



Kyriakos Christodoulides (kyriakos@novelintelligence.ai, [linkedin.com/in/dr-kyriakos-christodoulides/](https://www.linkedin.com/in/dr-kyriakos-christodoulides/)) is the Managing Founder of Novel Intelligence Ltd in London, U.K.

Navigating compliance and risk management in the data science era

By Kyriakos Christodoulides, PhD, CFE

Amid stressed supply chains and inflation, can you afford reputational destruction and a damaged relationship with regulators? As organizations globally grapple with an increasingly complex risk and regulatory landscape, the growing integration of compliance, risk management, and data science is transforming the approach organizations take toward governance. This article sheds light on why “data science for compliance” has a better business case than ever, and it explains how prevention frameworks are enabled to reach their true potential. It also elaborates on how to start engaging in data-driven risk and compliance projects.

Data science: The answer to an evolving regulatory landscape

In the U.S., the Securities and Exchange Commission has enforced orders amounting to more than \$5 billion in 2023, highlighting the escalating cost of noncompliance.^[1] Merely introducing policies and tick-box exercises is no longer recognized as sufficient for improving or even signaling genuine active interest in assuring compliance. For example, the U.S. Department of Justice emphasizes that a company’s monitoring and evaluation of its compliance program should be data-driven and continuous.^[2] This shift emphasizes a growing recognition that a proactive and data-driven approach becomes necessary as regulators demand more efficient risk management. Also, the frequency of mandating additional proactive measures by legislation is projected to increase—not only within the U.S. but also globally.

In the U.K., for example, the recently passed Economic Crime and Corporate Transparency Act requires organizations to exhibit evidence of proactive fraud detection.^[3] In the EU, most financial entities are expected to be impacted by the Digital Operational Resilience Act that will come into effect in January 2025.^[4] Among other factors, information and communication technology risk management—as well as advanced digital operational testing—are central to the Digital Operational Resilience Act.

These realities and more can be summarized in a sentence: A new global incarnation of compliance requires drastically improved risk management, necessitating leveraging data science. That is because data science augments both existing processes and people, and it is therefore poised to not only play a multilayered role within this newly revamped compliance landscape but also emerge as its fundamental cornerstone. Let us see how data science is related to proactive fraud risk management.

The Fraud Triangle is perhaps the most straightforward framework for understanding the relationship between data science and risk management.^[5] According to the Fraud Triangle, the factors synergizing behind an individual’s decision to commit fraud are opportunity, pressure, and rationalization. Of these three components,

opportunity is the only component an organization can have considerable objective control over. By strengthening and automating internal controls, data science diminishes opportunity through improved detection and deterrence, further discouraging potential perpetrators.

This document is only available to members. Please log in or become a member.

[Become a Member Login](#)