ENHANCING CYBERSECURITY RESILIENCE: AN ANALYSIS OF DORA AND NIS2 IN THE EU DIGITAL ECONOMY

George Cristian Gruia*
University Titu Maiorescu, Bucharest, Romania

Abstract
This article investigates the pivotal role of the European Union's Digital Operational Resilience Act (DORA) and Network and Information Security Directive 2 (NIS2) in bolstering cybersecurity resilience amid escalating threats to sensitive data in the digital economy. Employing a descriptive methodology, the study contextualizes the shift in cybersecurity discourse from questioning if to when an attack will occur, highlighting the urgency for proactive regulatory frameworks. It describes the scope of DORA, targeting financial entities such as banks and insurance firms and NIS2, which extends to essential and important sectors like transportation and manufacturing, offering a comparative analysis of their mandates. Key requirements—including governance, risk management, incident reporting within 24 hours (NIS2), and third-party oversight—are examined in detail, alongside enforcement mechanisms such as administrative fines, remedial orders, and operational restrictions. The analysis reveals non-compliance risks, substantial penalties and reputational damage, with small financial institutions particularly vulnerable to market exclusion. Furthermore, the study shows some practical solutions, such as the Emulex Secure Fibre Channel Host Bus Adapters, which encrypt data in transit to meet regulatory standards. Findings indicate that while compliance entails significant initial costs, the long-term benefits—data protection, operational continuity, and consumer trust—outweigh these investments. The article concludes by advocating for the strategic adoption of advanced cybersecurity technologies to align with DORA and NIS2, ensuring resilience against evolving threats like ransomware and quantum computing risks in the EU's interconnected digital landscape.

Keywords
NIS2, DORA, EU, regulation, differences, operational risk.

JEL Classification
G28, F14, F21, M15

* Corresponding author, **George Cristian Gruia** – george.gruia@prof.utm.ro .

Introduction

In today's economy, maintaining the internal security of the sensitive data of companies and states is crucial. Companies are in continuous search for implementing top-edge security software to protect their intellectual property and to maintain their market share with their specific products. The intellectual property can take different forms, from an easy one (a logo and a registered name) to a complex one (like the recipe of famous brands like Coca-Cola or Pepsi). The attackers could be internal employees who, when laid off, are taking all the documents with them to competition or external actors (competitors or state actors) who are taking advantage of several IT vulnerabilities and attacking the company when least expected.

As a result of these breaches, public institutions have created different standards and regulations to protect the data of the companies within a certain geographical area. Here we mention the DORA (Digital Operational Resilience Act), NIS 2 (Network and Information Security) or PSD 3 (Payment Services Directive) of European Union or the United States' Commercial National Security Algorithm (CNSA) 2.0.

1. Review of the scientific literature

A short evaluation of the above-mentioned regulations was conducted and conclusions were drawn. The purpose of the article is to familiarize the reader with the actual economic context where the companies and state actors are facing every day the question "WHEN will we be attacked?" instead of the old version of the question "IF are we going to be attacked?". In the current economic environment, digital currency is widely used (Lin Tan et al., 2021) and is a novel form of digital central bank money that represents the culmination of state efforts to manage this digital transition. They are designed to provide attractive instruments for both wholesale and retail functions, as well as boost central banks' influence and control over the economy through new monetary, fiscal policy tools and programmable capabilities (L. Dionysopoulos et al. 2024). Due to the wide availability of and trend towards the digital currency to be used by individuals as well as by companies and states, one of the article's main purposes is to also consider and better explain that the international regulations for managing the operations risk from conducting business will become of crucial importance in the near future. There are several other studies available where the need and advantages of digital currencies are presented (Abhinandan et.al. 2025, Vikrant et.al 2025), however we will focus on the question in case, i.e. the need to address the operation risk and how through different EU regulations companies managed to take this risk out of their business. The cost of implementing these regulations is not low (Vandezande, 2024 and Papakonstantinou, 2022), and some companies even refuse to comply with these regulations due to the increased operational costs. There is the question of how these regulations affect the small financial institutions which did not manage and will not implement these regulations, following the risk of receiving a penalty which eventually will put them off the market. However, this is not part of the current article and is being included in the author's extended research.

The Digital Operational Resilience Act (DORA) addresses a critical gap in EU financial regulation. Before DORA, financial institutions primarily managed operational risks by

allocating capital to cover potential losses, which was not efficient from the cost – management point of view.

2. Research methodology

Subjective qualitative research was employed based on the output of the business environment from IT industry in the Czech Republic, Slovakia and Romania, where the respondents shared their feedback on the solutions which they use or should be using to protect their sensitive data from outsiders or internal threats. This research has been in continuous development and change since 2015. Thus, the current research started from the need of the financial institutions to evaluate the risk from their operations, of WHEN instead of IF are going to be attacked and lose the data they were entrusted by their clients. The European Union decided to strengthen the financial sector of the Union, and thus, DORA and NIS2 were implemented.

This article will address the main difference between the (only) two regulations with the purpose of propagating the advantages as well as the penalties which companies must pay if they don't comply with the NIS2 regulation.

The Research Questions fit the logical narrative of every manager with a decisive making role within any financial company, where profit and operational margin are part of their daily forecasts. The research tackles these questions throughout the article, and with the help of the existing regulations, we answer

- Why do we need it?
- What is it? and
- How to comply? with DORA and NIS2 regulations.

3. Results and discussion

Why was DORA needed?

DORA already officially entered into force on January 16th, 2023. Also, the requirements outlined by DORA have become directly applicable to financial entities and Information and Communication Technology (ICT) service providers on January 17th, 2025, following a two-year implementation period. This transition period allows affected organizations time to prepare, conduct gap analyses, update their systems, and put the necessary frameworks in place to comply with the regulation's requirements before enforcement begins.

It aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe can stay resilient in the event of severe operational disruption.

The financial sector is more than ever dependent on technology and on tech companies to deliver financial services. As stated above, the professionals within the financial industry asked themselves the question of WHEN instead of IF and started to take into consideration what will happen with their ICT (Information and Communication Technology) infrastructure when attacked or when it will be disrupted by different external or internal factors. When not managed properly, ICT risks can lead to disruptions of financial services offered across borders. This, in turn, can have an impact on other

companies, sectors and even on the rest of the economy, which underlines the importance of the digital operational resilience of the financial sector.

DORA was introduced by the European Union to harmonise and strengthen the digital resilience of the financial sector. In recent years, financial entities and their service providers have faced a surge in cyber threats, IT failures, and technology-driven disruptions. Existing regulations often varied across Member States, resulting in fragmented standards and inconsistent levels of preparedness. DORA aims to ensure that all financial firms and their technology providers maintain a robust and uniform level of digital operational resilience, thereby increasing market stability and consumer protection across the EU.

DORA applies to a wide array of financial sector entities, including banks, payment service providers, investment firms, credit institutions, insurance companies, crypto-asset service providers, and central counterparties. It also extends to ICT third-party service providers that supply technology services to these financial entities.

DORA's main requirements fall into several key areas:

1. **Governance and Risk Management**: Entities must integrate digital operational resilience into their overall risk management framework, assigning clear responsibilities and ensuring accountability at the board and senior management levels.
2. **ICT Incident Handling and Reporting:** Firms must have robust processes for detecting, managing, and reporting ICT-related incidents. Reporting protocols will be standardised so that authorities receive timely, consistent, and actionable information.
3. **Resilience Testing**: Firms must regularly assess the effectiveness of their digital resilience through testing, including vulnerability assessments, penetration testing, and threat-led penetration tests.
4. **Third-Party Risk Management**: A standardized approach to managing and monitoring the risks posed by external ICT service providers must be established. This includes due diligence, contractual requirements, and ongoing oversight.
5. **Information Sharing**: Entities are encouraged to participate in information-sharing arrangements to enhance collective threat intelligence and improve sector-wide cyber resilience.:

The European Commission came forward with the DORA proposal on 24 September 2020. It is part of the larger digital finance package, which aims to develop a European approach that fosters technological development and ensures financial stability and consumer protection. In addition to the DORA proposal, the package contains a digital finance strategy, a proposal on Markets in Crypto-Assets (MiCA) and a proposal on Distributed Ledger Technology (DLT).

This package bridges a gap in existing EU legislation by ensuring that the current legal framework does not pose obstacles to the use of new digital financial instruments and, at the same time, ensures that such new technologies and products fall within the scope of financial regulation and operational risk management arrangements of firms active in the EU. Thus, the package aims to support innovation and the uptake of new financial

technologies while providing for an appropriate level of consumer and investor protection.

The Council adopted its negotiating mandate on DORA on 24 November 2021(European Insurance and Occupational Pensions Authority, 2025).

The Act is part of the digital finance package, a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks arising from it. It is in line with the European Commission priorities to make Europe fit for the digital age and to build a future-ready economy that works for the people.

The digital finance package includes a new Strategy on digital finance for the EU financial sector 1 with the aim of ensuring that the EU embraces the digital revolution and drives it with innovative European firms in the lead, making the benefits of digital finance available to consumers and businesses.

In addition to this proposal, the package also includes a proposal for a regulation on markets in crypto assets, a proposal for a regulation on a pilot regime on Distributed Ledger Technology (DLT) market infrastructure, and a proposal for a directive to clarify or amend certain related EU financial services rules.

Digitalization and operational resilience in the financial sector are two sides of the same coin. Digital, or Information and Communication Technologies (ICT), gives rise to opportunities as well as risks. These need to be well understood and managed, especially in times of stress.

Policymakers and supervisors have therefore increasingly focused on risks stemming from reliance on ICT. They have notably tried to enhance firms' resilience through the setting of standards and the coordination of regulatory or supervisory work. This work has been carried out at both international and European levels, and both across industries as well as for several specific sectors, including financial services.

ICT risks nevertheless continue to pose a challenge to the operational resilience, performance and stability of the EU financial system. The reform that followed the 2008 financial crisis primarily strengthened the financial resilience of the EU financial sector, only addressing ICT risks indirectly in some areas, as part of the measures to address operational risks more broadly.

While the post-crisis changes to the EU financial services legislation put in place a Single Rulebook governing large parts of the financial risks associated with financial services, they did not fully address digital operational resilience.

The measures taken about the latter were characterized by several features that limited their effectiveness. For example, they were often devised as minimum harmonization directives or principled-based regulations, leaving substantial room for diverging approaches across the Single Market. In addition, there has been only some limited or incomplete focus on ICT risks in the context of the operational risk coverage.

Finally, these measures vary across the sectoral financial services legislation. Thus, the intervention at Union level did not fully match what European financial entities needed for managing operational risks in a way that withstands, responds and recovers from the impacts of ICT incidents. Nor did it provide financial supervisors with the most adequate tools to fulfil their mandates to prevent financial instability stemming from the materialisation of those ICT risks.

The absence of detailed and comprehensive rules on digital operational resilience at EU level has led to the proliferation of national regulatory initiatives (e.g. on digital operational resilience testing) and supervisory approaches (e.g. addressing ICT third-party dependencies).

Action at the Member State level, however, only has a limited effect given cross-border nature of ICT risks. Moreover, the uncoordinated national initiatives have resulted in overlaps, inconsistencies, duplicative requirements, high administrative and compliance costs - especially for cross-border financial entities - or in ICT risks remaining undetected and hence unaddressed. This situation fragments the single market, undermines the stability and integrity of the EU financial sector, and jeopardises the protection of consumers and investors.

It was therefore necessary to put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities. This framework will deepen the digital risk management dimension of the Single Rulebook.

In particular, it will enhance and streamline the financial entities' conduct of ICT risk management, establish a thorough testing of ICT systems, increase supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities, as well as introduce powers for financial supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers. The proposal will create a consistent incident reporting mechanism that will help reduce administrative burdens for financial entities and strengthen supervisory effectiveness.

The proposal for regulation is based on Article 114 of the Treaty on the Functioning of the European Union (TFEU). It removes obstacles to and improves the establishment and functioning of the internal market for financial services by harmonizing the rules applicable in the area of ICT risk management, reporting, testing and ICT third-party risk. Current disparities in this area, both at legislative and supervisory levels, as well as national and EU levels, act as obstacles to the single market in financial services because financial entities that engage in cross-border activities face different, where not overlapping, regulatory requirements or supervisory expectations with the potential to impede the exercise of their freedoms of establishment and of provision of services.

Different rules also distort competition between the same type of financial entities in different Member States. Moreover, in areas where harmonisation is absent, partial or limited, the development of divergent national rules or approaches, either already in force or in the process of adoption and implementation at the national level, can act as a deterrent to the single market freedoms for financial services. This is particularly the case as regards digital operational testing frameworks and the oversight of critical ICT third-party service providers.

As the proposal has an impact on several Directives of the European Parliament and of the Council adopted based on Article 53(1) of the TFEU, a proposal for a Directive is also adopted at the same time to reflect the necessary amends to those Directives.

Why should we comply with DORA?

Non-compliance with DORA can result in supervisory measures, administrative penalties, and enforcement actions from relevant authorities. While exact penalties vary, the overarching goal is to ensure that non-compliant entities take swift corrective

measures and enhance their cyber resilience posture. However, organisations can generally expect some, or all, of the following consequences:

A) Administrative Fines and Financial Penalties:

Non-compliance can result in substantial administrative fines. While DORA sets overarching principles, each EU Member State may establish its specific monetary penalty ranges. These penalties are intended to be "effective, proportionate, and dissuasive," meaning they should not be easily absorbed as a cost of doing business.

B) Remedial Orders and Corrective Measures:

Authorities may require the offending entity to take corrective action within a set timeframe. This could include implementing stronger cyber controls, enhancing governance procedures, upgrading IT infrastructure, or restructuring contracts with third-party providers.

C) Restrictions on Business Operations:

In more severe cases, supervisory bodies may impose restrictions on certain business activities until compliance is achieved. For instance, they could limit the entity's ability to offer certain financial products or services if these are deemed vulnerable to cyber threats.

D) Increased Supervisory Scrutiny and Ongoing Monitoring:

Organizations found non-compliant may be subject to heightened oversight, such as more frequent inspections, stringent reporting obligations, and targeted audits by regulators. Continuous supervisory pressure can raise operational costs and divert internal resources.

E) Reputational Damage and Loss of Client Trust:

While not a direct "penalty" from regulators, non-compliance can seriously harm an entity's reputation. Losing the trust of customers, investors, and partners can have significant long-term financial implications and impact competitive standing.

F) Potential Implications for Senior Management:

In certain jurisdictions and under certain frameworks (including potentially overlapping regulatory regimes), senior managers or board members could face personal liability, warnings, or disqualification if they are found to have wilfully ignored or inadequately managed operational resilience risks.

DORA builds on widely recognised standards and frameworks (e.g., ISO/IEC 27001, NIST CSF) by aligning with global best practices in cybersecurity and operational resilience. Its goal is not to replace these frameworks but to unify requirements at the EU level and ensure a consistent resilience baseline across the financial sector.

DORA designates responsibilities to the European Supervisory Authorities (ESAs) — namely the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA), and the European Insurance and Occupational Pensions Authority (EIOPA). The ESAs will work together to develop technical standards, guidelines, and oversight frameworks. They will also collaborate to supervise critical ICT third-party providers and ensure consistent application of DORA across the financial sector.

DORA is specifically tailored for the financial sector, addressing unique operational and ICT risks faced by financial institutions. While the NIS2 Directive and other cybersecurity legislation provide broad cybersecurity guidelines for critical infrastructure and essential services, DORA zeroes in on financial stability, market integrity, and

consumer protection. Entities subject to both regulations must ensure compliance with each, leveraging overlapping principles and controls to streamline their efforts.

What is NIS2?

NIS2 is comparable to the GDPR (General Data Protection Regulation), which shook up how businesses have to think about and protect data back in 2018. However, while the GDPR is about the guardianship of data itself, NIS2 is far broader in scope and covers protecting the infrastructure around the data (NIS 2 Directive, European Parliament Legislative Observatory, 2025).

Table no. 1 – Comparison between GDPR, NIS2 and DORA

GDPR	NIS2	DORA
Data Availability (Art. 32)	**Continuity Requirement (Annex III)**	**Protection & Prevention (Art. 9) Backup Policies (Art. 12)**
Rapid Access Restoration (Art. 15-17)	**Service Continuity (Art. 18)**	**Stability Assurance (Art. 11)**
Portability Rights (Art. 20)	**System Interoperability (Recital 19)**	**Standardized Exchange (Art. 12, 25)**
Data Protection (Art. 32, 33)	**Cybersecurity Risk Management (Art. 21)**	**Detection Capabilities (Art. 10)**
Transparency & Accountability (Art. 30, 35)	**Reporting Obligations (Art. 23)**	**Proactive Monitoring (Art. 19)**
Data Backup	**Data Recovery**	**Data Portability**	**Data Security**
Data Intelligence			

Source: own contribution

Table 1 shows a comparison between GDPR, DORA and NIS2 regulations, where one can easily find in which article of the corresponding norm one can find the standard requirements to comply with the above mentioned regulation. For example, the Data Protection, which GDPR explains in articles 32 and 33 are being evaluated within the NIS2 regulation within the Cybersecurity Risk Management in art.21 and within DORA regulation in art.10 Detection Capabilities.

As cybersecurity threats evolve and pose ever-greater risks to individuals and businesses, regulations continuously develop to keep pace with threats and elevate minimum security standards. NIS2 (Network and Information Security version 2), the latest such directive from the European Union, is a significant development in this space.

An expansion and reinforcement of its predecessor, the NIS Directive (2016), NIS2 is a significant overhaul of the EU's cybersecurity regulation landscape, aiming to bolster the overall level of cyber resilience across member states and any entities that do business

with them. It extends the scope of the original NIS Directive by broadening the range of sectors and types of entities that fall under its jurisdiction, including those considered to play an 'essential' and 'important' role in the EU's internal market.

For such organisations, NIS2 presents a step up in security compliance — they will either find themselves included under the regulatory scope for the first time or held to much higher standards (and penalties) than under the previous directive.

NIS2 introduces more significant obligations, requiring entities to adopt comprehensive incident reporting mechanisms, robust risk management practices, corporate accountability measures, and effective business continuity strategies.

Significantly, the NIS2 Directive also introduces significant consequences for non-compliance, including substantial fines and the potential for litigation.

NIS2 significantly expands the scope of regulation beyond its predecessor, casting a much wider net over a range of sectors deemed critical for the EU's international market.

This expansion covers not just sectors considered directly critical but also includes those that are part of the supply chain to these sectors, increasing the number of companies and sectors now falling under regulatory scrutiny.

A key development in NIS2 is the classification of entities into two categories: "essential" and "important". This distinction affects the directive's reach and the implications for different types of organizations.

This category, also recognized under NIS encompasses sectors foundational to societal and economic well-being. These include transportation, financial services, healthcare and utility companies such as energy suppliers.

For these entities, NIS2 reaffirms their critical status and escalates compliance requirements. For instance, incident reporting must occur within 24 hours — a major update from the previous directive.

The most significant change for these companies is the introduction of substantial fines and consequences for non-compliance. So, the rules have changed, and the stakes have never been higher.

'Important' entities are a brand-new addition to NIS2, meaning the directive will cover these organisations for the first time. Sectors like digital infrastructure, public administration, and manufacturing must quickly adjust and audit their cybersecurity practices.

Given the breadth of the requirements and shorter timeline, this may present a steeper initial challenge. The good news for these entities is that the directive imposes less stringent obligations than organisations classified as 'essential', with lower potential repercussions for non-compliance. However, the need to prepare should not be underestimated.

In short, the NIS2 Directive broadens the regulatory scope, covering more sectors and introducing a classification system that dictates the level of requirements and potential penalties. To understand how to prepare for NIS2, organizations must understand which classification they fall under to know what's expected of them and the possible consequences.

Why do we need NIS2?

NIS2 mandates a comprehensive approach to cybersecurity, encompassing a range of organisational responsibilities:

a) **Duty of Care** - organizations are required to implement robust risk management measures to minimise cyber risks. This includes incident management, securing the supply chain, enhancing network and access control security, and employing encryption where necessary. A key part of this, and one specifically called out in the directive, is ensuring business continuity during significant cyber incidents. This includes system recovery, emergency procedures, and establishing a crisis response team.

b) **Duty to report** - Essential entities are mandated to establish processes for promptly reporting significant security incidents, with specific notification deadlines, such as a 24-hour "early warning" system. NIS2 also significantly emphasises corporate accountability, requiring management to be actively involved in and knowledgeable about the organisation's cybersecurity measures. Management may face penalties for breaches, including liability and potential temporary bans from management roles.

Once organisations understand if (and where) they fall under the NIS2 scope, the next step is to gain clarity on the implications of the directive, including the broad organisational requirements, the ten minimum cybersecurity measures, and the specific consequences for non-compliance.

The directive outlines ten minimum cybersecurity measures that organisations must adopt to comply with its requirements:

1. Conduct risk assessments and establish security policies for information systems.
2. Develop policies and procedures to improve the effectiveness of security measures.
3. Implement policies and procedures for the use of cryptography and encryption where relevant.
4. Define a plan for handling security incidents.
5. Ensure security in the procurement, development, and operation of systems, including vulnerability reporting.
6. Provide cybersecurity training and maintain basic computer hygiene practices.
7. Implement security procedures for employees accessing sensitive data, including data access policies and asset management.
8. Manage business operations during and after a security incident, ensuring up-to-date backups and access to IT systems.
9. Utilize multi-factor authentication, continuous authentication solutions, and voice, video, and text encryption.
10. Secure supply chains, assessing vulnerabilities and overall security levels for all suppliers.

While the broad requirements and ten minimum measures give companies a good steer on where to address their policies to prepare for NIS2, as with any regulation, the devil is in the details. Reviewing the directive fully or working with a partner who understands the ins and outs is essential. Crucially, the challenge of tracking the variation across different member states will be pivotal to ensuring compliance, particularly for businesses working across several European countries.

As with most business-wide projects, you need to start with a thorough plan and review what you currently have in place and where you need to get to.

Scope and Classification — Begin by determining whether NIS2 applies to your organisation and, if so, whether you are classified as an "important" or "essential" entity. This will dictate the extent of the requirements you need to meet.

Review and Audit — Thoroughly examine the NIS2 requirements and the ten minimum measures. Audit your current cybersecurity posture, processes, and technology against these standards to identify areas needing improvement.

IT and compliance teams cannot meet NIS2 requirements on their own. It requires team effort throughout. From initial planning stages to ongoing review and maintenance, ensure every affected party has a seat at the table.

Cross-team collaboration — Implementing the required security measures and processes demands collaboration and buy-in from all levels of the organisation. Leadership backing is crucial for initiating change, and because NIS2 mandates corporate management's responsibility for cybersecurity. IT, security, and operations teams must also work together to implement security, backup, and encryption measures effectively.

Organisational Training — Beyond leadership, adherence to NIS2 involves training the organisation to update security practices in line with minimum measure 6. It's crucial that this training isn't a one-time action, but a continuous process that helps maintain awareness of responsibilities long-term, evolves over time, and onboards new employees effectively.

How do we apply NIS2?

Meeting the requirements of NIS2's 'duty of care' requires a thorough audit of security risk across the organisation. This includes data storage, data access, security and vulnerability scanning.

Data Management and Hygiene — Ensure good data management practices, such as data tagging, appropriate data locality, secure storage and backups. Extending the duty of care to backups is also important. This includes having immutable backups (which can't be targeted or changed by attacks like ransomware) and keeping multiple copies of data in case of errors.

Security Measures — Continuously evaluate and ensure appropriate security measures are in place, especially for personnel accessing sensitive or important data. Incorporate zero-trust frameworks, cryptography, and encryption, and ensure all systems (third-party and first-party) are secure and regularly scanned for vulnerabilities. Implement robust security measures for supply chain vendors and enforce multi-factor authentication where appropriate.

Why report the incidents of NIS2?

NIS2 mandates having a comprehensive plan for security incidents that includes maintaining operations and continuity during and after an incident. Therefore, businesses need to have a dedicated incident response team, including stakeholders across different business units, to define and regularly drill a robust incident response process.

Threat Detection — Early detection of incidents, such as ransomware attacks that may breach systems well in advance, is critical. Invest in threat

detection capabilities, monitoring, alerts, and malware detection to catch incidents as early as possible.

Backup Strategy — Ensure up-to-date backups are in place, focusing on mission-critical data. Companies have developed several backup rules as the 3-2-1-1-0 Golden Backup Rule. This includes having three copies of data on two different media, with one copy offsite and one to be air-gapped, immutable, or offline, and aiming for zero errors in backup and recovery verification.

Response and Recovery — Develop processes for incident reporting and communication during an incident. For recovery, have disaster recovery processes in place to ensure business continuity. Reliable backups are crucial, but a robust recovery process that includes planning for recovery in a separate, secure environment is vital to minimise downtime and its associated costs. Strategic

Planning for Recovery Environments — Organizations must consider their recovery environments. Often, you cannot recover in the same environment where the incident occurred. Planning for a separate, secure recovery environment in advance is essential. For example, the middle of a security incident is not the time to integrate with a new cloud provider for the first time!

Conclusions

The key distinction lies in their applicability: **NIS2** sets a baseline for cybersecurity across multiple sectors, while **DORA** provides a targeted approach for financial entities, offering a more granular set of rules.

As part of the ICT risk management framework, DORA requires that all financial entities put in place a comprehensive ICT Business Continuity Policy, forming an integral part of the overall business continuity policy of the financial entity.

This policy must contain provisions that ensure the continuity of the financial entity's critical or important functions. As a result, several vendors from the IT industry have developed products to meet these requirements and to ensure their products address the new regulations from the European and non-EU markets.

For example, on January 28th, 2025, at Palo Alto, California, USA, company Broadcom Incorporated (which trades at NASDAQ stock exchange under index AVGO) announced an industry-first: the new, innovative Emulex Secure Fibre Channel Host Bus Adapters (HBA), which is a cost-effective, easy-to-manage solution that encrypts all data as it moves between servers and storage.

Encrypting mission-critical data is no longer a nice-to-have, but a must-have. The cost of ransomware attacks continues to rise, with attacks in 2024 costing USD $5.37 million[†] on average per attack. Upcoming generative AI and quantum computers magnify the risk if data is not encrypted at all points in the data center, including the network.

To address these cybersecurity issues, governments have responded with mandates, including the **United States' Commercial National Security Algorithm (CNSA) 2.0, the European Union's Network and Information Security (NIS) 2, Digital**

[†] Cost of a Data Breach Report 2024, Ponemon Institute, available online https://www.ponemon.org/

Operational Resilience Act (DORA) and more that require enterprises to modernize their IT infrastructures with post-quantum cryptographic encryption algorithms and zero trust architecture.

Today, data centres have the option of deploying application encryption or network encryption to protect their data. Network encryption offers several important advantages versus application-based encryption, including preserving storage array services such as dedupe and compression, which are destroyed when using application-based encryption. Network encryption also enables real-time ransomware detection, while application-based encryption hides ransomware attacks. Additional highlights of this solution include no encryption performance penalty and simple, session-based key management.

"Customers are seeking ways to protect themselves against crippling and expensive ransomware attacks as well as complying with new government regulations mandating all data be encrypted," said Jeff Hoogenboom, vice president and general manager, Emulex Connectivity Division (Broadcom, 2025). "The Emulex Secure Host Bus Adapter meets these needs by providing an elegantly simple solution that, once installed, encrypts all data across all applications."

"As enterprises face an ever-growing wave of cybersecurity threats, the Emulex Secure HBA stands out as a simple drop-in solution that enhances SAN security without compromising performance," said Brian Beeler, president, StorageReview.com. "In our testing, we found these HBAs excelled at securing in-flight SAN data encryption while seamlessly complementing existing security technologies. We're excited to see these adapters become a standard layer of improved SAN security in 2025, ***providing enterprises with an essential tool to safeguard their critical data***."

To sum up, we need these regulations in order to protect our sensitive data from unwanted access and theft and even if the initial investment in such systems which comply with these regulations are high, the risk of losing the data is even higher and it can translate in the loss of reputation and trust from our customers.

References

[1] Abhinandan K., S M Riha P., Sahana D., Abhishek N, Niyaz P. & Muhammad R., 2025. Developing a digital currency adoption scale: A validity and reliability study, *Sustainable Futures*, *9(100422)*, https://doi.org/10.1016/j.sftr.2024.100422.

[2] Broadcom Press Release [online] <www.broadcom.com> [Accessed on 20 February 2025]

[3] Cost of a Data Breach Report 2024, Ponemon Institute, [online] <https://www.ponemon.org/> [Accessed 20 February 2025]

[4] Digital Operational Resilience Act (DORA) [online] Available on European Insurance and Occupational Pensions Authority website <https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en> [Accessed on 20 February 2025]

[5] European Parliamentary Research Service [online] Available on <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf> [Accessed 20 February 2025].

[6] High common level of cybersecurity across the Union – NIS 2 Directive, European Parliament Legislative Observatory. [online] <

https://oeil.secure.europarl.europa.eu/oeil/en/procedure-file?reference=2020/0359(COD)> [Accessed 15 January 2025]
[7] L. Dionysopoulos et al. 2024 Central bank digital currencies: A critical review, *International Review of Financial Analysis 91* https://doi.org/10.1016/j.irfa.2023.103031
[8] Lin Tan et al. 2021, Research on the Development of Digital Currencies under the COVID-19 Epidemic. *Procedia Computer Science 187 p.89–96* https://doi.org/10.1016/j.procs.2021.04.037
[9] Papakonstantinou, V., 2022. Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? , Computer Law & Security Review, 44(105653), https://doi.org/10.1016/j.clsr.2022.105653.
[10] Storage Review Press Release [online] <www.storagereview.com> [Accessed on 20 February 2025]
[11] Treaty on the Functioning of the European Union (TFEU) [online] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4301854> [Accessed on 20 February 2025]
[12] Vandezande, N. 2024. Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor, *Computer Law & Security Review, 52(105890)*, https://doi.org/10.1016/j.clsr.2023.105890.
[13] Vikrant, S., & Mayank, Y., 2025. User adoption of digital currency: A systematic review and future agenda using TCCM approach, *Central Bank Review, 25(1), 100183*, https://doi.org/10.1016/j.cbrev.2024.100183.