Grant Thornton

TOPHIC JUNE

New technologies: towards integrated compliance

Contents

Overview

Our professionals analyse in depth the key implications of artificial intelligence and the latest European regulations on digital compliance. The adoption of AI systems offers new opportunities to strengthen monitoring, risk management and internal control processes, but at the same time introduces new responsibilities in terms of governance, transparency and supervision. In this context, regulations such as the AI Act and the DORA Regulation promote an integrated approach to compliance, in which artificial intelligence, cybersecurity, operational resilience and technology risk management are closely interlinked. For businesses and financial institutions, the challenge lies in transforming regulatory obligations into tools for growth, by developing organisational structures, skills and safeguards that are appropriate to manage innovation in a secure, sustainable and compliant manner.

Regulations such as the AI Act and the DORA Regulation promote an integrated approach to compliance, in which artificial intelligence, cybersecurity, operational resilience and technology risk management are closely interlinked

Expert's opinion

Silvia Laura Rossi
Lawyer - Manager

Investing in a culture of technological responsibility enables businesses to understand the opportunities and limitations of artificial intelligence, reduce the risks arising from its misuse and strengthen their ability to manage innovation in a sustainable and compliant manner.

HOW IS ARTIFICIAL INTELLIGENCE CHANGING BUSINESS COMPLIANCE

WHICH IS THE ROLE OF ARTIFICIAL INTELLIGENCE IN BUSINESS COMPLIANCE NOWADAYS?

Artificial intelligence is profoundly transforming businesses' internal control systems. Thanks to automated data analysis and to their ability to identify anomalies and risk situations, artificial intelligence systems make compliance a continuous and dynamic process: They enhance the effectiveness of monitoring activities, promoting more advanced prevention models and improved risk management capabilities.

DOES THE USE OF NEW TECHNOLOGIES ENTAIL NEW OBLIGATIONS FOR BUSINESSES?

Businesses developing or using artificial intelligence systems are faced with an increasingly complex regulatory framework. With the entry into force of the AI Act, the European Union introduced a regulatory framework based on a risk-based approach, which provides for different obligations depending on the features of the systems used. Compliance can no longer be considered as a series of formal fulfilments, but rather a strategic element of corporate governance and of technology risk management.

WHY IS THERE INCREASING TALK OF INTEGRATED DIGITAL COMPLIANCE?

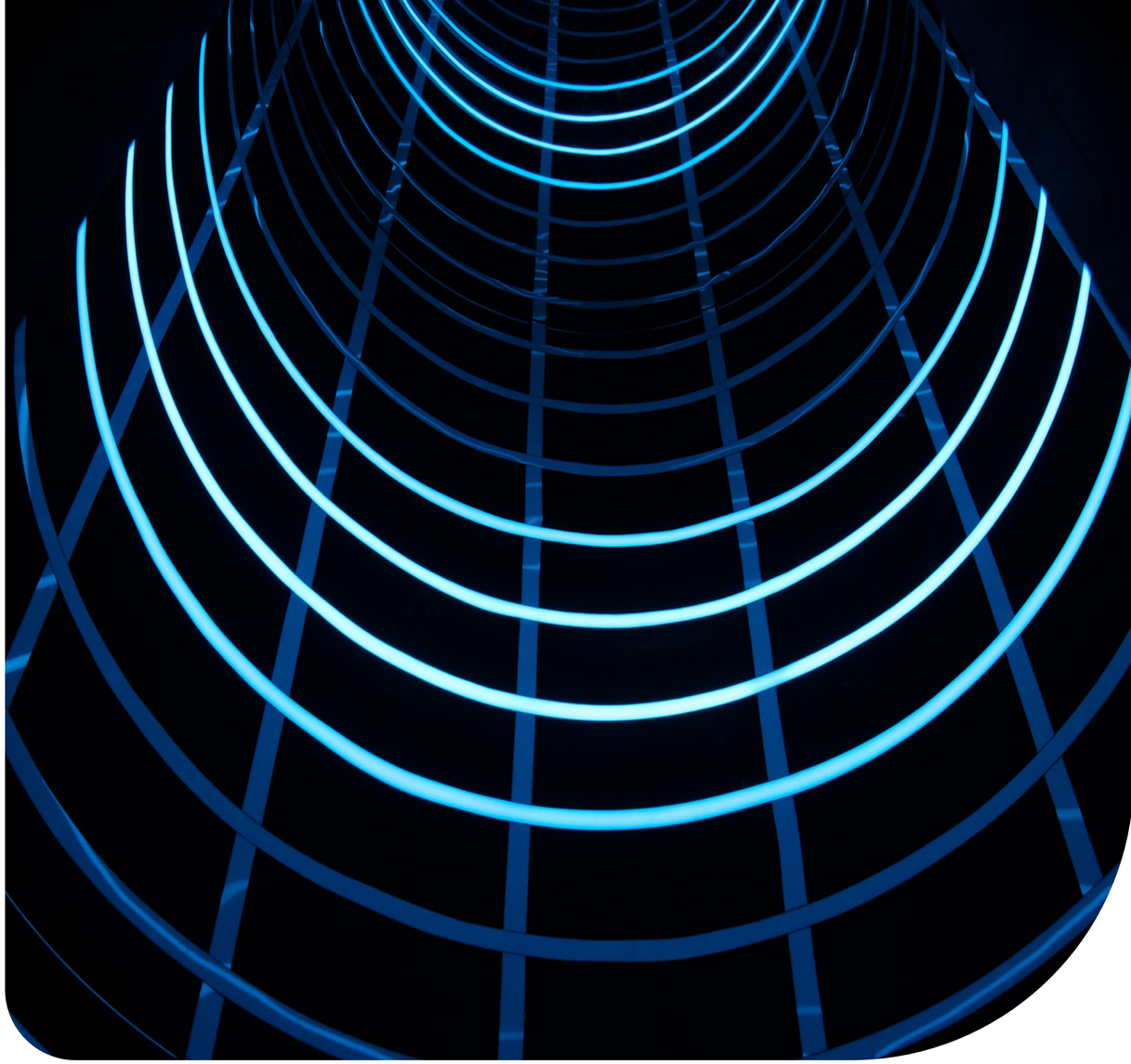
European regulatory evolution is progressively overcoming a fragmented vision of compliance. Data protection, cybersecurity, digital resilience and AI governance are increasingly interconnected and require a unified approach. Businesses must therefore develop organisational structures capable of coordinating legal, IT, cybersecurity, risk management and internal control functions, thereby promoting an integrated approach to technology risk management.

WHICH ARE THE MAIN CHALLENGES INTRODUCED BY THE AI ACT?

The AI Act is the first comprehensive regulatory framework dedicated to artificial intelligence and introduces a risk-based approach. Compliance is not limited to formal compliance with rules, but requires structured governance, risk assessment systems, adequate internal documentation and constant human oversight. The aim is to ensure that technological innovation is developed and used in a safe, reliable manner that respects fundamental rights.

WHY IS TRAINING A STRATEGIC ELEMENT OF AI COMPLIANCE?

The spread of artificial intelligence systems makes it essential to develop adequate skills within organisations. The AI literacy principle, introduced by the AI Act, places particular emphasis on the training of those involved in the development and use of artificial intelligence systems. Investing in a culture of technological responsibility allows businesses to understand the opportunities and limitations of artificial intelligence, reduce the risks arising from improper use and strengthen their ability to manage innovation in a sustainable and compliant manner. Developments in European legislation require an increasingly integrated approach to compliance, in which AI governance, cybersecurity and operational resilience are closely intertwined. It is in this context that the most recent European regulations come into play, transforming these principles into concrete organisational and operational requirements for businesses.



Focus on

Marco Ondoli
Senior Manager

DORA as a pillar of integrated digital compliance

REGULATION (EU) 2022/2554 - DORA

The growing integration between technology risk management, cybersecurity and operational resilience is most clearly reflected in Regulation (EU) 2022/2554 (DORA), which represents one of the key building blocks of Europe's journey towards integrated digital compliance.

The DORA Regulation has been in force since 17 January 2025 for banks, payment institutions, investment firms and other regulated financial intermediaries. For these entities, the question is no longer "do we need to comply?" but rather "how ready are we really?"

For financial intermediaries registered in the register pursuant to art. 106 of the Consolidated Banking Act (TUB) – Confidi (i.e. credit guarantee consortia), leasing companies, factoring companies and consumer credit companies - the deadline is set for 1 January 2027; given the complexity of the measures required, eleven months is too short a time.

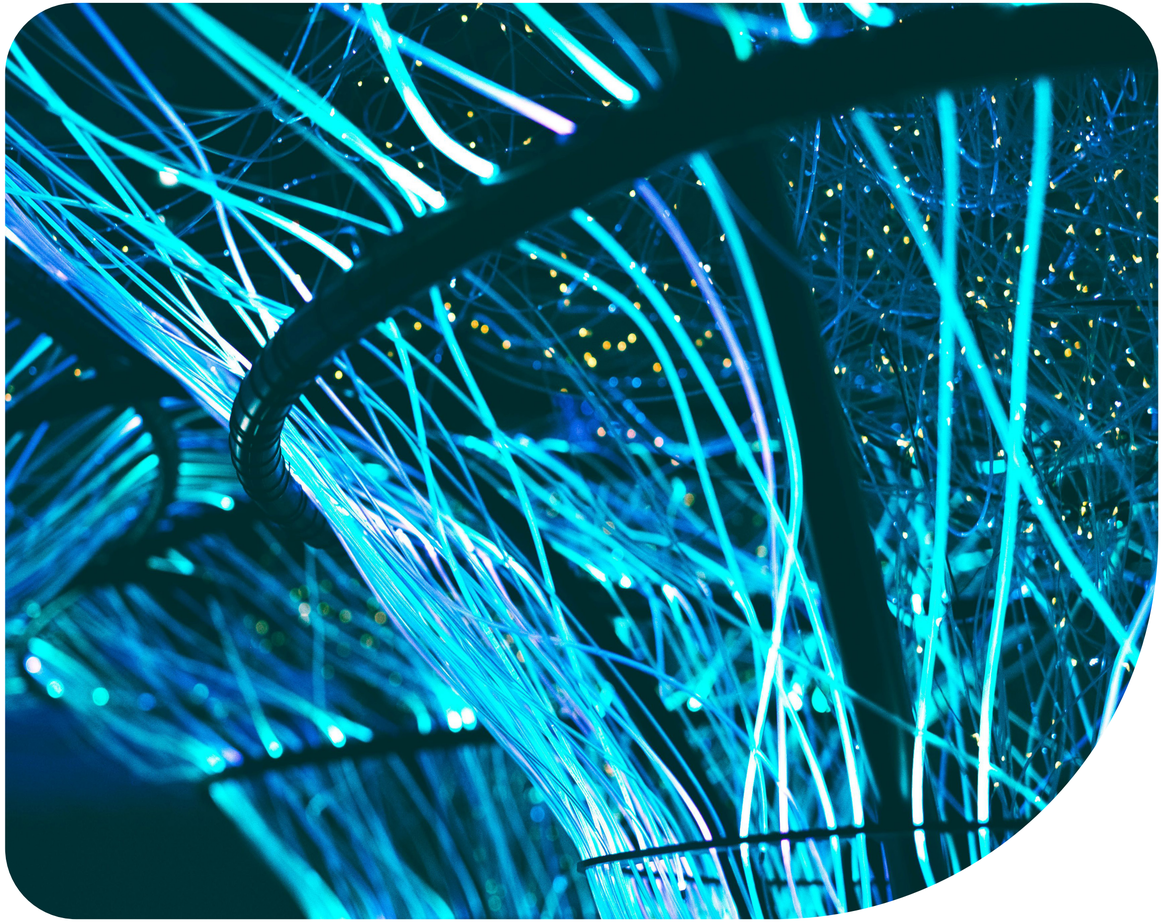
The Grant Thornton Business Risk Services team has gained first-hand expertise in both areas: compliance with DORA requirements, with gap analysis and the implementation of frameworks and policies, and the independent verification of the level of compliance achieved through structured audits applicable to all entities for which the Regulation is already in force. The case studies below show how the principles of integrated digital compliance are put into practice in risk management and operational resilience processes, providing a concrete illustration of the challenges faced and the level of maturity achieved by the Italian market.

CASE STUDY 1

Gap analysis and development of the DORA framework for a regulated financial intermediary

SCENARIO

The first project originated in 2023, when a regulated financial intermediary decided to address the implications of the DORA Regulation in advance, well ahead of the 17 January 2025 deadline. The request was not for an ex-post verification, but for proactive support: to carry out a structured gap analysis based on the five DORA pillars and then to build and implement the frameworks and policies necessary to ensure compliance. As is frequently the case, ICT risk management procedures were in place, but they had been developed in a non-systematic way with respect to the logic of the Regulation: the starting point was to bring them in line by integrating the missing elements.



1

The method

The gap analysis covered all five pillars through a documentary analysis, structured interviews with representatives of the functions involved (ICT, Risk Management, Compliance, Internal Audit) and random reviews of operational processes. The key tool was a three-dimensional assessment matrix for each requirement: existence of the control system, compliance with DORA definitions and actual day-to-day effectiveness. This distinction - between what exists on paper, what is compliant and what actually works - enabled us to prioritise actions in a realistic manner.

2

The issues that have emerged

The most critical areas concerned ICT incident management (existing procedures were not aligned with the six classification criteria of art. 18 of DORA, posing a real risk of failure to notify the Bank of Italy) and third-party risk management, with partial supplier mapping and contracts lacking the minimum required clauses.

3

The interventions and the solution

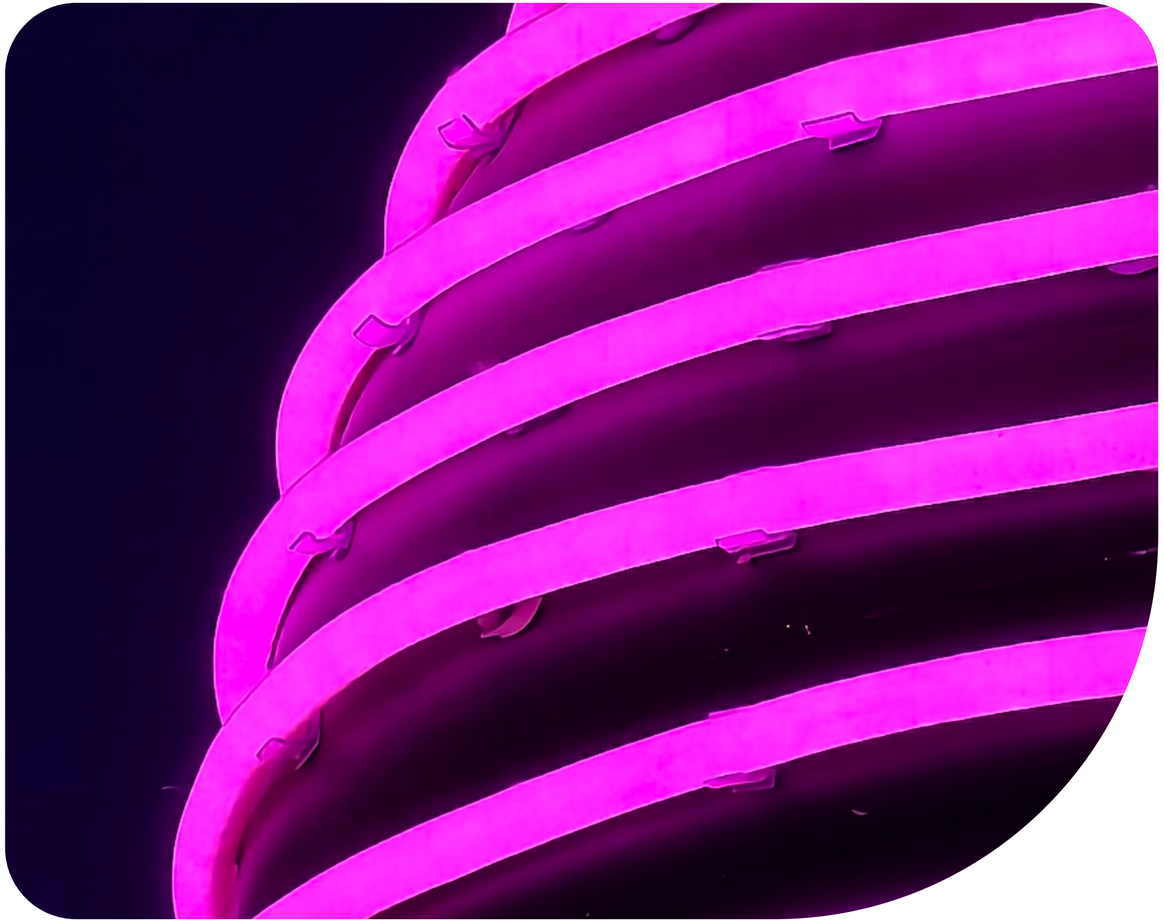
Throughout 2024, the team supported the organisation with the following implementation activities: reviewing the Incident Management procedure, creating a Register of information for critical suppliers, updating contracts to include DORA-compliant clauses and defining a RACI (Responsible, Accountable, consulted and informed) matrix for ICT risk.

CASE STUDY 2

A self-assessment at the request of the Bank of Italy: responding to a request for a DORA self-assessment of ICT risk management

SCENARIO

The second project involved a regulated financial intermediary that had already independently completed a major process of alignment with the DORA requirements, equipping itself with a structured body of documentation (ICT risk management framework, security policies, incident management procedures, business continuity and disaster recovery plans, regulations for the management of third-party suppliers) approved by the company's governing bodies. In this case, it was not an internal choice that led to the launch of the project, but an explicit request from the Bank of Italy: the Authority asked the financial intermediary to carry out a structured self-assessment of its level of ICT risk management, specifically for DORA purposes, using the self-assessment model drawn up by the Authority itself.



1

The method

The Bank of Italy self-assessment model includes five main sections, corresponding to the applicable DORA pillars: ICT risk management (art. 5 to 15), classification and reporting of incidents (art. 17 to 19), operational resilience testing (art. 24-25), management of third-party risk (art. 28 to 30) and information-sharing arrangements (art.45). For each requirement, intermediaries are called upon to state their position and provide documentary evidence of compliance, with explicit reference to internal policies, procedures and regulations.

2

The results of the self-assessment

Thanks to the compliance process already carried out, almost all the requirements received a full compliance rating. The few discrepancies identified related to areas that are naturally evolving: the Business Impact Analysis for the previous year was still being updated; the contractual adjustments with certain third-party ICT suppliers, although initiated through a two-phase plan, were partly pending the contractual renewal cycles; the change management process for applications outside the scope of the main supplier was being consolidated through the adoption of dedicated ticketing tools.

3

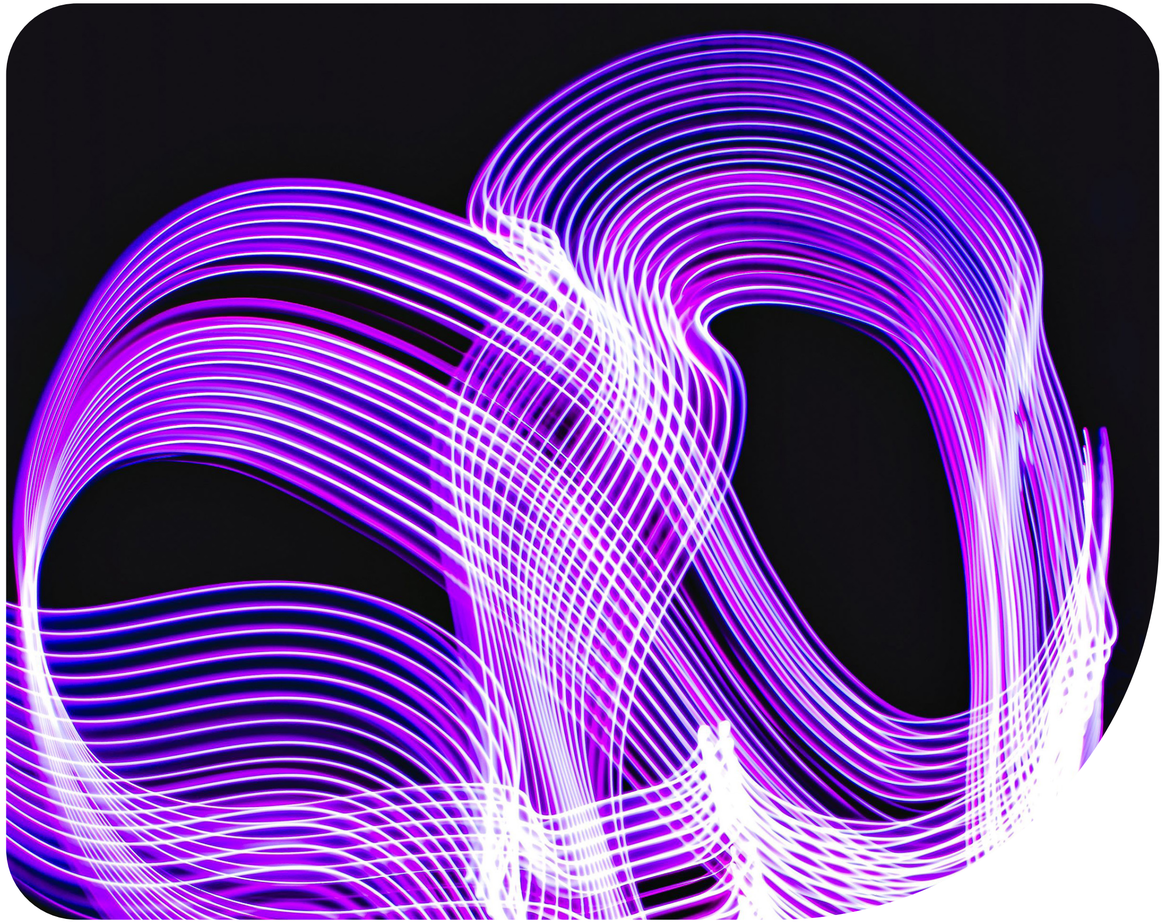
The signal for the market

This case illustrates a trend that is set to become increasingly common: the Bank of Italy does not simply wait for institutions to submit their declarations of compliance but is already actively monitoring compliance with the DORA requirements - even before all the deadlines have come into effect. Being able to respond to this type of requests implies not only having carried out the necessary work but also being able to demonstrate it with structured documentary evidence. The ability to produce a rigorous self-assessment, with precise references to internal policies and regulatory requirements, is a distinct skill from compliance itself - and it is this that supervisors assess.

Two experiences, one lesson

A comparison of the two approaches reveals a common lesson: the level of DORA compliance is not measured by the number of documents produced, but by the organisation's ability to put controls into practice in day-to-day operations and to demonstrate this with evidence. Untested procedures, outdated records and formally correct but non-operational governance are some of the gaps that internal assessment and the supervisory authority aim to identify.

For those entities for which DORA is already in force - banks, payment institutions and investment firms - the compliance audit is now a practical and readily available tool, capable of providing a snapshot of the organisation's actual status and guiding any remaining actions. For intermediaries ex art. 106 of TUB (Consolidated Banking Act), the message is different but equally urgent: the 1 January 2027 deadline leaves less time than it might seem. A structured approach requires month of actual work, the involvement of different functions and contractual reviews that depend on suppliers' cycles. Those which start today will reach the deadline with a margin to spare; those who wait, will not. DORA demands genuine resilience, not just resilience on paper.



Contacts

Our professionals are available to answer any questions or provide further clarification.

Silvia Laura Rossi
Lawyer - Manager
silvia.rossi@bgt.it.gt.com

Marco Ondoli
Senior Manager
marco.ondoli@gtc.it.gt.com

Grant Thornton

Applying AI where **business happens**