Deep Science Publishing
https://doi.org/10.70593/978-93-7185-253-1_12

DeepScience
Open Access Books

Chapter 12: Future-proofing compliance programs with blockchain, artificial intelligence governance, and predictive compliance engines

12.1. Introduction

Compliance programs exist to create a pathway to avoiding risks that can make your organization vulnerable. Minimum elements of compliance programs were established in the United States Federal Sentencing Guidelines. The Sarbanes–Oxley Act established compliance programs for publicly traded companies in the United States, mandated certain monitoring activities from external auditors, and imposed criminal liability for obstructing justice with respect to destroying documents that were relevant to any pending investigation with respect to federally insured financial institutions. Certain other laws impose similar requirements for their scope of activity. Various national government authorities have called for compliance programs in public and private companies and related entities to address risks of bribery and corruption. These requirements have often been incorporated in investment and funding agreements (Nabil, 2024; Das & Adhikari, 2025; Ponnusamy & Aruldas, 2025).

Compliance programs address areas of risk that vary from organization to organization and that develop over time given the nature of the organization's activities and its ongoing oversight of them, as well as changes in the applicable legal environment. Certain compliance risks traditionally include risk of money-laundering surveillance; maintenance of appropriate license and regulatory approvals; reporting of insider information; current private investment fund sponsor declarations and reporting exempt and non-exempt foreign sources of funds; export and trade compliance security screening; compliance with economic sanctions; consumer and commercial protection; defense procurement; compliance with other anti-corruption and bribery laws; compliance with diversity and related contractor oversight of minority and women-owned businesses; protection of data privacy; prevention of fraud; mitigation of foreign espionage; dissemination of intellectual property; equal employment opportunity;

misuse of position; disclosure of third party engagements and financial interests; money laundering governance; oversights on outside contractors; protection of security; trade secrets protection; and taxation compliance. However, they are not limited to these areas. Compliance risks are identified based on the activities of the organization and the applicable laws (Vashishth et al., 2024; Srivastava & Ghazala, 2025).

Fig 12.1: Future-Proofing Compliance Programs with Blockchain

12.2. The Role of Blockchain in Compliance

The first step in compliance 4.0 is to carry out compliance operations on blockchain networks. Whether it is risk assessment or due diligence or monitoring or audits, these activities can take place on the blockchain. The work from compliance 2.0 and compliance 3.0 can take place on the blockchain with improved efficiency or cost-effectiveness, but these improvements actually do not change the substantive nature of compliance work. Compliance 4.0 changes the nature of compliance work itself by implementing compliance features from the outset, by code. When compliance features are built into the actual structure of the blockchain, such features could be used to critically limit the need for compliance verification and reports, by assigned compliance actors or compliance engines. Globalization and digitization have altered the paradigms of compliance, by significantly increasing the volume, speed and complexity of systemic, unintentional and criminal violations of laws and norms. The limitations and tensions of compliance 1.0, compliance 2.0 and compliance 3.0 made a previous effort

to transform the nature of compliance from an ex-post activity into an ex-ante activity, by integrating compliance features into contracts and procedures. Compliance 4.0 extends this strategy and vision by defining compliance features that could be programmed into code. Compliance 4.0 carries the aim to support and monitor compliance requirements via automated, structured coding and tracking inherent to the blockchain – thereby reducing the need for ex-post reviews.

12.2.1. Understanding Blockchain Technology

Blockchain technology has emerged as one of the primary technologies heralded with the capacity to support stronger compliance programs within organizations. Yet, for the vast majority of people, conversations about blockchain tend to induce confusion after five minutes. This will be the first challenge for organizations starting to think through how to future-proof compliance using blockchain – getting knowledgeable feedback and guidance on the merits of the technology to consider its adoption and use.

The implications of blockchain are profound, enabling an erosion of the significant social trust required to have fully functioning societies, particularly those involving commerce. However, uses of blockchain are nascent, with few explorations into the socialization of its use. This is not unusual. The earliest uses of telecommunication devices made it possible to communicate more rapidly over longer distances. Over time, society decided on a set of telecommunication norms, guided by our need to cooperate and collaborate with one another socially and economically, and telephony developed into what we see today with mobile communication capabilities integrated into devices able to support multiple distinct uses.

Just as potential use of telecommunication devices predated our understanding of how society would integrate its use, blockchain's unique technical features are starting to bring about demands for compliance from participants in commerce. Blockchain generates an immutable, cryptographically secured ledger containing transaction data that is time-stamped, publicly viewable, provable, and impossible to alter without the consensus of other participants within that blockchain. Because of its unique technical features, blockchain heralds the new forms of finite, controlled trust required among parties unable to or unwilling to place that trust in a third party.

12.2.2. Benefits of Blockchain for Compliance

The compliance advantages of blockchain lie in its revolutionary record-keeping capabilities. Most compliance obligations have a record-keeping component: Companies must collect and store a variety of documentation in a readily auditable form. Blockchain

can automate many of these requirements, making creation, access, audit, and secure storage of that documentation less burdensome. No one would claim that blockchain makes record-keeping for compliance utterly simple. Blockchain would diminish, not eliminate, the load of documentation. Smart contract self-executed compliance with rules denoting those document standards would improve the efficiency of the record-keeping burden. The types of documents that transaction verification in the blockchain could cover are numerous. First, the timestamps. A time-stamped record that demonstrates a transaction occurred at a specific date and time strengthens a compliance case. Examples include when a contract is signed, steps in a transaction occur, or when an inquiry to a bank's compliance department is submitted.

Second, the verified terms of the agreement. Because transactions exist on a blockchain, the specifics of a transaction can be verified. If part of the compliance requirement is a unique, unalterable record that can withstand scrutiny, blockchain can provide that verification. Examples include employee non-disclosure agreements and records of confidentiality disclosures connected to contract negotiations. Third, the transactional partners involved in a transaction. Because transactions will only occur if the parties comply with the smart contract terms, this ensures the compliance process functions properly. Fourth, a complaint history. A transactional history can be made to provide proof of a pattern of behavior, as with money laundering or fraud charges. The benefits of blockchain record-keeping in compliance are two-fold. First, blockchain records should improve compliance with the financial regulations themselves, providing outside regulators with additional assurance against risk. Second, that blockchain audit trail should make any compliance audit conducted internally or by regulators more efficient and cost-effective.

12.2.3. Challenges of Implementing Blockchain

Despite the exciting potential and benefits of blockchain technology, however, companies need to be careful before rushing to implement it in their compliance program. Blockchain adoption for large enterprises comes with high overhead, including uncertainty over cost, the challenges of data integration, and a lack of consensus standards over how to best implement the technology. Enterprises with thousands of intercompany transactions each day should carefully consider the applicability of a blockchain solution to their compliance program. Questions that a company should consider include, but are not limited to, the following:

Are the transactions that the company is trying to validate on a regular basis sufficiently decentralized and numerous that creating a blockchain for the compliance program will provide noticeable benefits? The larger the network size and the more organizations involved, the more compelling the case for adopting blockchain for verifying

transactions. Does the company have sufficient transaction volume to drive blockchain economics? What would be the volume of transactions recorded on blockchain technology, be it inter-company and vendor trading transactions, validation of trade content and documents, or remittance, payment, or settlement of shipments? Would this volume justify the blockchain technology costs? How effective is blockchain technology for the specific use case? The optimum use cases for blockchain technology are where validation of identity and decentralized locations are required, allowing for secure and validated transactions. If validation of identity is handled by a third party or counterpart successfully today, how can blockchain assess the risks related to the transaction and, therefore, provide better advantages, become more efficient, or lower costs? What is the right governance model? A company implementing blockchain technology for compliance will need to think about how to determine access rules and permissions and what to do with participants who do not follow those rules. Designing the optimal governance system is critical for a successful implementation. Governance requirements are complex and will vary greatly depending on the market and geography.

12.3. AI Governance in Compliance

AI governance is becoming increasingly important as organizations scale their use of AI technologies. Broader industry trends are pushing compliance leaders to think about how AI will affect their compliance operations and organizational compliance profile. It is important to note that AI governance is categorized differently depending on the context. While sometimes understood broadly as composing all relevant policy and regulatory guidelines for AI design and operation, some contexts categorize AI governance more narrowly, as the internal governance initiatives around trustworthy, ethical, and legal use of AI in organizations. As organizations advance on their AI journey, compliance leadership needs to be part of the AI governance landscape. They need to understand the data, models, and processes used in AI; promote and support a culture of AI trust and responsibility; guide, coordinate, and regulate the different AI initiatives in the organization; and drive accountability around the performance of AI systems.

As compliance functions help organizations achieve business goals while minimizing risk, additional perspectives from compliance leaders can only further the wider AI governance agenda. Compliance functions can support existing AI governance in various ways. Compliance can help identify and classify compliance risks related to the development and use of AI, especially where different types and combinations of AI are used at scale. Compliance can further strengthen AI governance by promoting policies and processes that ensure compliance risks are mitigated, procedures are followed, and expectations around accountability for compliance are clear. Compliance can drive accountability by coordinating, enabling, and collaborating with other organizations

involved in AI initiatives. For instance, corporate compliance could work with risk management to establish global risk requirements for the organization's AI.

Fig 12.2: AI Governance in Compliance

12.3.1. AI Technologies in Compliance

Many compliance tasks rely on data-intensive processes, making them ideal candidates for AI tools. Businesses assess customer risk and evaluate sanctions lists and other watch lists for potential connections, or "hits." In addition to the basic architectures for AI technologies, such as generative AI, there are an expanding array of "compliance-native" AI tools that optimize the compliance process, some of which have reached a maturity level suitable for commercial deployment. For risk management, an AI-driven third-party risk management product prioritizes and contextualizes potential third-party risk scenarios, making it easier for compliance teams to efficiently assess and mitigate risks. For transaction monitoring, AI is employed to monitor every transaction in real time against user history and a wide variety of external factors to block fraudulent

transactions. AI is used to analyze user behavior, transactions, and other external factors to help detect account opening and bust-out fraud.

A large number of AI solutions are designed to improve the performance of KYC and AML compliance surveillance programs. These tools assess the quality of the underlying data, including the completeness of data fields, the accuracy of the data, and the quality of the provider, as well as the rules engine and the overall performance of the program itself. Companies with these tools include various providers. A related area is AI models that help AML compliance investigators prioritize alerts for review. An AI solution helps compliance teams streamline and automate alert triage processes by prioritizing AML alerts based on a variety of factors. Finally, AI tools that automate investigations based on business logic, including KYC and AML rule sets and risk assessments, are appearing in the compliance space.

12.3.2. Ethical Considerations in AI Governance

Artificial Intelligence (AI) is emerging in corporate compliance programs through both the use of AI technologies and the need for compliance in the AI decision-making process. Both avenues of AI implementation in compliance demand attention and preparation to avoid negative consequences at multiple levels. As with other technologies, using AI in corporate compliance services introduces ethical factors that must inform the compliance program design. An AI model is a probabilistic mathematical function connecting an input to an output. These models make predictions on responses that have derived from previous choices and are based on the inherent biases in the data on all prior decisions and outcomes.

To the degree that data reflects social conditions and institutions, these datasets may replicate unequal opportunities and ignore common ethical principles of fairness, justice, and equality. The prediction-powered decision draws on past choices using the same input variables and emits the same output variable, while an explanation-driven decision uses statutes and policies to weigh various input factors to make a specific verdict. As organizations deploy predictive decision models, there are increased risks of ethical violations since AI does not make morally/ethically driven decisions. In risk applications where predictive modeling is used to identify high-risk individuals or groups, organizations with predictive models are obligated to explain the basis of their predictions or signals when making decisions affecting the predicted person or group. Companies deploying predictive modeling tools should also plan for remedial processes that correct prediction errors. The ethical obligation to correct prediction errors may be triggered by the prospect of an illegal decision.

12.3.3. Best Practices for AI Implementation

One area that has received considerable coverage in the literature is principles and practices for the governance of AI systems. Such recommendations can be seen as a first step in the direction that we propose—namely evaluating AI models using compliance program models that include controls—that will allow compliance programs to treat AI outputs as the outputs of a controlled process. However, in the short run, dependence on principles and other recommendations will be necessary to ensure the proper implementation of AI within compliance programs.

For example, although the recommendations regarding trustworthy AI are not compliance requirements, they can be treated as additional controls over and above existing compliance requirements, enabling additional compliance utility in the monitoring of AI systems by companies engaged in regulated activities.

12.4. Predictive Compliance Engines

Today, predictive analytics can identify abnormal behavioral patterns to preemptively flag events with higher risk of violations. Increasingly, firms are using predictive analytics to anticipate regulatory compliance violations. Predictive modeling applies statistical techniques to data in order to answer specific questions or predict specific outcomes.

These models draw on pre-existing outcomes or results available in the dataset to assess the relationship between independent variables and a dependent variable. Organizations can then begin using the model with unmeasured outcomes to guide decision-making in situations where the model finds the highest likelihood of the unmet outcome occurring. In the compliance context, those outcomes would be prior incidents of fraud, bribery, or other types of misconduct.

Models based on known past outcomes allow organizations to identify specific behaviors associated with high-risk individuals. For instance, to create a “dishonest employee” model, the organization would use historical data on employees who were once found to have committed fraud. The organization would then compare that data to current data on employees who have not committed fraud to assess what factors distinguish the two groups. The organization could then assess every current employee considering the variables involved — whether they are prior fraud offenders, are of a similar profile, and/or meet other high-risk indicators — to determine which were most likely to commit future fraud.

Using predictive modeling, compliance officers can better assess the risk associated with customers, vendors, and other third parties. They could use predictive analytics and risk

priorities that have the highest likelihood of a compliance breach based on historical information, precedent, or industry standards to track the behaviors of lower-risk vendors while revisiting the higher-risk and more complicated vendors.

12.4.1. Overview of Predictive Analytics

Predictive analytics is defined as the branch of advanced analytics that is used to make predictions about unknown future events. Predictive analytics encompasses a variety of statistical and machine learning techniques, disparate data resources, and modeling procedures to develop predictive information beyond that now standard—e.g., historical regression and correlation modeling with small datasets that can be deployed publicly or internally to deliver, at best, terrifyingly blunt instruments of prediction. Predictive analytics can combine and condense information from disparate data sources for a transaction, model, or individual into a few input indicators—e.g., from open source sources, social networks, internal data, device fingerprinting, and others. It can also do this with larger datasets and more sophisticated learning techniques, such as neural nets, ensemble techniques, natural language processing, unattended language translation, and more.

Depending on the depth and breadth of the use of predictive models, predictive analytics can be broadly and narrowly defined. Narrowly defined, it involves the use of predictive exposure and risk models to direct specific resources to particular people, events, or externalities. This kind of predictive analytics is simple—indeed, the whole idea of forecasting resides within this narrow definition. Broadly defined, predictive analytics can mean anything predictive, including pure exposure modeling based on historical data and regressing on a probability model or information-based directional and size-of-move forecasting models. All of these elements fall under the predictive analytics umbrella.

12.4.2. Applications in Compliance

Predictive analytics is applied in several compliance-related contexts like information security, anti-money laundering, insider threats, security risk assessments, infraction prediction, privacy risk prediction, sanctions screening, fraud detection, and Code of Conduct compliance. Most of these implement predictive models to identify likely infractions on historic data, usually some variety of classification or anomaly detection. The models deployed are generally standard statistical ones like Bayesian classifiers, regression analysis, or heuristics based data alarms. Information security analytics is used to predict likely infraction events, like failures of the CIA triad confidentiality, integrity, availability, or development risk violations. Predictive models evaluate risk-exposure and likelihood of security-related issues in the enterprise architectural design

and operations. The assessments alert security officers to vulnerabilities needing additional proactive defenses. Cyber security compliance deals with the disciplinary aspects of cybersecurity, while cybersecurity analytics focuses on operational project compliance assessments, and forward-looking recommendations. Predictive models have been used for enterprise security anomaly detection tasks including cybersecurity event classification, expert guidance, incident response, and general cybersecurity event analysis.

Anomaly detection algorithms assign some normality score to all relevant tuples in the enterprise data model, usually some sort of predictive examination of past behavior. Security analytics are often built up from classifier ensembles. Anti-money laundering analytics is about identifying dubious individuals for enforcement. For predictive anti-money laundering models, banks have used supervised models on historic infraction cases. Models that predict who is likely to engage in financial crime have also been developed. For any entity in the AML system, previous or current owner of discharged shell companies, or recognized accountants of recognized shell companies are some of the characteristics more strongly associated with a prediction of financial crime perpetration.

12.4.3. Case Studies of Predictive Compliance

This section describes topics relevant to the topic of enhancing compliance with predictive analytics. It provides risk modeling of Medicare fraud. It provides predictive and cognitive machine analysis of compliance-related eDiscovery data as providing the foundational accuracy and trust required to avoid the problems of problematic false positives.

Governments face increasing problems of compliance oversight, particularly due to the astronomical costs of non-compliance such as from healthcare fraud by providers and other players. The Government is in the vanguard of using predictive analytics in this area. It developed a predictive analytics solution in 1996, and has continuously refined and improved it. The solution uses risk modeling to proactively identify for investigation potential cases of healthcare service fraud by providers and others. It uses predictive algorithms on Medicare claims data and reviews them to identify irregular medical billing activity. It leads investigators to providers committing potential fraud and abuse, as well as conduct post payment audits of providers, use the data in jury trials and other litigation for civil and criminal violations. It detects health care service fraud, abuse, and over-utilization via a proprietary regression analysis algorithm based on various risk factors, including trend analysis, predictive algorithms, and data mining techniques. It identifies questionable billing patterns, and identifies and monitors at risk providers, and compares provider performance with that of their peers. In all, it analyzes, compares,

and relies upon 550 risk factors to guide investigations. It continues to be a major tool for reducing fraud, abuse, and over-utilization of services in the Medicare program, particularly with regard to the private sector. Its results are impressive. In fiscal year 2018, it analyzed approximately 220 million claims and made over 545,000 predictive alerts on potential fraud or abuse. That resulted in an estimated $295.6 million in savings.

12.5. Integrating Blockchain and AI for Compliance

The elements that make up the future-proof compliance framework can be further integrated, creating synergies that can ease the burden for compliance operations. For instance, smart contracts can directly call predictive compliance engines, taking appropriate action according to engine outputs. Integration between predictive analytics and compliance assurance through smart contracts creates a Feedback Loop in which prescriptive and predictive elements complement and enhance each other. A more complex Feedback Loop is created by integrating the AI automation with compliance monitoring through the use of secure ledger technology. Alerts generated by predictive analytics may trigger automated compliance actions through the smart contracts, which then generate audit reports or self-verify their subject matter, which are stored in a blockchain. Incorporating either AI or blockchain offers significant advantages; incorporating both offers unique advantages.

A comprehensive approach uses Blockchain, AI, and predictive analytics to transform almost all aspects of the compliance function: first and foremost monitoring and auditing, but also the day-to-day operations and the assessment of compliance policies and risk vectors. The overall scheme provides incentives to compliant actors by making compliance the path of least resistance. Non-compliant actors incur substantial penalties beyond what is manageable within frameworks that do not incorporate permissioned, automated, secure technology. Significant cost savings arise from the efficient allocation of resources, allowing for the concentration of human resources on solving the rare high-risk and high-cost scenarios and questions. The strategy enhances security and reduces risk at the firm as well as enterprise level.

12.5.1. Synergies Between Blockchain and AI

The emergence of new digital technologies such as blockchain and artificial intelligence (AI) represents a shift in the way firms design their business strategies, as well as an opportunity for performance enhancement. Blockchain functions as a distributed ledger technology that offers improved security and traceability, while at the same time, granting real-time access to which specific actor of a network made specific alterations to the data contained in a digital document. Leveraging this property, AI systems on top

of blockchain would have access to a reliable, trustworthy, expert-validated source of past data about any specific document, which in turn could improve the accuracy, autonomy, and explainability of the AI. Conversely, AI would add value to blockchain by speeding up processes through the automation of cumbersome tasks.

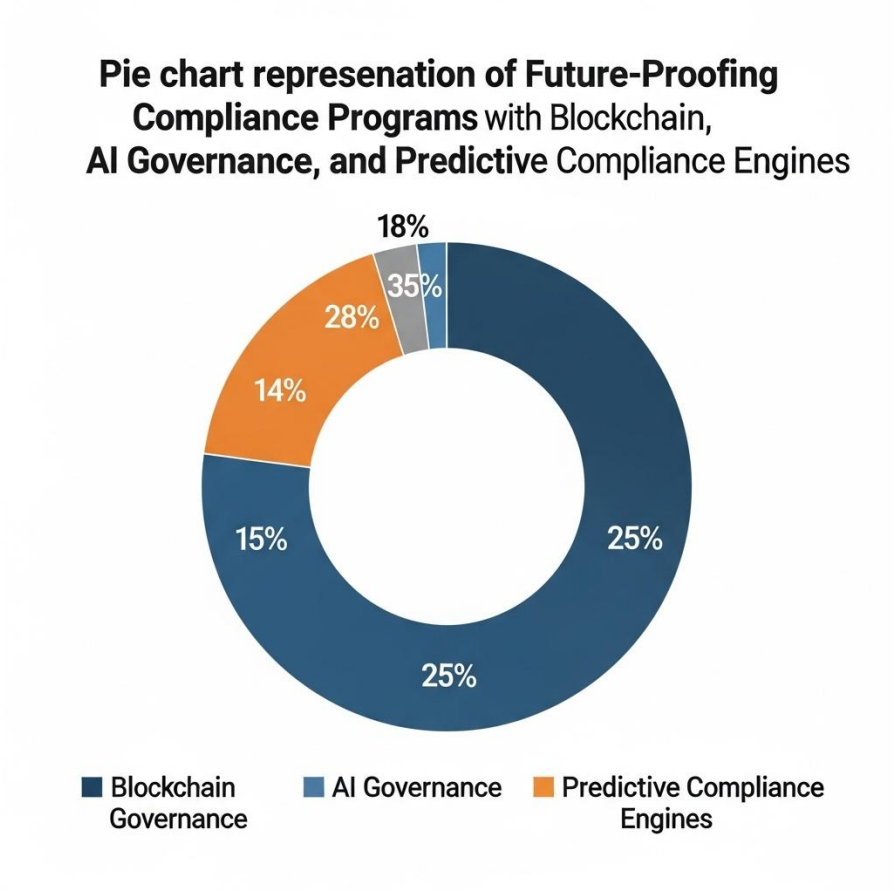

Fig 12.3: AI Governance, and Predictive Compliance Engines

For AI systems to be effective in their outputs, in a way that drives value creation for any business, the AI systems need data to work, which in turn allows for a set of numerical outcomes to be performed based on the contribution of deep learning algorithms. However, firms often struggle to prepare their datasets in a way that allows for predictions to be performed with maximum accuracy, primarily because datasets have to be massive, complete, trustworthy, and free of flaws. Exploiting blockchain's properties allows for improved datasets to then be employed in AI systems and therefore improve the automation of processes in any industry. Furthermore, as AI output data come with a high degree of external risks and potential damage associated with them, making the AI more explainable reduces risk.

12.5.2. Framework for Integration

We systems should consider the proposed multi-layered governance context and examine the verticals in play in compliance, information, and decision environments. Smart contracts, coupled with logic-layer standards, have proven beneficial in numerous tech-driven environments where traditional governance is insufficient. The nature of the governance problem typically dictates the configuration. Policy Injection Points or PIPs are deemed likely preliminary success use cases since they lessen the burden of bureaucracy, while also providing an easy to understand and use entry point for compliance in numerous use-cases across regulatory verticals and decision environments. Regulatory verticals help identify relevant Tech Content Standards for decentralized network systems; information and decision environment dimensions will help de-interest themselves, and propose the relevant Governance Structure coordinated by an appropriate blockchain use case.

The Trade Compliance example demonstrates the proposed framework's usefulness. Tariffs, standards, and enforcement are enforced (or ignored, in the case of infractions) at the border by the Customs Agency responsible for taxation and oversight enforcement directly, while other border commercial requirements are enforced by the Customs Agency, primarily through regulation by in-house inspectors of relevant DocFix Standards.

12.6. Regulatory Considerations

Software and AI that advances predictive compliance assistance into the realm of real-time assistance does exist today. If existing business rules, laws, and predictive models created by machine learning are built into the compliance engine, extensive predictive assistance can be applied to various areas of corporate and regulatory compliance. Although predictive modeling capability, predictive assistance, and real-time communication with the compliance engine can be invoked in a variety of ways, it is certainly possible to dispatch vendors or contractors who are doing work outside of their regular expertise areas a smartphone alert to see if they are doing something technically prohibited by the business rules set up in the predictive compliance engine. Real-time compliance assistance is more challenging than typical recommendations as delivered by consumer applications. Businesses largely ignore the need for compliance assistance until the risk is significant to warrant a high cost, take significantly longer to recover from issues than do consumers, and have the resources to hire those giving predictive compliance assistance. Therefore, compliance engines optimizing business processes and risk evaluations that have either predictive or exceptionally low costs conducted at variable and infrequent intervals are the only truly feasible options for real-time predictive assistance on the market. These will also likely require regulatory approval to

try to sign off on the reduced cost of compliance and risk windows, even if it is not particularly warranted. Such a process would, however, be good business policy and best practice because a streamlined process would enable a very rapid compliance engine development phase along with the completion of company policies.

12.6.1. Current Regulations Impacting Compliance

In the modern business world, regulatory compliance is not just an ethical checkbox; it is a building block for long-term success. Ignoring compliance can cost organizations significantly in terms of monetary penalties, loss of reputation, and increased level of scrutiny from regulators. While establishing compliance programs around current regulations is a little more black-and-white, future-proofing compliance initiatives is a more difficult task as businesses must anticipate new and emergent regulations that make the traditional, prescriptive approach to compliance ineffective. Additionally, organizations must also abide by regulations across jurisdictions. The complexity of compliance greatly increases for organizations doing business globally. Compliance officers release their operators' relationships with many new laws when establishing compliance initiatives owing to the volume, recency, and harshness of the penalties of these regulations. At the same, these compliance initiatives must fall in line with current regulations enforced by various regulatory bodies.

12.6.2. Future Regulatory Trends

A flurry of current global geopolitical activity is sparking initiatives by sovereign governments and regulatory agencies to develop their own centralized digital asset currencies utilizing distributed ledger technology driven by concerns about handing over complete control of local monetary operations to private sector entities and by a desire for alternative settlement infrastructure to mitigate risk during future episodes of international conflict. At the same time, regulatory agencies in the U.S. are attempting to create a full-fledged regulatory framework around private sector tokenization and blockchain implementation activities while nationalization and development initiatives put the country squarely at the center of a classic economic war with its allies. In light of these cross-currents, we should expect that future relevant compliant program building regulations will be focused and proprietary.

Finally, a lone conference held earlier this year highlighted some of the directions that global regulation is likely to take as the world moves quickly to stage a regulated virtual economy that is built on distributed ledger and tokenization technology. There has been lots of talk in the U.K. about developing a regulatory framework for tokenized climate bonds, and one-off talks have come from countries about developing regulator

guardianship frameworks for the issuance of tokenized bonds in their respective capital markets. The accelerating and constant flow of regulations for AI, important progress on the Human-Centric AI and Risk Charter, and prominent talks about developing international risk registries more or less by themselves guarantee that similar international activities are on the way for tokenized products and services.

12.7. Risk Management in Compliance Programs

Implementing an effective compliance program requires aligning policies and procedures with the relevant requirements. Organizations must then ensure policies and procedures are followed, and risks are minimized. Creating and documenting compliance policies and procedures is accomplished through governance documents and the organizational structure designated responsibility for compliance operations and oversight. Enterprises may issue separate policies for compliance-related activities including: information made available to the public, controls around customer and supplier relationships, technical defenses against cybersecurity threats, and any other requirements or activities unique to the organization. Yet policies and procedures alone have a minimal impact in mitigating compliance risks. Employees must follow policies and procedures and be trained in using both as part of their day-to-day operations. Identification of risks informs the design and assessment of compliance policy effectiveness in reducing or mitigating compliance risks. Risk management is a critical step and an ongoing process intended to manage risk to an acceptable level. The key steps are the identification of compliance risks, assessment of the likelihood and impact of risks, mitigation of the risks, and periodic reassessment of risks. The methodology supports organizations in taking a practical and targeted approach to risk assessment, taking into consideration the expected return on investment of various compliance design and operation expenditures.

12.7.1. Identifying Risks

Determining what compliance risks a company has is inherently subjective and imperfect. The most common input to a compliance risk mapping exercise is the company’s size. This is also the biggest risk, as some large companies doing business globally, likely using hundreds of thousands of suppliers, are able to effectively manage and prioritize compliance in an automated and predictive fashion. A small company, especially if it has a big footprint in a high-risk area or area of business, such as manufacturing or healthcare, may have significant compliance obligations that it cannot effectively and reasonably comply with. But risk mapping is more than just size. There

are a variety of qualitative and quantitative inputs into the risk mapping exercise. These include industry, market, geography, personnel, and growth.

The company's industry is one of the most significant considerations. Just as certain industries have higher risks for trade compliance, such as aerospace and commodities, other industries face heightened risks in human rights and anti-corruption. These industries are often capital-intensive with a big external footprint and are highly-regulated. Traditional glossaries for risk mapping include sectors like extractive industries, construction and engineering, and defense and aerospace. Industries like manufacturing and retail may be flagged for specific supply chain concerns. Market characteristics can pose increased risks as well. Markets with rapid growth can often correlate with heightened compliance risk, especially where these markets are geographically concentrated. Young and fast-growing companies, whether early-stage private equity-backed startups or post-IPO companies with a small footprint in high-growth markets, may have additional risks. In combination with other characteristics, this increased risk may be reason enough to have a robust compliance program.

12.7.2. Mitigating Risks with Technology

Technology has advanced to the point that the risks that organizations face can be better managed, and there are several tools that can assist compliance professionals in reducing compliance program risk. Blockchain creates a permanent digital evidence trail of transactions and activities that is immutable and carries accountability risk, provided that people can be held accountable for their actions. Moreover, blockchain technology allows the immutable elements to be shared and accessed by authorized parties, which can promote access to evidence without the parties duplicating the information or holding information that could be lost or compromised. All of this allows organizations to better share risk accountability and to conduct digital due diligence.

Artificial intelligence can similarly assist in managing compliance program risks. AI can perform sentiment analysis and natural language processing to determine employee sentiment about the compliance program. Bias detection software can evaluate compliance communications to ensure that the compliance program is uniformly applied and not having a disparate impact on a particular group of employees. Some enterprises have begun to explore using emotion recognition software to monitor live compliance communications for red flags. Other AI tools assist in the collection, analysis, and validation of compliance data. Today's predictive compliance engines, using pattern recognition learning models, can predict risk behavior based on hundreds of data points, such as employee background and travel frequency and location, among other data. Such predictive compliance engines observe and continuously improve learning models, data point algorithms, and group behavior that can add to identifying risk in real-time,

enhancing resource allocation for increased efficiency and reducing false positives and negatives.

12.8. Conclusion

In conclusion, organizations must modernize their compliance programs for economic resilience and growth in the era of digitalization and remote work. The rapid growth of remote work has posed new risks for both companies and regulators. Compliance obligations and best practices have also changed. Organizations need to strengthen compliance obligations to the business round and the employee's home and create compliance policies that recognize the personal/private nature of the home circle. Compliance management must leverage AI technology, Blockchain, and predictive compliance engines powered by Data Analytics. Tokenizing the unique identity and user behavior of each employee can help organizations, regulators, and enforcement authorities in policy setting, data analysis, model building, and validation. This text discusses key concepts and technologies that can address challenges in the rapidly emerging new compliance space.

There is increased interest in exploring how AI, Blockchain, and Predictive Modeling-Based Data Analytics can help organizations comply with both internal organizational policies, as well as external legal, regulatory, and contractual obligations in a rapidly digitizing economy marked by remote work and digital employee-employer relationships. Ensuring compliance with obligations in a digitized, work-from-home environment is a complex and non-trivial task. Organizations can no longer simply rely on the internal control functions to create binding rules or instructions or policies and make sure employees follow the rules. At the same time, it is difficult for employees and their families to compartmentalize work from home and live like it's another business-as-usual day. Hence, organizations, regulators, and parents need to more proactively use technology tools to find and mitigate risks in a timely manner. The technology-forcing forces focus on enabling predictive compliance analytics engines and token-based, near real-time data-sharing networks so that alerts can be provided across the compliance business ecosystem.

12.8.1. Future Trends

Though there is a trend in compliance towards the maturing offerings of vendors, the overall picture shows a landscape dominated by bespoke solutions, making excessive use of Excel spreadsheets. Predictive engines that can tell companies when they are going to breach compliance are commonplace today and are expected to gain a dominant position in the future. These include predictive disaster recovery, predictive enterprise

security, predictive mobile device management, predictive network management, predictive IT compliance and audits, predictive supply chain, predictive enterprise application integration, predictive data protection, predictive enterprise risk management. Others, such as predictive security network anomaly detection are also being proposed. By their nature, predictive solutions are multijurisdictional. Further, the vast majority of laws and regulations covered by these various predictive solutions are technology-related and multijurisdictional by nature. The challenge of compliance lies ultimately in being capable of examining, cross-correlating and acting upon the relations linking companies across regulations in different jurisdictions.

To use compliance engines more effectively, their developers will create more advanced parsing modes for regulations so that for banks and other regulated firms, the regulatory obligations linked to information security and technology will be dereferenced, and consequently the obligation to put technology compliance policies in place, as well as the compliance documents that substantiate these policies. These documents will also become more advanced because compliance engines will have been tasked with generating tool-based templates for example of data protection impact analyses, which also include the related verification checklists as part of the overall compliance management system. This verification will also be done through predictive compliance engines that will signal when the obligations of checking compliance with the policies would already have become due.

References

Das, A., & Adhikari, N. (2025). Future-Proofing IoT Security: The Impact of Artificial Intelligence. In The Intersection of 6G, AI/Machine Learning, and Embedded Systems (pp. 369-390). CRC Press.

Vashishth, T. K., Sharma, V., Sharma, K. K., & Chaudhary, S. (2024). 10 Future-Proofing. AI-Oriented Competency Framework for Talent Management in the Digital Economy: Models, Technologies, Applications, and Implementation, 153.

Ponnusamy, V., & Aruldas, H. R. (2025). Future-Proofing Emerging Technologies. In Future-Proofing Emerging Technologies for Business Transformation (pp. 439-474). IGI Global Scientific Publishing.

Srivastava, M., & Ghazala, S. (2025). Future-Proofing Sustainable Urban Development: Harnessing Fuzzy Logic for Smart Cities. In Fuzzy Logic in Smart Sustainable Cities (pp. 215-257). Jenny Stanford Publishing.

Nabil, D. Q. (2024). For a Future-Proofed Law of the Sea: Challenges and Opportunities Emerging from the Rapid Development of Technology. AIS: Ars Iuris Salmanticensis, 12(2), 11-39.