HORS-SÉRIE° 2

CYBER-IT MAGAZINE

CYBER IS A MARATHON NOT A SPRINT!

Anticipate, Transform, Take control

The power of GRC

In partnership with crise box

Any questions? Please contact us
cyberit.magazine@gmail.com

EDITO

Dear reader,

Our recent deep dive into Governance, Risk, and Compliance (GRC), through a series of posts and a survey, drew strong engagement and thoughtful feedback. Many of you asked us to bring all that content together in one comprehensive special issue. Consider it done.

You are now reading our second special edition, entirely devoted to the complex yet fascinating world of governance, risk, and compliance. Talking about GRC can feel repetitive sometimes, the same frameworks, the same standards… so this issue takes a different angle. Our approach connects regulatory requirements and real-life situations.

How can certifications and compliance rules actually build customer trust? Is certification really worth the investment ? And could solid GRC practices have prevented or mitigated the impact of certain cyberattacks? These are the questions we explored in this issue.

Of course, we could not cover every single regulation, the topic is far too broad and constantly evolving. But we chose to highlight a few essential pillars: DORA, NIS2, ISO 27001, and the GDPR.

Each of these elements plays a unique role in the structure of GRC. Now, more than ever, organizations must not only understand and apply these frameworks, but also embrace them as strategic assets as these mechanisms can protect them through crisis.

Enjoy!

ARNAUD LEROY

TABLE OF CONTENT

*CNIL: Commission Nationale de l'Informatique & des Libertés. The French data protection authority responsible for ensuring the protection of personal data contained in digital systems and files, across both public and private sectors

Long before the term cybersecurity entered common language, governance and risk management already played a central role in organizing human societies. Throughout history, people have tried to protect themselves against uncertainty, safeguard their possessions, and establish collective rules to prevent abuse. History is full of examples where the pursuit of security and predictability shaped economic and social practices.

In ancient times, Phoenician merchants, renowned for their maritime trade routes, created a joint fund to compensate for losses caused by shipwrecks or pirate attacks. This early form of insurance already reflects an intuitive understanding of risk sharing. A few centuries later, medieval guilds established charters and internal solidarity mechanisms. Their purpose was to protect members from individual bankruptcies, regulate competition, and limit fraud. What might have seemed like a simple convenience was, in fact, an early form of what we would now call control and compliance frameworks.

With the rise of information technology in the 1960s and 1970s, everything changed dramatically. Information became a critical asset, just as valuable as infrastructure and physical property. For the first time, organizations had to consider protecting physical assets but also data, systems, and networks.

The first IT audits began to appear, often led by pioneers who improvised verification methods in an undeveloped environment.

But the importance of these efforts grew as information systems became the beating heart of the modern economy.

Scandals that changed everything

The real turning point came in the early 2000s. The high-profile financial scandals of Enron and WorldCom revealed the risks and vulnerabilities of a system lacking robust controls. The collapse of these giants, which manipulated their accounts to hide losses, sent shockwaves around the world. In response, the U.S. Congress passed the Sarbanes-Oxley Act in 2002, requiring transparency in financial practices, strong internal controls, and holding executives personally accountable. This marked the beginning of the modern formalization of GRC. Originally designed for finance, this integrated approach would soon expand to other domains, including the digital world.

While regulators were redefining financial rules, the digital landscape was living its own revolution. The early 2000s were marked by a series of spectacular cyberattacks. The SQL Slammer worm from 2003, spread across thousands of servers in just minutes, disrupting critical services from ATMs to airline reservation systems for weeks.

A few months later, the Blaster virus infected millions of machines, forcing Microsoft to increase its security mechanisms. Then came MyDoom, widely regarded as one of the most destructive worms in history, which slowed the Internet on a global scale. These attacks made it painfully clear that digital resilience had become just as critical as solid financial statements.

Exporting to Europe

The European Union soon recognized the need to protect its infrastructure and citizens. Through a comprehensive regulatory effort, it aimed to assert its digital sovereignty. The adoption of the **GDPR in 2018** marked a major turning point: for the first time, personal data became the focus of strict regulation. Companies were now required to document their risk management, report any breaches within 72 hours, and design their services according to the principle of privacy by design.

This obligation fundamentally transformed how organizations collect, store, and use data. But Europe didn't stop there. The **2016 NIS Directive, updated in 2022 with NIS2**, introduced strict security standards for critical industries considered strategic, such as health, energy, transportation, digital services, and public administration.

The DORA regulation, set to take effect in 2025, aims to boost the operational resilience of the financial sector. And the **Cyber Resilience Act** widens the scope by requiring all manufacturers of digital products to integrate cybersecurity from the design stage. In France, the ANSSI (French National Cybersecurity Agency) leads the national strategy. Its EBIOS Risk Manager method, updated in 2018, helps organizations identify and prioritize risks based on their business objectives. It has a pragmatic approach that goes beyond technical aspects to consider the strategic value of information and the potential business impact of an attack.

The ANSSI also relies on demanding frameworks: **SecNumCloud** for cloud service providers, **PASSI** for security auditors, and **PDIS** for detection service providers, all of which help structure a broader ecosystem of trust. Globally, a common language has emerged: ISO standards. **ISO 27001**, focused on information security, has become essential for demonstrating an organization's maturity. It is complemented by **ISO 27005** on risk management, ISO 27701 on privacy protection, and **ISO 31000** on enterprise risk management. Together, these standards form a robust global framework, recognized across continents, that facilitates collaboration and builds trust between economic partners.

But the future holds disruptions of unprecedented scale. Quantum computing, developing at a rapid pace, threatens to make today's encryption systems obsolete. Algorithms like RSA and ECC, which currently secure our communications, could be broken in seconds by tomorrow's quantum machines. This sparked a global race toward so-called "post-quantum" protocols, designed to withstand this exponentially greater computing power.

At the same time, the rise of generative artificial intelligence is reshaping the landscape of cybercrime. Fully automated phishing campaigns are already emerging, producing messages that are linguistically and stylistically almost impossible to distinguish from official messages. Deepfakes can replicate a person's face or voice for fraud, blackmail, or disinformation.

Did you know?

In 2019, the British company Arup lost nearly $26 million after scammers used an AI-generated voice clone to impersonate its CEO.

As the threat landscape evolves, GRC will have to evolve. It can no longer rely solely on applying standards and ticking compliance boxes. It must integrate AI into detection and prediction tools, develop forward-looking scenarios, anticipate upcoming international regulations, and build genuine collective resilience.

Only under these conditions will our societies be able to continue functioning in an ever-changing digital landscape, where threats evolve as fast as the technologies meant to stop them.

Inside Europe's Digital Revolution

Derrière les centaines d'articles du règlement, il y a un objectif simple mais fondamental : redonner aux citoyens le contrôle sur leurs données personnelles et restaurer la confiance dans l'économie numérique.

Behind the hundreds of articles in the regulation lies a fundamental goal: to restore citizens' control over their personal data and rebuild trust in the digital economy.

Implemented on May 25, 2018, the General Data Protection Regulation (GDPR) marked a historic shift in how personal information is managed and protected. Rarely has a European law had such an international impact.

For some, it represented a heavy burden, administrative complexity or extensive documentation. For others, it was a founding act, a safeguard against the excesses of a digital capitalism where the individual had become a product and private life reduced to a monetizable stream of data.

The impact of this regulation goes far beyond the borders of the European Union. Today, whether it is California startups, Asian banking groups, or South American e-commerce giants, all must comply with GDPR requirements when handling data belonging to European citizens.

The regulation also introduced a new philosophy: data is not an unlimited resource to be exploited without consideration, but a fundamental asset that carries ethical, economic, and political responsibilities.

To understand the origin of the GDPR, we need to go back to the 1990s, when the European Union made its first attempt at harmonization with **Directive 95/46/EC**. This directive already established some basic principles of data protection, but as with all directives, it allowed member states to adapt its content through their national legislation. The result was a regulatory patchwork, with France, Germany, Spain, and Ireland each adopting very different legal frameworks. Multinational companies operating across several countries had to comply with as many different regimes as they had markets, creating costly legal complexity and undermining consumer trust.

Everything changed in the 2000s with the explosion of the Internet, the rise of tech giants, and the massive collection of personal data. The 2013 Snowden revelations, exposing the scale of NSA surveillance, reinforced European policymakers' conviction: a stronger, more uniform regulation was needed, capable of standing up to the ambitions of both states and corporations.

It was **Viviane Reding**, then European Commissioner for Justice, who launched the project for a new regulation in 2012. After years of intense debate, often shaped by the pressure of tech lobbies, **the text was finally adopted in April 2016.**

Purpose ?

Beneath the legal technicalities of the text, the GDPR has multiple objectives and they are deeply political.

Source : CNIL

The first is to protect individuals against the industrialization of data processing. In an economy where everything is measured, archived, and monetized, citizens risked becoming mere statistics. The GDPR seeks to restore balance: data belongs first and foremost to the individual, and its processing must respect fundamental rights.

The second objective is economic and strategic. By harmonizing rules across Europe, the EU creates a single data market. A startup in Barcelona or Warsaw can handle data under the same legal conditions as a multinational company in Paris or Berlin. This simplification strengthens competitiveness and reduces distortions.

The third objective is geopolitical. Europe aims to establish itself as a "law-based power", capable of exporting its standards. Thanks to its extraterritorial reach, the GDPR even compels American and Asian tech giants to comply if they want access to the European market. This assertion of sovereignty places the EU at the heart of global data regulation, alongside the liberal model of the United States and the authoritarian model of China.

Finally, there is a democratic goal. In an era marked by opinion manipulation, as the Cambridge Analytica scandal showed in 2018, the GDPR seeks to protect freedom of thought and expression by preventing the abusive exploitation of personal data for political purposes

Content ?

The GDPR contains 99 articles and 173 clauses. Behind this legal framework, however, several core pillars can be identified:

Basic principles

Data processing must respect the principles of lawfulness, fairness, and transparency, purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. These principles establish a logic of restraint and rigor: collect less, secure more, and always document.

Rights of individuals

The GDPR strengthens existing rights such as access, rectification, and objection, and introduces new ones like data portability and the right to erasure. These rights allow individuals to regain control over their personal data and impose unprecedented transparency obligations on organizations.

Organizations responsibilities

Data controllers and processors are required to maintain records, report data breaches within 72 hours, appoint a Data Protection Officer (DPO) in certain cases, and conduct impact assessments for high-risk processing activities. The approach is no longer declarative, as it was under the 1995 directive, but accountability-based: organizations must be able to demonstrate compliance at any time.

Authorities and sanctions

Each Member State has its own independent supervisory authority (such as the CNIL in France or the ICO in the UK), working together within the European Data Protection Board (EDPB). Sanctions can reach up to €20 million or 4% of the company's global annual revenue, giving the regulation considerable enforcement power.

Scope ?

The GDPR applies to any organization, public or private, that processes personal data on its own behalf or on behalf of others, provided it is established within the European Union and/or targets EU residents through its activities.

The Economics of cybersecurity and the Benefits of GDPR

CNIL Study

The economics of cybersecurity shows that organizations make investment decisions by comparing the direct costs and benefits for themselves. However, these decisions do not always take into account the broader effects on society as a whole.

Cybercrime does not only affect the victim company, it can impact its customers, partners, and even other businesses through a contagion effect. These impacts are known as negative externalities. As a result, the level of investment in cybersecurity is often lower than what would be socially optimal. The GDPR helps correct these imbalances. Beyond requiring companies to internalize externalities, meaning to consider the wider impact of their actions on society, the GDPR also fosters greater transparency and awareness.

A concrete example of the GDPR's impact involves personal data breaches. Without regulation, a company is not required to disclose a data leak, leaving customers exposed to negative consequences such as identity theft. Some companies may voluntarily report minor incidents to protect their reputation, but they often hide major breaches to avoid reputational damage. This information imbalance contributes to insufficient investment in cybersecurity.

By imposing mandatory breach notification, the GDPR holds companies accountable and encourages them to invest more to prevent financial losses and reputational harm. Studies show that such disclosures reduce identity theft,

demonstrating the regulation's positive effect on security.

The fact that companies are closely connected is another factor leading to the lack of investment. A cyberattack can spread from one company to another, as illustrated by the WannaCry virus or botnets, which use infected computers to carry out malicious activities. When a company invests in cybersecurity, its primary goal is usually to protect its own systems, often without considering the wider ecosystem. Additionally, in cases of outsourcing, data security depends on the subcontractor's protection level. If the subcontractor neglects investment, the data controller is exposed.

The GDPR imposes legal responsibility on subcontractors, encouraging them to maintain high security standards and improving overall cybersecurity.

The ransomware market provides another example of the importance of wider impacts. The size of the ransoms demanded by cybercriminals depends on the victims' willingness to pay. Companies that fail to implement adequate cybersecurity measures increase ransom demand, which raises costs for the broader community.

This illustrates the lack of investment in cybersecurity and the need for regulatory intervention to correct these externalities.

Economic models, such as the one developed by Gordon and Loeb, show that companies' limited investments can be significant, representing between 20% and 66% of the optimal investment when externalities are taken into account. Eurostat data indicate that the GDPR's entry into force led to an increase in updates to cybersecurity protocols among French companies, confirming its positive impact on cybercrime prevention.

A case study on identity theft helps quantify some of GDPR's direct benefits

> **In France, mandatory disclosure of data breaches has helped prevent losses estimated between €90 million and €219 million over four years**

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Across the European Union, these savings are estimated **between €585 million and €1.4 billion.** Around 82% benefits businesses, while the rest goes to individuals. These figures account only for identity theft cases and do not include other forms of cybercrime such as ransomware, nor the impact of mandatory security measures introduced by the GDPR, suggesting that the real impact could be even greater.

Beyond data breach notifications, the GDPR also promotes the adoption of security measures such as encryption, data minimization, and limits on data retention periods. These measures help reduce and the average cost of cyberattacks and lower the exposure of both individuals and companies to risk. They also fortify trust in online activities and foster innovation by securing digital services

The GDPR encourages companies to increase their investment in cybersecurity so it can benefit them but also their clients, partners, and competitors. The figures capture only a fraction of the potential benefits, and many other areas remain to be explored to assess the GDPR's full impact on cybersecurity.

By combining legal obligations and increased awareness, regulation plays a key role in shaping a safer, more resilient digital environment for all.

NIS 2 : Europe plans to turn cybersecurity into a collective safeguard

Adopted in December 2022 and transposed into national law since October 2024, the NIS 2 Directive (Network and Information Security) broadens and strengthens the European cybersecurity framework. It replaces NIS 1, which was considered too limited.

The principle is simple: to require more companies and public administrations to improve their cybersecurity, with specific obligations in risk management, governance, incident detection, and reporting.

Whereas NIS 1 targeted only a handful of strategic sectors (such as energy, transport, and healthcare), NIS 2 now applies to more than 160,000 entities across Europe, including actors from logistics, postal services, the chemical industry, manufacturing, and even some public administrations.

As France's national authority for cybersecurity and cyberdefense, ANSSI is responsible for leading the integration of the directive into national law and overseeing its implementation. The transposition process began with the preparation of a draft bill, presented to the Council of Ministers on October 15, 2024, and then submitted to Parliament for adoption in the coming months.

In the months following the enactment of the law, the implementation process will continue with the development of decrees and ministerial orders. NIS 2 will take effect in France once all the transposition texts, the law, decrees, and orders have been enacted. It is important to understand that while the law comes into force on a certain date, not all regulatory requirements apply immediately to the entities concerned.

Purpose ?

According to **Vincent Strubel**, Director General of the Agence nationale de la sécurité des systèmes d'information (ANSSI), France's national cybersecurity agency:

> ***The NIS 2 Directive elevates the overall level of cybersecurity by introducing harmonized and simplified rules. Amid rising cyberthreats, NIS 2 Amid rising cyberthreats, NIS 2 aims to safeguard France's economic and administrative landscape.***
>
> ***The requirements set by the European directive encourage many organizations to develop a clear roadmap for deploying and strengthening their cybersecurity capabilities, aiming for more secure operational structures, greater trust with stakeholders,***

and enhanced competitiveness for businesses. Ultimately, in coordination with other European Union member states, the goal is to achieve a higher level of cybersecurity maturity across Europe."

Content ?

NIS 2 includes approximately **44 main articles** that define all obligations. Each article often contains multiple paragraphs or "sub-rules" that specify detailed requirements.

Organizations must be able to identify, analyze, and address threats that could affect their information systems. This involves implementing formal cybersecurity policies, as well as developing business continuity and incident response plans.

Regarding incident reporting, any incident or cyberattack with a significant impact must be reported to the competent national authorities within 24 hours. Within 72 hours, a more detailed report must be provided to allow authorities to fully assess the situation and respond properly.

Companies are required to appoint a cybersecurity officer, often a Chief Information Security Officer (CISO), responsible for overseeing their cybersecurity strategy.

Roles and responsibilities must be clearly defined, and boards of directors have to regularly and rigorously monitor the measures they put in place. Regular audits and specific security measures must be conducted to mitigate risks related to external partners. Employee training and awareness are also essential to reduce the human risk factor.

Scope ?

Two categories of entities are now defined:

Essential Entities

These are organizations that perform critical activities for the functioning of society or the economy:

•Energy (electricity, gas, oil)

•Transport (air, maritime, rail, road)

•Banking, finance and insurance

•Drinking water and wastewater management

•Healthcare (hospitals, laboratories, …)

Important Entities

These organizations are less critical but remain exposed:

•Postal and courier services

•Chemical industries

•Research institutions

•Online service providers

•Manufacturers of critical technologies (electronics, communication equipment)

Sanctions

Essential entities: €10 million or 2% of global revenue

Important entities: €7 million or 1.4% of global revenue

Investing in Cyber is cheaper than facing a cyberattack

To compare the costs of compliance with the costs of cyber incidents, we relied on publicly available or verified data.

For this analysis, we relied on the European impact assessment, sector-specific estimates, the economic reference study used by the Commission (Frontier Economics), ENISA's technical guidance, the IBM Cost of a Data Breach report (measuring the average cost of an incident), as well as documented incident involving companies such as Maersk, Norsk Hydro, HSE Ireland, and Derichebourg..

The total cost of NIS2 compliance is estimated at tens of billions of euros across the European Union, translating to an average cost of a few hundred thousand euros per entity.

Recorded cyber incidents have caused losses between a few million to several hundred million euros for a single organization, often exceeding the cost of regulatory compliance.

Public data and official reports consistently show that the investment required to meet NIS2 standards remains, well below the financial impact of a major attack.

Here are a few reference points for this study. Two key political and economic indicators worth noting: An assessment from consulting firms, later referenced by the European Commission, puts the overall cost of NIS2 compliance cost European union at about **€31.2 billion**, according to the technical reports used in the official impact assessment.

The European Commission has noted that NIS2 extends its scope to around 160,000 entities. Based on this estimate, **€31.2 billion divided by 160,000 entities** results in an average cost of approximately **€195,000 per entity.**

This provides a broad benchmark, though the actual cost of implementing NIS2 varies significantly across sectors and organizations.

Large corporations and critical organizations will face significantly higher costs (millions of euros), while many mid-sized "important" entities will incur lower expenses. he Commission also estimated that average cybersecurity spending would increase by around 12% for sectors already covered under the original NIS directive, and by approximately 22% for the new sectors added under NIS2.

Sur la base des estimations publiques et des sinistres documentés, payer la conformité même quand elle représente plusieurs centaines de milliers d'euros ou quelques millions pour un grand acteur est en général moins coûteux que subir un incident majeur (coûts directs + interruption d'activité + réputation + juridique + pertes indirectes).

Le rapport IBM (Ponemon) 2023 montre que les organisations ayant un plan d'intervention, des tests fréquents, de l'automatisation, du chiffrement, des sauvegardes et une segmentation de leur réseau, réduisent nettement le coût moyen d'une violation (parfois de l'ordre de 1 à 2 M€ d'économie) et diminuent le délai d'identification & confinement.

Autrement dit, investir dans la sécurité n'est pas seulement une dépense; c'est une réduction mesurable du coût du sinistre.

Quantifying the impact: the Maersk, Norsk Hydro, HSE, and Derichebourg cases

2017 - Maersk

Worldwide operational disruption leading to a complete infrastructure reset. **Estimated losses : €300 million.**

2019 - Norsk Hydro

Forced to shut down most of its network and temporarily switch to manual operations. **Estimated losses: €75 million**

2021 - HSE Irlande

Ransomware deployed to encrypt critical data and demand payment for its restoration. Estimated losses: €100 million.

2023 - Derichebourg

Temporary shutdown of the main operating software following a third-party intrusion. Estimated losses: €20 million.

SETTING THE STANDARD FOR SECURITY & TRUST

ISO 27001, the international standard for information systems protection, has established itself as a key reference. More than just a technical framework, it represents a comprehensive risk management methodology, adopted by thousands of organizations worldwide.

The story begins in the UK. **The British Standard 7799** (BS 7799), published in 1995, was the first to propose a structured framework for information security management. This pioneering reference was later adopted by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

In 2005, the first official version of the international standard **ISO/IEC 27001** was released, marking the transition from a national initiative to a universal standard. The standard went through first revision in 2013, followed by a major update in 2022. Each iteration reflects the evolution of the digital landscape: the explosion of the internet, the rise of cloud computing, and the growing number of cyberattacks targeting businesses as well as governments.

Contrary to popular belief, ISO 27001 is not a checklist of technical measures. **It requires the creation of an Information Security Management System (ISMS)** based on a continuous improvement cycle, directly inspired by the ISO 9001 quality model.

The goal is clear: **identify** the risks affecting data, **define** appropriate policies, **involve** all employees, and regularly **verify** the effectiveness of the security measures in place.

Purpose ?

The core purpose of ISO 27001 is to ensure that an organization's information, whether digital, physical or verbal, is systematically and sustainably protected against potential threats.

More specifically, the standard aims to establish an Information Security Management System (ISMS) that ensures data confidentiality, allowing access only to authorized personnel, integrity, protecting data from accidental or intentional modification, and availability, ensuring that information and the systems processing it are accessible to legitimate users when needed.

Beyond these three pillars, confidentiality, integrity, and availability, ISO 27001 also provides organizations with a continuous risk management methodology. The goal is not to promise absolute security, which is impossible to achieve, but to demonstrate that the organization has identified its threats, assessed its vulnerabilities, and implemented appropriate measures to protect its most critical assets

Content ?

ISO 27001 is built on two complementary pillars :

The first pillar consists of the main clauses of the standard, numbered 4 to 10. These clauses define the foundational rules for establishing an Information Security Management System (ISMS). It all begins with analyzing the organization's context, identifying key issues, stakeholder needs, and the boundaries of the security scope.

Next comes leadership, which places management at the heart of the process, with a clear policy and well-defined responsibilities. Planning is essential: risks must be identified and assessed to set measurable protection objectives.

The subsequent clauses focus on support, covering resources, training, awareness, communication, and document management. The operational section addresses the implementation of controls and the day-to-day management of risks.

The standard also emphasizes performance evaluation, achieved through internal audits, monitoring indicators, and management reviews. Finally, the principle of continuous improvement ensures that weaknesses are addressed, non-conformities are resolved, and the organization's security posture is progressively strengthened.

These clauses are mandatory and must be implemented by any organization seeking certification.

The second pillar is found in Annex A, which serves as a comprehensive catalogue of security measures. Unlike the clauses, these measures are not automatically required, each organization must review them and determine which are relevant to them based on their own risk profile.

In the 2013 version, Annex A included 114 measures across 14 domains, ranging from asset management and business continuity to access control and cryptography. The 2022 revision simplified this structure for greater clarity, reducing the total to 93 measures grouped into four broad themes: organizational, human, physical, and technological.

These measures cover a wide array of areas, including supplier management, physical security, data protection through encryption, and the implementation of processes to manage and report incidents. Organizations must document their choices in a Statement of Applicability, explaining why certain measures are implemented and why others are not.

Scope ?

Today, more than 70,000 organizations worldwide are ISO 27001 certified. Each organization may have its own objectives for obtaining ISO 27001 certification.

ISO 27001: Turning cybersecurity into a competitive strength

ISO 27001 certification is widely recognized as a mark of reliability and strength for organizations. More than just a technical framework, it represents a strategic approach that involves operational teams, governance, and client relations. Its value goes well beyond compliance, boosting both the organization's credibility and long-term resilience..

The primary benefit for a company is the implementation of a structured and rational approach to risk management. ISO 27001 requires the identification of critical assets, assessment of threats, and definition of appropriate measures to protect data confidentiality, integrity, and availability.

This methodical approach prevents improvised responses and cultivates a proactive mindset. The organization gains the ability to anticipate risks and to respond rapidly and effectively when incidents occur.

From the client's perspective, certification directly influences the company's credibility. In any business relationship, trust is key, especially when sensitive or strategic data is involved.

An ISO 27001 certified company demonstrates that it follows internationally recognized practices to protect entrusted information, demonstrating trust to clients.

In competitive sectors, this advantage can make the difference when winning a tender or convincing a hesitant partner or prospective client.

The impact is also felt at the executive level. ISO 27001 requires senior management to be directly involved in the cybersecurity strategy, through a clear policy, defined responsibilities, and measurable objectives.

This accountability changes governance: information security is no longer confined to technical teams, but becomes a strategic management priority.

Executives gain access to precise indicators from audits and performance monitoring, allowing them to assess the effectiveness of the security measures in place. This not only improves control over financial and reputational risks but also supports informed decisions on security investments.

From a regulatory perspective, certification provides a solid foundation for compliance. Whether it is GDPR, the EU NIS 2 Directive, or sector-specific requirements (banking, healthcare, energy), ISO 27001 offers a methodology that is already aligned with most obligations. Organizations reduce their risk of sanctions, demonstrate compliance during audits, and gain peace of mind amid evolving regulations.

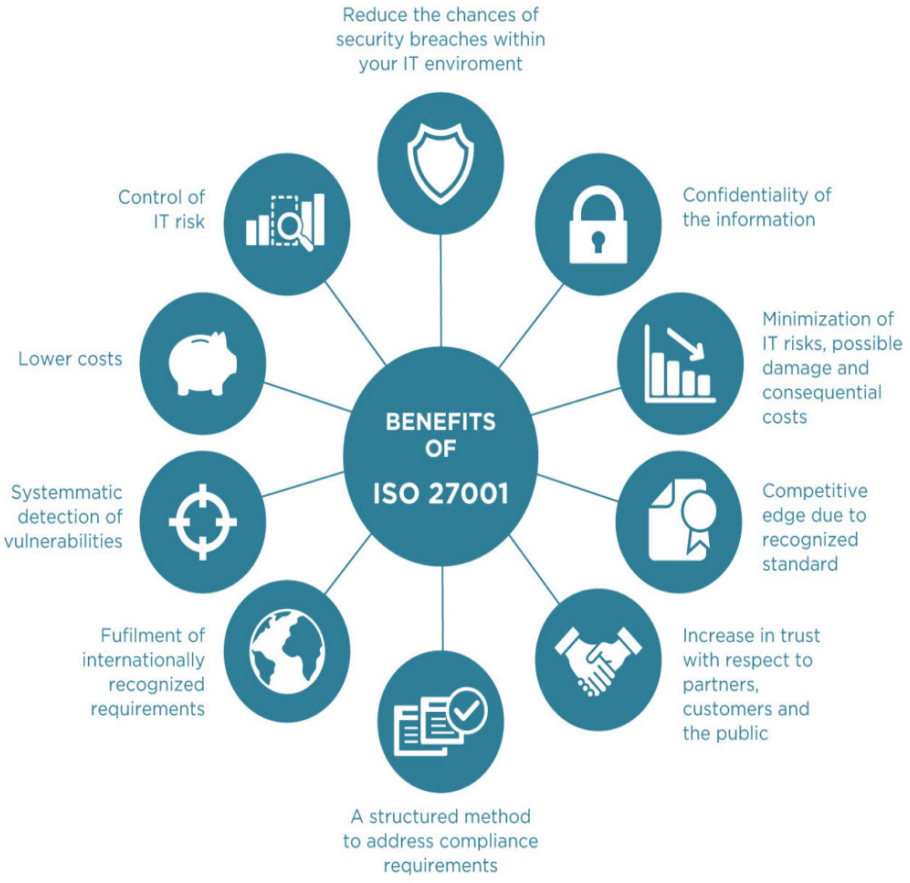
For senior management, this adds an extra layer of assurance: they face lower legal exposure while improving their organization's reputation for reliability.

Finally, the standard strengthens business continuity. Incident recovery plans, backup management, regular testing, and crisis scenarios mandated by ISO 27001 ensure that the organization can continue operating even in the face of a major disruption.

This asset is crucial not only for limiting financial losses but also for maintaining the trust of clients and partners, who see a resilient supplier as a sign of long-term reliability.

ISO 27001 certification is more than a basic compliance exercise, it represents a genuine transformation of governance and client relations. It equips organizations to anticipate threats, strengthen their business credibility, and secure their strategy at the leadership level.

Key pillars of ISO 27001



DORA: Europe's Financial Resilience

One acronym keeps coming up when examining recent developments in European cybersecurity regulation: DORA, the **Digital Operational Resilience Act**. Behind this rather technocratic-sounding name lies a major reform, reshaping the rules across Europe's financial sector. The directive was adopted in December 2022 by the European Parliament and Council, came into force in January 2023, and has been fully applicable since January 2025.

DORA makes cybersecurity a strategic imperative for Europe's financial sector.

The story of DORA emerged in a very specific context: a financial world increasingly reliant on information technology and therefore highly vulnerable to cyberattacks.

This growing dependence on digital infrastructure has also created a new type of systemic risk. Whereas in the past the main threats came from market instability or liquidity crises, today they can stem from a hack, an IT outage, or an incident at a third-party provider like a cloud service.

European regulators, alerted by several high-profile events, including ransomware attacks that paralyzed financial groups and incidents affecting critical service providers, recognized the need for a single, harmonized, and enforceable framework.

The DORA directive marks a turning point in how European financial institutions approach digital security. Beyond its hundreds of pages of provisions lies a simple truth: cybersecurity is no longer a technical concern for IT teams only. It is now a strategic priority impacting the survival, reputation, and competitiveness of the financial sector.

DORA DIGITAL OPERATIONAL RESILIENCE ACT

Purpose ?

Its primary purpose is to put an end a fragmented set of rules. Before DORA, each EU country imposed its own cybersecurity requirements on banks and insurance companies, often with inconsistent, and sometimes contradictory obligations. This resulted in increased complexity for groups operating across Europe, as well as potential gaps that cybercriminals could exploit.

By establishing a regulation directly applicable in all member states, the European Union raises the overall level of resilience while simplifying the regulatory landscape.

Content ?

The content of DORA is structured around five key pillars.

The first one requires financial institutions to implement a robust framework for managing risks related to information and communication technologies. Each organization must identify its critical assets, map its digital dependencies, assess the threats to its systems, and establish appropriate policies to reduce the likelihood and impact of incidents. This approach goes beyond the deployment of technical tools, it also incorporates organizational and human factors such as training, governance, and clearly defined responsibilities.

The second pillar focuses on digital resilience testing. Financial entities will no longer be able to simply claim they have a business continuity or disaster recovery plan, they must demonstrate their resilience through regular simulations, including advanced red teaming exercises in which specialized teams simulate attacks to test defenses under realistic conditions. These tests, mandatory for the most critical entities, are designed to identify vulnerabilities before they can be exploited by malicious actors.

The third one particularly innovative, targets third-party technology service providers, especially major cloud providers on which much of Europe's financial infrastructure now depends. Until now, these players have largely operated outside the direct control of financial regulators. DORA changes this dynamic: providers deemed critical will fall under the direct supervision of European authorities, with specific obligations regarding transparency, resilience, and cooperation..

The fourth pillar concerns incident reporting. Any major event significantly affecting the availability, integrity, or confidentiality of systems must be reported promptly to the relevant authorities. The goal has a dual purpose: to enable a coordinated response across Europe and to increase transparency for the public. In certain cases, clients directly affected must also be notified..

The fifth pillar encourages information sharing between financial institutions regarding emerging threats, discovered vulnerabilities, and attacker tactics. While this collaboration might seem counterintuitive in a competitive environment, it is in fact a powerful tool for collective security. Experience shows that attackers share knowledge and coordinate their actions and the best defense is to mirror this dynamic on the defenders' side.

Scope ?

It covers the entire European financial sector, impacting over 22,000 entities.

- Banks
- Insurance and reinsurance companies
- Asset management firms and investment funds
- Investment and brokerage firms
- Payment service providers
- Market infrastructure (stock exchanges, clearing houses, settlement systems)
- Crypto-asset providers
- Critical third-party service providers

Finance & Cybersecurity

How DORA redefines trust across the financial system

DORA redefines the trust relationship between market participants, institutions, clients, and investors.

By establishing a common digital resilience across the European financial sector, DORA brings stronger security for all and builds trust as a collective asset.

One of its key benefit is in relationships with clients and investors. By demonstrating strict compliance with DORA, a financial institution sends a strong signal of trust and control. Clients can be confident that their data, transactions, and digital assets are protected according to the highest industry standards. Investors see this as a mark of stability and long-term resilience. Compliance becomes a competitive edge, improving the company's reputation and appeal in a context where digital trust has become a strategic asset.

DORA also acts as an accelerator for responsible digital transformation. By structuring security requirements around technological innovation, the directive enables companies to deploy modern tools such as artificial intelligence, cloud computing, blockchain, without compromising operational integrity.

It establishes a framework of trust where innovation can flourish safely. This "security by design" approach fosters an environment in which technological performance goes hand in hand with regulatory prudence.

By reinforcing the digital resilience of the financial sector, DORA helps safeguard the economic stability of the European Union. Attacks targeting financial institutions can have systemic repercussions: disruption of payments, leaks of sensitive data, and damage to market confidence.

In June 2025, UBS confirmed that over 130,000 employee records were exposed following a ransomware attack on Chain IQ, its procurement services provider.

The breach involved sensitive data, including home addresses, private phone numbers of senior executives (including the CEO), and other personal information.

This example clearly shows that vulnerabilities are not always inside the bank itself, but rather in its broader ecosystem, service providers, vendors, and other third-parties. DORA specifically targets these external weak points, imposing resilience standards to help prevent such incidents.

By standardizing security levels, it reduces disparities between market players and makes the financial system more transparent. For clients, this means a safer banking experience, better protection of their data, and assurance of service continuity even in the event of a major cyber incident. In this way, DORA transforms client trust into a tangible and measurable asset.

For investors, it serves as a form of insurance against digital risk. By requiring firms to map their dependencies, test their continuity plans, and reinforce supervision of their third-party providers, DORA significantly reduces the risk of chain disruptions. This translates into greater predictability, lower systemic risk, and, ultimately, higher market confidence in compliant firms.

On a broader scale, DORA also elevates the stability of the European financial system. By establishing a common foundation of digital resilience, it creates collective immunity against cyber threats. A cyberattack on a single bank or critical provider can no longer extend easily throughout the whole ecosystem, as each link in the chain is now subject to stronger security and coordination requirements.

This systemic approach protects individual firms but also critical public infrastructures, payment systems, clearinghouses, and trading platforms. In this sense, DORA becomes a tool of economic sovereignty
.

CREDITS

Editor-in-Chief : Arnaud LEROY
Graphic Design : Arnaud LEROY
English Translation : Maëva ASTORGA
Magazine's sponsor : Guillaume POUPARD

September 2025

In partnership with

crise box