International In-house Counsel Journal
Vol.16, No. 63, Spring 2023, 1

On A Strategic Management Approach to the New EU Risk-Based Compliance Regulations

ANDREJ SAVIN
Professor of IT and Internet Law
CBS LAW, Copenhagen Business School, Denmark*
&
CONSTANCE E. BAGLEY
CEO, Founder, and General Counsel, Bagley Strategic Advisors LLC, USA
Visiting Professor of Law
CBS LAW, Copenhagen Business School, Denmark

Abstract

CEOs cite the rise of disruptive digital technologies at the top of the list of trends that have had the greatest impact on how they are now leading their organisations. Companies require advanced data analytics, better artificial intelligence-driven processes, and reliable cybersecurity to meet ever-changing threats. To remain competitive and compliant, it is essential that the top management team and the board understand the strategic implications of new and proposed EU regulations calling for risk-based compliance.

Although many law firms are creating new compliance departments eager to step in to serve as their clients' compliance team, compliance is too important a function to outsource. In-house counsel may seek outside advice to better understand how the regulations apply to aspects of their firm's business. But we submit that this sea change requires in-house counsel to work with management to develop a core managerial competency we call strategic compliance management. It may also require in-house counsel to work with national regulators to develop the rules of the road. For example, companies must proactively address demands for increased user rights, including transparency about how personal data are used, and become more skilled at managing the costs of compliance.

This article explores the key components of strategic compliance management and its application to new EU regulations. Our main premise is that in-house counsel must not only understand the effect of the new regulations on the formulation of firm strategy but also ensure that the regulations are met and that the strategy is coherent and offers sustainable competitive advantage. In-house counsel are well-situated to serve as trusted advisors committed to winning with integrity by not only helping to mitigate the risk of compliance failures but also by enhancing opportunities for value creation and capture.

1 Introduction

The European Union regulates the digital world comprehensively.[1] Recent years have seen not only an increase in the volume of that regulation (number of acts) but also an expanded scope (the number of subjects included), depth (the extent of the lawmaker's intervention), and compliance requirements affecting businesses. This creates uncertainties as businesses

* The authors are grateful to Jamian Smith, Chief Executive Officer, Arcana Solutions, for her insightful comments and help with this article.

[1] For an overview see Andrej Savin. *EU Internet Law*, 3rd ed. Edward Elgar, 2020.

face unfamiliar regulatory environments, new rules that need to be interpreted, unknown enforcement mechanisms, new regulatory agencies, and a fast-evolving environment relying on a combination of traditional regulation, delegated acts, and soft law.

The Importance of the EU in Digital Regulation

The EU regulation of the digital world is globally important due to the large volume of transatlantic, Sino-European, and other trade with the EU. Companies doing business with the EU have no choice but to familiarise themselves with the EU regulatory environment and comply. This is because European law poses direct demands on firms' products, services, or business practices due to its extraterritorial effect.[2] Digital regulation is also increasingly viewed as a trade barrier by non-EU governments.[3] Restrictions on cloud computing, cross-border data flows, wide platform regulation, and other digital issues feature high on any non-EU firm's priority list.

The virtual and digital nature of many products, platforms, and services, coupled with the complexities of modern supply chains, also puts stringent requirements on both EU and non-EU firms' management and their legal teams. Not only is an enterprise likely to be affected by EU rules the moment it has European customers, but it may, due to the opacity of its supply chain, be affected without its management's knowledge.

Dynamic regulatory environments such as the EU present unique challenges for managers. They can include rapidly changing and occasionally broadly written laws, uncertain interpretations that often end in years-long legal battles, new regulatory agencies with increased powers, and the need to comply with a very diverse set of laws governing business functions ranging from e-commerce, consumer protection, and data protection, to telecommunications and sector-specific rules on new technologies.

Law & management as an approach[4] starts with the idea that there is a direct link between law, value creation, risk management, and strategy[5]. Law helps shape the competitive environment and affects each of Porter's five forces; legally astute managers can strategically use law as a source of competitive strategic advantage.[6] Dynamic regulatory environments require constant threat assessments and the ability to proactively work with regulators to define this landscape and to do so in a transparent and responsible manner.

Note that this model disrupts traditional notions of corporate governance, risk management, and compliance. Compliance today—traditionally seen as observance by firms of rules created externally by legislators or administrative agencies—does not fit traditional models of corporate governance but forces changes in a firm's internal governance structure from the outside.[7] Compliance is increasingly also an exercise in risk management.[8] At the same time, legally astute managers can strategically use aspects of the new regulatory reality in the digital world to the firm's legitimate competitive advantage.

A modern company is necessarily digital in one or more of its aspects: digital presence (email, social media accounts), sales practices (orders, deliveries, supplies), payments, and

---

2 See GDPR Art. 3, DMA Art. 1(2) or DSA Art. 2(1).

3 US Trade Representative, 2023. National Trade Estimate Report on Foreign Trade Barriers, https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.

4 Constance E. Bagley, 'Winning Legally: The Value of Legal Astuteness' (2008), 33 *Academy of Management Review* 378.

5 Constance E. Bagley, *Winning Legally: How to Use the Law to Create Value, Marshal Resources, and Manage Risk*. Boston, Massachusetts, USA: Harvard Business Review Press, 2005.

6 Constance E. Bagley, 'The value of a legally astute top management team: A dynamic capabilities approach' *in The Oxford Handbook of Dynamic Capabilities* (David Teece & Sohvi Heaton, eds.). Oxford, United Kingdom: Oxford University Press, 2016.

7 See Sean J. Griffith, 'Corporate Governance in an Era of Compliance' (2016) 57 *William & Mary Law Review* 2075.

8 On the connection between governance, risk management and compliance, see Geoffrey Miller, *The Law of Governance, Risk Management, and Compliance*. Kluwer, 2020.

the like. Although the new EU rules are relevant for intermediaries, digital actors, and platforms, they are also important for all businesses for the simple reason that platforms enable customer reach and lower transaction costs, and they play a crucial role in the value chain. Companies must adjust their strategies whether they view the rules as company-friendly or not.

The Impact of New EU Regulations on Business Strategy

The method of EU digital regulation has changed significantly in recent years. The new rules affect business strategy for both EU and non-EU firms in two fundamentally different ways. First, businesses themselves are subject to the rules in as much as they fall under the scope of new EU framework instruments and sector-specific laws in the digital sector. Second, because businesses depend on platforms, the behaviour of platforms affects business strategy for other firms.[9]

While customers believe that platforms should protect users and promote safety, businesses prioritize the limitation of their liability and focus on designing platforms that can be proactive in moderating risk. While businesses strive to do this, they also need to keep costs low and remain competitive in EU and other markets. Clear procedural obligations with known penalties for platforms create a climate of certainty, but businesses perceive overregulation of platforms as undesirable as it decreases business opportunities. Consistent rules like the EU Digital Services Act (DSA) help create a level playing field for businesses by furthering this balance.

Enabling the Balance Between Protection and Competition

First, there has been increased platform regulation, increased consumer/user protection requirements, and demands for improved cybersecurity. Traditional EU digital regulation, largely formulated in the early 2000s, rested on the idea that there should be no 'regulation for regulation's sake' and that the Internet should not be regulated like other networked industries. This laissez-faire approach has now been replaced by complex and demanding rules. The new laws, including certain sector-specific ones discussed below, do not just present more regulation but have groundbreaking features that require adjustments in strategy. Five are of note: asymmetric legislation, Ex Ante Approach, risk-based legislation, increased uncertainty in enforcement, and uncertain interplay between sources.

Asymmetric regulation means that different platforms are regulated differently with progressively more onerous obligations imposed on the largest gatekeeping platforms. This brings more flexibility but also more uncertainty. Ex Ante approach is a new method of regulation already present in the EU Digital Markets Act (DMA) and the proposed Artificial Intelligence (AI) Act. It imposes restrictions on dominant gatekeeping platforms in danger of abusing their positions. Contrary to ex post regulation, this approach applies before an actual violation occurs and in anticipation of the same. The new models of enforcement mean new national and EU regulatory bodies but also the presence of delegated acts that further complicate the regulatory milieu. Finally, the multitude of regulatory sources decreases regulatory clarity.

The second and possibly the most important development is the increased compliance obligations, in particular risk-based compliance, which is the main focus of this paper. Compliance is the act of conforming to rules, regulations, and laws set forth by the lawmaker, the regulatory bodies, or through industry standards. Compliance programs are implemented to ensure that an organisation operates within the boundaries of the applicable laws and regulations. Contrary to traditional compliance, which is conforming to rules supported by a sanctions system, and which comes in the binary comply/not-comply form,

---

9 Oxera, The impact of the Digital Services Act on business user, October 2020, available at https://www.euractiv.com/wp-content/uploads/sites/2/2020/10/Impact-of-DSA-on-EU-business-policy-paper-2020-10-20.pdf.

risk-based compliance requires that a risk-assessment process take place before a clear picture of what needs to be complied with is formed. In particular, risk-based compliance requires management to identify the specific risks facing an organization, to assess the magnitude and likelihood of those risks, and to implement measures to manage and mitigate those risks.

In the presence of the above, the In-house counsel team is often left with difficult choices as comprehensive risk-management programs must be integrated with business operations and be measured so they do not overly blunt the firm's competitive edge by making it overly risk averse.

2 New EU Digital Risk-Based Compliance Regime

The four main EU digital framework directives require risk-based compliance. They are the General Data Protection Regulation (GDPR)[10] , the Digital Service Act (DSA)[11], the proposed AI Act[12], and the Network and Information Security 2 (NIS2) cybersecurity directive.[13] Each deals with a fundamental aspect of digital business: data, platform economy, AI technologies, and cybersecurity. Each brings a sea change in its own area but each is also of general importance for any firm, not just the ones dealing in digital products or services. The risk-based compliance regulations look different for different entities—creators, collaborators, retailers, and consumers. The lack of clarity about where the responsibility for compliance lies is a challenge that is not easily resolved but is one that can be mitigated through strategic management of the firm's business landscape and its value chain.

At the centre of the risk-based approach to regulation is a simple idea: the risks in various regulated industries differ and efforts should be concentrated on identifying and mitigating the most serious ones. Risk-based regulation is both an attempt to target risks and to give a proportionate response to them. The challenges of risk-based compliance include uncertainty, the complexity of the digital sector, the ever-changing nature of digital regulation, and the difficulty of keeping up with it.

There are two basic approaches to risk-based regulation: bottoms-up and top-down,[14] depending on whether the risk evaluation is defined in law or not. The choice of the method has an impact on the burden imposed on in-house counsel. The bottoms-up approach, seen in GDPR, leaves the compliance mostly in the hands of the regulated entity. In contrast, the top-down approach mandates actions to be taken in case of identified risks.

2.1 Data Protection

The General Data Protection Regulation,[15] a de-facto worldwide standard for personal data protection, introduced high standards for personal data protection, significant fines, and new compliance requirements. Although well-known for its stringent compliance requirements, it was the first digital law to also base some of its most important provisions on risk assessment.[16]

---

10 Raphaël Gellert, *The Risk-Based Approach to Data Protection* (Oxford, UK: Oxford University Press 2020).

11 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277/1, 27.10.2022.

12 Proposal for a Regulation, Artificial Intelligence Act, COM (2021) 206 final, 21.4.2021.

13 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) OJ L 333/80, 27.12.2022.

14 Giovanni De Gregorio and Pietro Dunn, 'The European risk-based approaches: Connecting constitutional dots in the digital age' (2022), 59 CMLR 473-500.

15 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1, 4.5.2016.

16 See Rapahel Gellert, 'Understanding the notion of risk in the General Data Protection Regulation' (2018), 34 *Computer Law & Security Review* 279.

Data Protection by Design and *Data Protection by Default* are key concepts which incorporate risk assessment.[17] These demand that appropriate 'technical and organisational measures' designed to implement data-protection principles be put in place. Controllers must also ensure that only data necessary for each specific purpose are processed. In other words, data protection needs to be "built into" the products and services, and firms must take a minimal approach to data collection. Crucially, this is to be done considering "the risks of varying likelihood".

When 'a high risk to the rights and freedoms of natural persons' results from data processing using new technologies, Article 35 mandates that a data protection impact assessment be conducted. Three cases, each prevalent in modern economy, are specifically mentioned: automated data processing and profiling, special categories of data, and systemic monitoring of public areas.

Risk assessments in GDPR are not concentrated only on cybersecurity or risks of theft but also on accidental or unlawful destruction, loss, or disclosure. In other words, they are about creating business models where data can lawfully, meaningfully, and ethically be made to work to the firms' benefit.

2.2 Digital Service Act

The Digital Service Act is one of the two acts (the other being the Digital Markets Act) that change the EU framework for platform regulation. A comprehensive instrument, it takes the asymmetric approach, gradually increasing the obligations to which platforms are subject.

The EU Commission, under the DSA, can define 'very large online platforms' and 'very large online search engines'[18] and subject them to the highest tier of obligations. This includes risk-assessment (Article 34), risk mitigation (Article 35), and the following system of sanctions. As of February 2023,[19] twelve companies with seventeen services seem to be the target of Commission's designation, including Alphabet and Microsoft in search; Alphabet, Meta, Microsoft, ByteDance, Snap, Pinterest, and Twitter in social media; Alphabet and Apple in app stores; and Amazon, Alphabet, Alibaba, and Booking in markets.

These providers are required to 'identify, analyse and, assess any systemic risks in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services.' The risk assessment is conducted at least on a yearly basis and must take severity and probability into consideration. Article 34 provides that the following systemic risks must be taken into consideration:

- the dissemination of illegal content
- negative effect on the exercise of fundamental rights
- negative effects on civic discourse and electoral processes, and public security
- negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.

---

17 Article 25 GDPR.

18 Defined in Article 33 as those that have a number of average monthly active recipients in the EU equal to or higher than 45 million.

19 Martin Husovec, 'The DSA's Scope Briefly Explained' (20 February 2023). Available at SSRN: https://ssrn.com/abstract=4365029 or http://dx.doi.org/10.2139/ssrn.4365029

Services that must be taken into consideration are:

- the design of their recommender systems
- content moderation systems
- terms and conditions and their enforcement
- ad presenting and selecting systems
- data related practices.

Similar to the NIS2 below, DSA imposes special governance obligations on the company management. Article 41 obliges large platforms and search engines to establish a compliance function, independent from their operational functions and composed of compliance officers. This needs to have 'authority, stature and resources' but also access to management. The management bodies are given specific obligations in this respect.

The DSA is important for two reasons. First, it imposes stringent requirements on the largest platforms, attempting to create a safer space for users and a level playing field for businesses. This means that businesses and users alike can be more reliant on platforms because the platforms are now forced to act more responsibly. This should reduce the risk for everybody now that a Big Tech competitor must pay a penalty if it imposes an additional cost on other market players through the Big Tech competitor's unfair or uncompetitive behaviour. Second, even in cases where risk-based compliance is not mandated by the Act itself (because of the low threshold), the risk identification and risk mitigation mechanisms prescribed in the Act are de facto blueprints for risk-based compliance that smaller firms need to engage in.

2.3 The Proposed AI Act

The development and implementation of AI-based solutions in modern businesses is rapidly expanding. EU legislators, among the first globally, proposed an autonomous act on AI. The AI Act takes a risk-based approach in proposing rules on the placing of AI-powered products and tools in the market as well as the use of AI systems. The Act applies not only to both the providers and the users of AI systems located in the EU but also to products and services where the 'output produced by the system' is used in the Union, expanding the scope of the Act significantly.

The AI Act bans certain technologies outright. Among these are systems that deploy subliminal techniques, those that exploit group vulnerabilities, and systems using a social score.[20] Other systems[21] classified as high-risk are listed in Annexes of the Proposal and include:

- biometric identification and categorisation
- management and operation of critical infrastructure
- employment
- essential private services and public services.

Unlike the bottoms-up approach in GDPR, the AI Act creates a top-down list of obligations to be complied with. Article 9 demands the establishment of a risk-based management system. This is a 'continuous iterative process run throughout the entire lifecycle of a high-risk AI system,' including the identification and estimation of risk and adoption of risk-management measures. This group of systems is subject to a wide spectrum of obligations including human oversight, transparency, cybersecurity, risk management, data quality, monitoring, and reporting obligations. Article 10 imposes data governance requirements for techniques involving the training of models with data. Penalties are high: fines up to the greater of €30 mil. or 6% of global revenue.

[20] Article 5.
[21] Article 6.

Although the scope of obligations imposed on the users is somewhat narrower than those to which AI producers or those who put AI systems on the market are subject, the risk management that Article 9 requires is impossible without the user's input and without a tighter cooperation of the producer and the company user.

2.3 Cybersecurity

Governments and the private sector need to protect their infrastructure more than ever before. Cyberattacks are getting more frequent and more of them target key infrastructure in society. The trends show that cybercriminals are motivated by monetisation, with ransomware as the prime threat and a surge in public sector breaches.[22] The NIS2 Directive is a continuation of the efforts in the first NIS Directive[23], which obliged certain operators of essential facilities and digital service providers to introduce security obligations and notification systems. It was a limited but significant step in improving cybersecurity. The NIS2 Directive[24] follows NIS1 but requires better training and better incident reporting, but, most of all, improved overall cybersecurity.

The Directive applies to essential and Important entities (listed in Annexes I and II) that carry out activities in the Union and meet the threshold requirements for medium enterprises. Irrespective of the size, the Directive applies to telecommunications, sole providers of critical services and in other situations, public administrations and central governments. Sectors of high criticality are energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, and public administration. Other critical sectors are postal, waste management, chemicals, food production, manufacturing, digital providers, and research.

The exact number of entities included is unclear at this stage as Member States have a small level of discretion in some listed cases but also because direct suppliers in the supply chain are included.[25]

Article 21 of NIS2 obliges the entities to consider state-of-the-art, EU, and international standards to ensure a level of network security 'appropriate to the risks posed'. Exposure to risk, entity's size and the likelihood of incidence occurrence all need to be taken into consideration. The "all hazards" approach is taken (Article 21 NIS2), which requires that the full scope of potential emergencies or disasters be considered when preparing for and developing responses, including:

- incident handling
- business continuity
- supply-chain security
- security of network
- risk management
- human resource security
- cryptography
- multi-factor authentication (MFA)

---

22 See ENISA, ENISA Threat Landscape 2021, October 2021, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

23 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L194/1, 19.7.2016.

24 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333/80, 27.12.2022.

25 The EC's impact assessment gives the current number companies under NIS1 as 15,500 and estimates the number of companies under NIS2 as about 110,000. Impact Assessment Report, SWD (2020) 345 final, p. 20 and 70. Danish Industries have recently estimated that 1079 Danish companies will be directly affected. https://www.danskindustri.dk/brancher/di-digital/nyhedsarkiv/nyheder/2023/2/ny-analyse-1079-virksomheder-pa-tvars-12-sektorer-ser-ud-til-at-blive-direkte-omfattet-af-nis2-direktivet/ .

Unique in the new directive is supply chain risk management. Not only is the company obliged to risk-assess its own operations, but also those of its 'direct suppliers or service providers' in the supply chain. The vulnerabilities specific to each direct supplier are to be considered as is the 'overall quality of products and cybersecurity practices'.

The national supervision consists of on-site inspections, random checks, and independent security audits. Ad-hoc audits can be ordered in cases of security breaches or non-compliance, but national authorities can also issue fines or suspend or ban entities or their managers. The fines for essential entities can be up to the greater of €10 million or 2% of worldwide turnover and up to the greater of €7 million or 1.4% of worldwide turnover for important entities.

As part of the new EU interest in governance of digital issues, NIS2 orders EU Member States to ensure that the management bodies, such as boards of directors, approve the cybersecurity risk-management measures taken by those entities on risk compliance, that they 'oversee its implementation', and that management bodies can be 'held liable' for infringements.

The in-house counsel is thus responsible for complex risk assessments of its own company's operations as well as those of direct suppliers. Risk ownership is placed at company management level and measures at state-of-the-art level are recognised as standard. Although the significant fines should serve as a deterrent, the main motivation should be that sound cybersecurity is good business.

3 The Role of In-House Counsel as Partner with Board and Top Management Team Engaged in Strategic Compliance Management

The increased use of artificial intelligence, reliance on data analytics, the growth of cloud computing, and the increased use of new technologies, such as the Internet of Things (IoT), blockchain, fintech and other developments, challenge the in-house counsel's role. Their interplay require in-house counsel and management to work together proactively to a heretofore unprecedented extent. The key observation is that the concept of compliance has evolved from the days when the in-house counsel's job was primarily helping companies to 'tick off' a checklist of rules provided by the regulator to a dynamic and challenging process requiring the in-house counsel to play an active role as a partner with the board and top management team engaged in strategic compliance management. Companies wanting to place products and services in European markets have no choice but to simultaneously pay attention to regulator demands and help develop competitive, yet ethically-sound, products and services. In short, the risk-based compliance requirements outlined in the preceding sections require in-house counsel to collaborate with management not only to make sure the many and diverse rules are respected but also to create value and ensure sustainable competitive advantage.

Compliance Management as a Strategy

Although it may be tempting to outsource compliance, this is often not a reasonable strategic move. There are two main reasons for this. One is that risk-based compliance requires an interplay between different departments in the company, constant managerial involvement, and active cooperation with regulatory agencies—all of which are more difficult to achieve when outsourcing. The second and even more crucial reason is that reducing the risk of sanctions, loss of reputation, and the like resulting from non-compliance is achieved not through simple compliance but through compliance management, which requires integration with company, and often product, strategy. It is equally important not to put too much confidence in the emerging AI risk assessment tools. Although these may be useful, lack of critical scrutiny of their results and recommendations may lead to increased risk, as these tools may rely on premises and research that is incorrect at best and wholly fictional[35] at worst.

Furthermore, strategic compliance management depends on the size of the firm, its business model, and its supply chain. Knowing when to use in-house counsel is crucial. Large companies have considerable resources in creating strategic compliance models. They have the financial power to use large legal teams. They are often able to analyse and process the laws and quickly come to workable solutions after understanding the impact the regulation will have on their products and services. Smaller firms may not have resources for this, but should not fall into a trap of believing that all problems can be solved with outsourcing or buying software solutions. Management for smaller firms must consider an even more hands-on approach, utilizing outside counsel to help create their internal compliance management programs;robust measurement, oversight, and continuous improvement must be key characteristics of these initiatives. On top of this, joint ventures, partnerships, and subcontracting arrangements need special considerations as each presents unique challenges, such as shared liability, conflicting approaches to data security and privacy requirements, and lack of visibility to individual company compliance practices.

Next, the role of in-house counsel needs to be reconceptualised. As Bagley points out,[26] strategically astute counsel understand business fundamentals, the applicable law, and the appropriate use of both managerial and legal tools. In-house counsel needs to be directly involved with the top management in the strategy formulation process and not act as the last port of call in times of trouble. Legally astute managers need to involve in-house counsel at all stages of development rather than as an exception. Strategically managing risk-based requirements requires closer collaboration between data protection officers, chief information security officers, and heads of compliance. Better cooperation between compliance officers and the management is needed as the consequences of the lack of this collaboration are very costly.

Finally, a crucial element of strategic compliance management is the link with regulatory agencies. Compliance often derives from the regulatory agencies that interpret the laws. It is very rare that there is a direct link between passed laws and compliance requirements. This, in turn, means that an active relationship with the regulatory agencies to promote common understandings of the regulatory requirements is a necessary element of modern strategic compliance management. A significant increase in the number of delegated acts is one of the additional reasons. This enables the firms to understand what is required of them but also to keep one step ahead of the competition. This is even more the case as the number of the relevant agencies is increasing and so are the complexities of their relationships with regulated firms. Frequently, the regulatory oversight over just one agency is given to several authorities, all of which need to be worked with.[27]

The sooner organisations adapt to the EU regulatory reality, the greater their success will be. Identifying and assessing the risks that an organisation faces and taking steps to mitigate those risks are only the first and natural steps in the process and so is keeping up with the latest regulations and providing adequate employee training. What will define the success of the in-house counsel in managing digital compliance, however, will be their ability to form meaningful relationships with the top management and the Board.

---

[26] Constance E. Bagley, 'The value of a legally astute top management team: A dynamic capabilities approach' *in The Oxford Handbook of Dynamic Capabilities* (David Teece & Sohvi Heaton, eds.). Oxford, United Kingdom: Oxford University Press, 2016.

[27] In Denmark, for example, regulatory oversight of the old NIS Directive was in the hands of the Business Authority while the security reporting was in the hand of the Center for Cybersecurity. The lists of covered entities was in the hands of the Trade Minister while that of financial institutions' cybersecurity was with the Financial Authority.

4 Role of Management

It is the duty of top management to ensure compliance with law. This can no longer be understood as a simple exercise of guaranteeing that everything that comes from the regulator must be followed in a mechanical way—nor, indeed, that following it would always guarantee that the firm is compliant—because new EU compliance is based on risk assessment. Instead of just mechanically following the letter of the law, companies need processes for strategic compliance management designed to help them reduce the risks of illegal behaviour, reinforce ethical conduct as a core value, and enhance the company's reputation as a good corporate citizen in the eyes of both regulators and stakeholders.[28]

Strategic compliance management as a concept rests on the idea that risk-based compliance is a dynamic process ensuring that regulations are met and that the firm strategy is coherent but is also a process that offers sustainable competitive advantages to the firm. Strategic compliance management ensures that:

- firms understand the effect of the new EU regulations on the formulation of firm strategy
- the firm adequately assesses the risk in those EU laws where risk-based compliance is demanded
- the firm complies with the spirit as well as the letter of the rules
- adequate dialogue and cooperation with EU and national regulatory agencies is maintained.

Strategy expert David Teece has argued that dynamic capabilities are the firm's ability to 'integrate, build, and reconfigure internal and external competences to address rapidly changing environments' and can be valuable sources of competitive advantage.[29] No environments are more rapidly changing than those based on data-based business models and AI technologies. In such environments, managements have a duty to make strategic choices. They must assess the impact of new EU digital regulations but also investigate the opportunities that they provide. The task is not just how to create business models that do not violate data protection laws. It is also to create business models that actively rely on robust data protection. The mission is not just to avoid using illegal and risky AI models; it is also to identify and perhaps create the lawful ones. The management's task is to work with in-house counsel to reduce the risks and create realizable value. The message should be simple: if products or services are not core to the business and are high risk, they should be eliminated; everything else that can be managed should be managed through strategic risk management approaches with the aim of obtaining an advantage over competitors.

Management should be aware of two points that go beyond EU-demanded governance obligations that are a part of a good compliance strategy.

First, winning with integrity and compliance must be set by the tone at the top.[30] Failure to meet these high standards should result in sanctions, including termination. That extends to a CEO who harasses a subordinate or who cheats on expense reports. Not only do some of the key new EU laws demand top management's direct involvement, but the lack of management engagement remains one of the main triggers for big (and very costly) legal crises. Major crises involving violations of digital regulations are almost guaranteed when

---

28 Constance E. Bagley, Bruno Cova, and Lee Augsburger, 2017. 'How boards can reduce corporate misbehavior'. *Harvard Business Review*. https://hbr.org/2017/12/how-boards- can-reduce-corporate-misbehavior. December 21.

29 Teece, D. J., Pisano, G., & Shuen, A. (1997). 'Dynamic capabilities and strategic management'. *Strategic Management Journal,* 18(7), 509–533.

30 Alfredo Contreras et al., 'Tone at the Top and the Communication of Corporate Values: Lost in Translation'. 43 *Seattle University Law Review* 497 (2019-2020).

management does not play an active role and protect those courageous enough to speak up. Although big tech is particularly in regulator's scope,[31] smaller firms should also be alert.

Second, firms should appoint a chief compliance officer (CCO) who reports to the independent members of the board of directors. There is already evidence that CCOs are elite lawyers and that their role is taken seriously but evidence is also emerging that the profile of an ideal CCO is not always clear.[32] To this must be added the uncertainties concerning the use of compliance officers in smaller firms. For US companies, EU compliance may be entirely different in nature from domestic compliance.

Third, firms should craft company-specific compliance standards, mission statements, and codes of conduct and procedures, post them online, and provide training for all workers. These need to be EU-specific whenever EU customers are targeted. It is crucial that this task be taken up by the board and the top management team and not be treated as just a technical issue relegated to underlings. Interactive board training, preferably by the in-house counsel and chief compliance officer aided by a skilled outside facilitator, is critical.

It is often said that a company's management owes a duty of loyalty and duty of care to the shareholders. A more accurate formulation would be that the Board owes a fiduciary duty to the company and is responsible for good governance. The EU has squarely stated that the board is responsible for ensuring that the firm's compliance system conforms with the regulations and that board members should potentially be personally liable for compliance failures. Ideally, the board should have a governance and compliance committee.

Managers need to be legally astute. This requires a set of the value-laden attitudes about the importance of law and ethics to the firm's success, a proactive approach to legal issues, the ability to exercise the informed judgment, context-specific knowledge about the law and the application of legal tools, and partnering with strategically astute counsel. Applying these to new EU digital regulations leads to the following key management takeaways:

- Data regulations can be used to create customer trust. Adequately assessing the risks involved with data collection and processing and complying with GDPR is not only a burden but a business opportunity.
- The Digital Service Act creates a safer digital space for all platforms.
- NIS2 enables the creation of cyber-secure environments.
- The AI Act gives scope for the use of lawful tech and identification and use of lawful advanced analytics.

A more general conclusion, however, is that the exercise of informed and sound judgment is needed to decide which risks are worth taking and what methods are available to mitigate and monitor them. The EU risk-based regulatory framework helps firms develop the capacity to do this more effectively.

The obvious danger of a risk-based approach to regulation and compliance is its focus on the negative aspects of regulation and the increased likelihood that it will cause managers and their counsel to view compliance as just a constraint, just a burden, and not a source of value creation. Yet, studies show that companies that incorporate human resource and environmental compliance in their strategy-formulation process can attain a strategic edge over those that add them at the end, only after management has already decided on the firm's overall product, marketing, and human resource strategy. Pollution can be viewed

---

[31] Texas Attorney General Paxton recently sued Google, alleging that the tech giant has unlawfully captured and used the biometric data of millions of Texans without properly obtaining their informed consent. https://www.texasattorneygeneral.gov/sites/default/files/images/press/The%20State%20Of%20Texas's%20Petition%20(Google%20Biometrics).pdf. At the same time, Google faces a €25 billion legal action in the UK and the EU over its digital advertising practices. https://www.bbc.com/news/technology-62891769

[32] Miriam H. Baer, 'Compliance Elites'. 88 *Fordham Law Review* 1599 (2019-2020).

as a wasted resource.With a better planned value chain, it can be eliminated, reducing costs of production as well as the cost of scrubbers and other tail-pipe equipment. Similarly, failure to have a fair and nondiscriminatory hiring process will not only reduce the likelihood of employment discrimination lawsuits but also enhance the likelihood of hiring the best people for the job. Studies on the value of diversity and inclusion bear this out. Similarly, taking a risk-based approach to business opportunities encourages firms to reject or get rid of risky business propositions with low yields and concentrate instead on those with returns commensurate with risks that can be adequately managed.

Conclusion

Demand for cybersecure products is growing[33] as is that for AI solutions.[34] Successfully adopting strategic compliance management creates room for sound new businesses opportunities, but it is a process that requires continuous analysis of the emerging legal rules as well as market forces and the firm's resources. Trusted in-house counsel have a key role to play on all three fronts.

***

Andrej Savin is a professor of IT Law and Internet Law and Director of CBS LAW at Copenhagen Business School. His main research interests lie in Information Technology Law, and in particular EU policymaking in the digital single market, the regulation of new business models, and Internet governance in the US and in Europe. Andrej Savin also works on law and management in the legal environment, with a particular focus on the interplay between law, ethics, business, and society in the digital world. His works include *EU Internet Law* (3rd edition, Edward Elgar 2020), *EU Telecommunications Law* (Edward Elgar 2018), *Research Handbook on EU Internet Law* (2nd edition 2023), and others.

Constance E. Bagley is CEO, Founder, and General Counsel of Bagley Strategic Advisors LLC, USA (constance@bagleystrategic.com), and currently a Visiting Professor at CBS LAW, Copenhagen Business School, Denmark. A.B., honors and distinction, Stanford University; J.D., *magna cum laude*, Harvard Law School; honorary doctorate in economics, Lund University. Formerly partner, Bingham McCutchen LLP; member of faculty, Young Presidents Organization International University in Hong Kong and Prague; Senior Lecturer, Stanford University Graduate School of Business; Associate Professor, Harvard Business School; Professor in the Practice of Law and Management, Yale School of Management; Senior Research Scholar, Yale Law School. Professor Bagley taught for multiple years in the executive programs for directors and lawyers at the graduate schools of business at Stanford, Harvard, and Yale Universities. Students in the Yale MBA programme awarded her the Excellence in Teaching Award twice. She is the author of numerous articles and books, including *Winning Legally: How to Use the Law to Increase Value, Marshal Resources, and Manage Risk* (Harvard Business Review Press, 2005), *Managers and the Legal Environment: Strategies for Business*, 9th ed. (Cengage Learning, 2019), and, with Craig E. Dauchy, *The Entrepreneur's Guide to Law and Strategy,* 5th ed. (Cengage Learning, 2018). She is also a Past President of the Academy of Legal Studies in Business.

---

33 McKinsey, 'New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers'. 27 October 2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers.

34 'The state of AI in 2022—and a half decade in review', 6 December 2022, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review.

35 Aaron Welborn, 'ChatGPT and Fake Citations', 9 March 2023, ChatGPT and Fake Citations—Duke University Libraries Blogs.