBIT 4 | Intensifying cybersecurity regulation over recent years



7. Verizon 2020 Data Breach Investigations Report, p. 40

Cybercrime costs spiral

The cost of global cybercrime is expected to grow by 15 percent a year over the next five years, reaching $10.5 trillion annually by 2025, up from $3 trillion in 2015. This would amount to one of the greatest transfers of economic wealth in history. Indeed, if it were a country, cybercrime would be the world's third-largest economy after the U.S. and China. The rising cost of cybercrime is reflected in the immense growth of the global cybersecurity market. In 2004 it was worth $3.5 billion, rising to $120 billion by 2017.[8]

CASE STUDY • **A corporate cyber hack**

A multinational B2C business becomes aware that hackers have been able to access individual customer accounts in different jurisdictions, but the intention of the hackers is still unclear. Regulators across the globe contact the company, while affected individuals speak to their lawyers. It turns out that a third-party vendor accidentally left open a "back-door", which allowed bad actors to access individual customer accounts.

Cyber-crime key facts

- The first 24 hours following a data breach are critical. Corporations must comply with strict notification and disclosure requirements, which may trigger follow-up investigations by regulators across the globe. Proper incident planning and war gaming are key, and decision makers should always bear in mind the international dimension.
- Data litigation and mass claims are on the rise and can impact companies across various jurisdictions. In instances in Europe, affected individuals have been awarded several thousand euros – a significant risk to the business if many individuals are affected.
- Europe is a high-risk landscape due to its stringent data protection regulation and turnover-based fining models. But challenges in the U.S., Asia and the rest of the world should not be underestimated. Some regulators are intensifying their collaboration. both on a national and international level. Getting a consistent message out while maintaining legal privilege of internal investigation results will be key to mitigating regulatory risk and follow-on litigation.
- Data breaches often trigger spin-off investigations, with regulators assessing compliance on a holistic level. This potentiality should be considered when implementing remediation measures.
- Regulators are often influenced by hindsight when evaluating the appropriateness of security measures. Proper documentation of technical and organisational measures, and related risk assessments, are therefore vital. Cyber-risk can be mitigated proactively by conducting regular technical risk assessments and by procuring cyber insurance coverage.
- Regulators expect data and cyber due diligence in the context of M&A transactions and related integration.

How to respond to a cyber-attack and become more resilient

Corporations should carefully manage their initial response and establish a target operating model to ensure long-term resilience.

8. Source: Cybersecurity Ventures

Mobilise your Response Team

Corporations should mobilise Cyber Security Incident Response Teams (CSIRT) immediately following any attack. In some cases, this will include activation of established arrangements with cybersecurity providers. Research has shown that the establishment of a CSIRT, including corresponding incident response procedures, can reduce the cost of data breaches by an average of 40 percent. The team should have regular global check-ins to ensure alignment and coordination. In order to contain damage, the team should conduct initial investigations to preserve evidence. It should also report to various regulatory authorities where required.

With regard to reporting obligations a tactical balance as how to prioritise Data Protection Authorities (DPAs) and other regulators/agencies and what to share with whom and when is key. Special consideration should be given to the likelihood of enforcement across jurisdictions, and which jurisdiction may be most significant from a business perspective. Businesses should be aware, however, of greater co-ordination between regulators, for example DPAs, law enforcement and cyber agencies.

Prepare for the investigation

Corporations should define procedures, checklists, and the requirements of any internal investigation in advance. Businesses must keep in mind that careless or non-compliant action after a security incident can lead to important evidence being inadvertently destroyed or deemed inadmissible to court. Furthermore, they should consider the impact of any right to information, either from the press, individuals, or a competitor. Corporations must be aware of the privilege status of their investigations/documents. Putting a wall between forensic teams may be advisable, particularly if one investigation is legally privileged and others are not. In this context, DPAs will assess the privilege of reports against local DPA privilege standards and not the standard where they were created. However, there may be some leeway for negotiation on this.

When identifying suitable forensic experts, it is important to assess whether they may have any conflict of interest – for example, if they have previously advised on the organisation's data security measures.

Plan your recovery

Immediately after the initial response has been completed, focus should turn to recovery procedures. In parallel, the business should perform a root cause analysis, aiming to identify the underlying security gaps that allowed the cyber incident to occur in the first place. Additional forensic experts may be required to assess any shortcomings in data security.

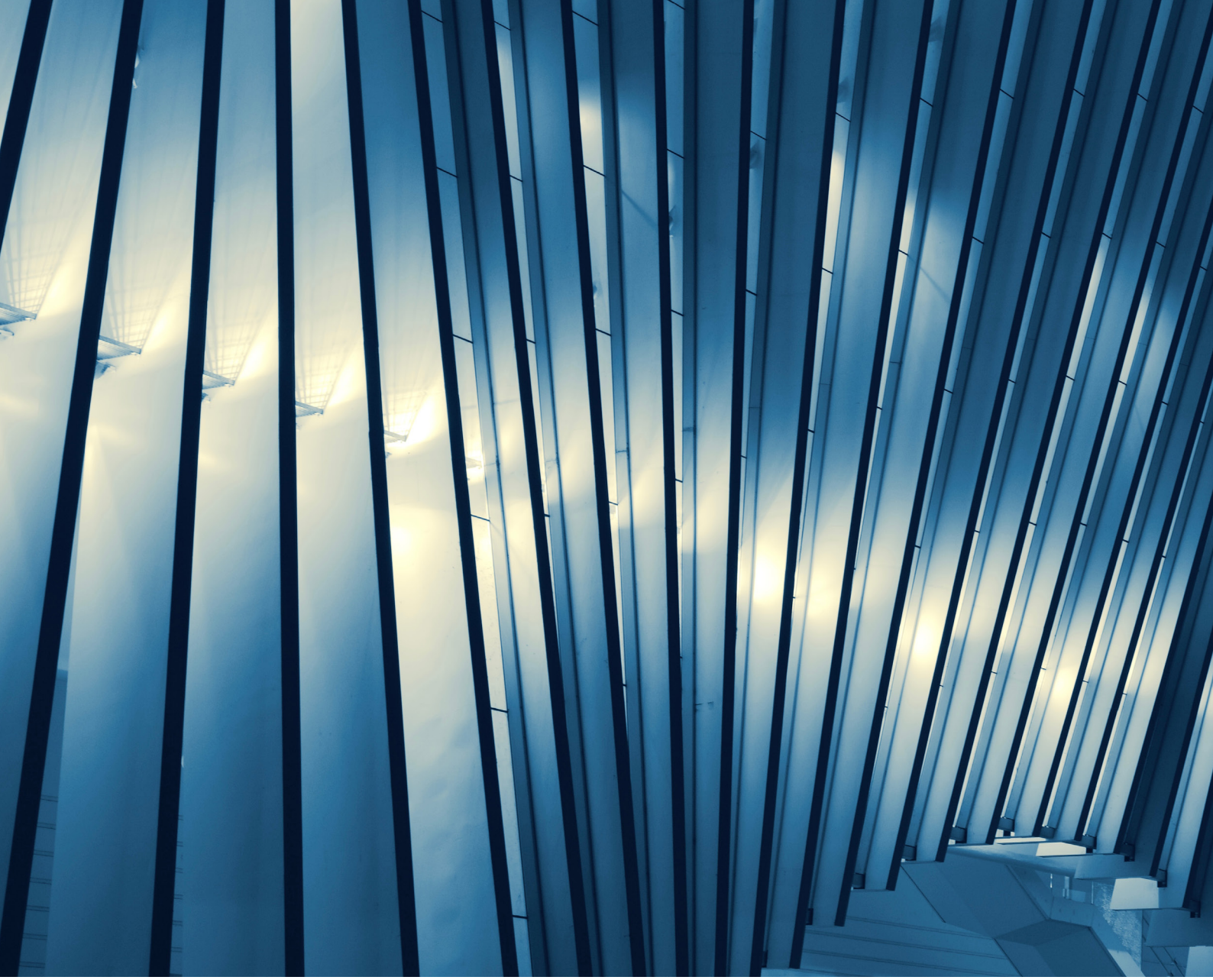
Ensure long-term resilience

To build resilience against cyber-attacks, corporations can rely on established industry standards (for example, from the National Institute of Standards and Technology (NIST) or International Organization for Standardization (ISO)). These standards specify the technical, organisational, and physical controls that should be implemented to prevent, respond to, and recover from a cyber-attack.

In parallel, these controls should be embedded within a broader context, to account for a corporation's specific business and operating model. For this reason, we recommend the establishment of a "Cybersecurity Target Operating Model", which will enable businesses to comprehensively address cyber-security risks (See Exhibit 5).

EXHIBIT 5 | **Cybersecurity target operating model – selected elements**

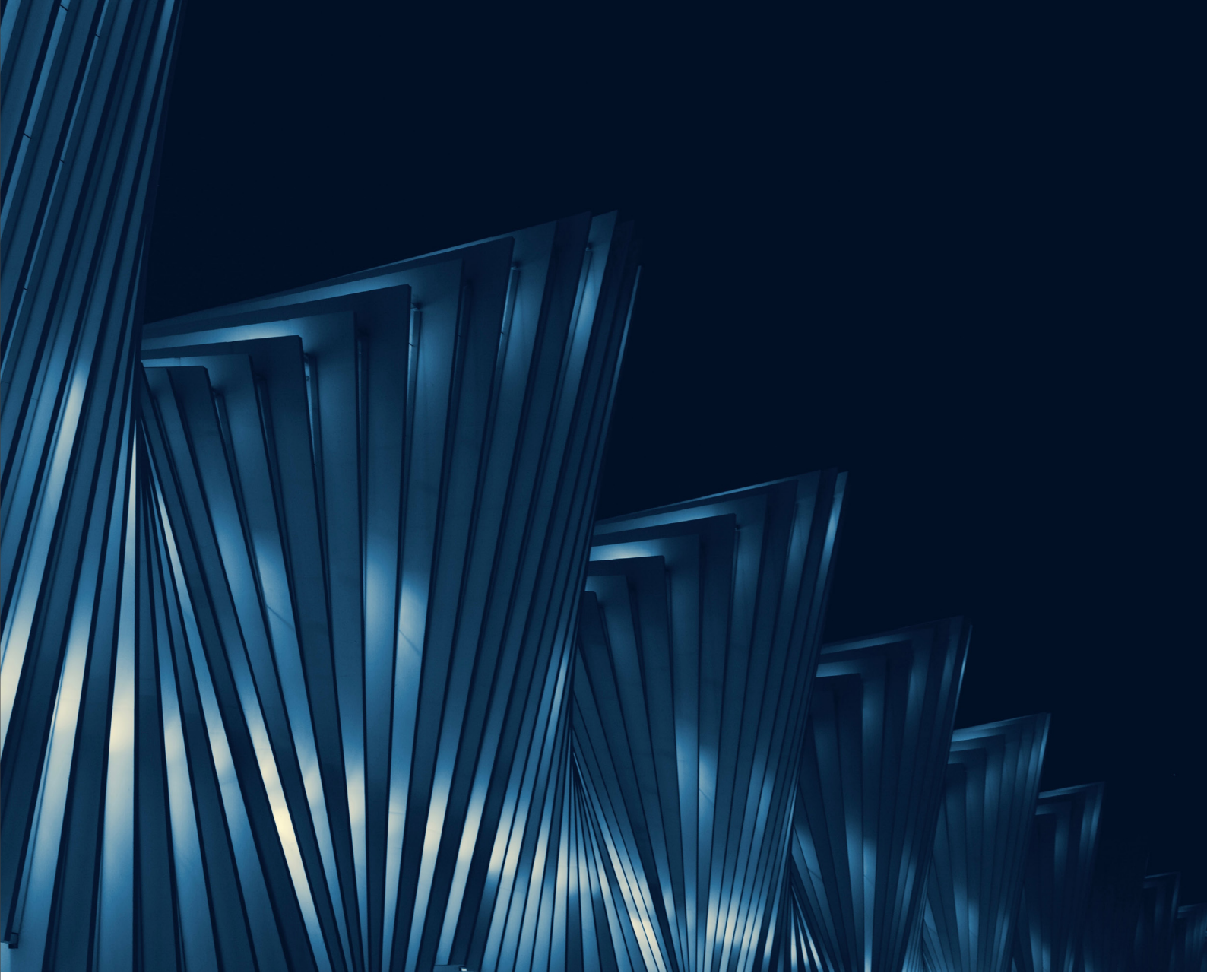
01	IS Strategy	• Development of a company's overarching strategy towards cybersecurity • Definition of affected risk types and determination of a company's overarching risk appetite
02	Governance & Organisation	• Clarification of overarching roles and responsibilities for cybersecurity unit • Definition of relationships between 1st and 2nd LoD functions as well as group-wide steering mechanisms
03	IS Risk Management	• Establishment of risk management cycle to allow for active steering of cybersecurity risk • Identification of applicable regulatory requirements, assessment of risk exposure, and control implementation
04	IS IT Architecture	• Assessment of criticality for data and underlying IT assets to determine required cybersecurity levels • Derivation of corresponding cybersecurity control requirements and definition of secure design principles
05	Culture of Integrity	• Establishment of adequate cybersecurity awareness and collaborative culture among all employees • Establishment of adequate communication from senior management regarding importance of cybersecurity



The challenges described in this paper can be tackled effectively and efficiently via three key measures:

01

Implementation of a group-wide non-financial risk target operating model. Through this harmonised solution, corporations can manage their risks and be confident that they are meeting regulatory obligations. Indeed, non-financial risk management should be holistic, exploiting synergies across risk types (e.g., in methodology of risk assessments, control design and governance). This will also enable consolidated and comprehensive risk reporting.

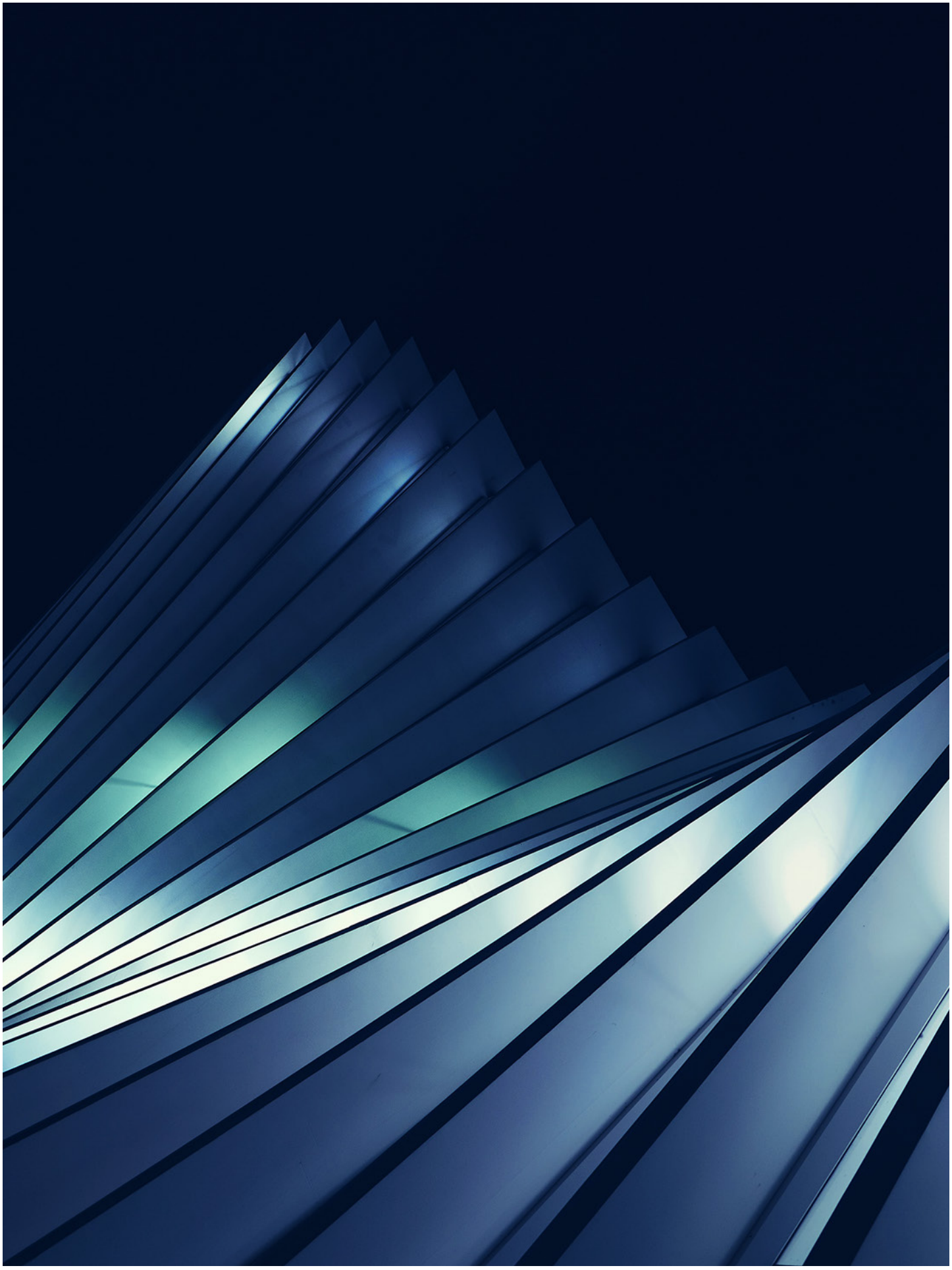


02

Beyond AML and cyber resilience identification of relevant non-financial risks based on business and operating model and implementation of adequate controls. In the banking industry, the ECB and local regulators already expect full transparency and sophisticated risk management solutions and for the non-financial industry this is only a matter of time.

03

Last but not least – culture is key. Corporations needs a common understanding of ethics and integrity, with the same set of do's and don'ts applied across business segments, entities and regions. This can only be achieved by constantly raising awareness in relation to compliance and its essential role in sustainable risk management. To hammer home the message, specific ethics and compliance awareness and culture initiatives are likely to be effective, both for senior managers and employees.



BCG BOSTON CONSULTING GROUP

Freshfields Bruckhaus Deringer