CybelAngel

COMPLIANCE AND CYBERSECURITY

Understanding what DORA and NIS 2 mean for your organization

Is simplified compliance in our sights?

Well, with this 2025 guide, we aim to draw back the curtain and detail the answers to your cybersecurity compliance-related questions.

You are probably aware that the January 2025 enforcement of The Digital Operational Resilience Act (DORA) is reshaping how financial institutions approach digital resilience in Europe. It is the backbone of a unified EU approach to managing ICT-related risks. In this Ebook we delve into how it ensures that financial entities can navigate digital turbulence (and more!).

A new compliance framework making waves is NIS 2 , an expansive yet comprehensive toolkit marketed as essential for organizations looking to tighten up screws and bolts. While NIS 2 casts a wider net, covering 18 critical sectors and introduces clearer rules, we break down the complexity factor involved, including the tools it recommends to aid your compliance efforts.

In nervous conditions for markets, teams are still enforcing a proactive approach to security to stay primed and on alert for hackers. Achieving and maintaining compliance amid new changes and challenges lends itself to credibility. As large companies embrace a skittish global market, compliance is a competitive differentiator.

What is clear is that the numbers don't lie.

> A recent Gartner® survey reveals that improving third-party risk management is the top priority for over **82% of compliance leaders in 2025.** Meanwhile, Forrester® predicts that breach-related class-action costs will surpass regulatory fines by **50% in the coming year.**

It makes perfect sense that compliant companies are charging ahead. Whether you're a fintech startup or an international banking magnate, the message is clear: adapt or risk issues in the near future.

Grégory Faitas
Deputy CEO, CybelAngel

CONTENTS

CYBERSECURITY & COMPLIANCE

Why is compliance and cybersecurity a red hot topic?

The compliance process for cybersecurity is one of the most important and most mysterious steps of the chain, and this guide should serve as a compliance aide for mastering the steps involved.

We share what exactly regulators are looking for, a simple framework for structuring your checklist, how to prime for future compliance updates and even specific legislation per region you should be focusing on. **If you read this Ebook and take its advice, you will significantly increase your chances of staying on top of compliance.**

Do keep in mind that this content is for informational purposes only and does not constitute legal advice. Compliance requirements vary based on jurisdiction, industry, and organizational context.

Below we've created a simple rundown of the top complexities at play today.

A checklist to meet compliance fundamentals faster

Regulatory updates

- [ ] Renew FinCEN registrations and licenses
- [ ] Identify Applicable Regulations
- [ ] Engage with Legal and Compliance teams for interpretation
- [ ] Establish processes for monitoring
- [ ] Align with SEC cyber disclosure rules (SEC federal requirement)

Third-Party risks

- [ ] Conduct continuous vendor risk assessments (PCI DSS 4.0)
- [ ] Update agent verification letters
- [ ] Inventory vendors with system/data access
- [ ] Include security requirements in contracts
- [ ] Monitor Vendors for security and risk

Data governance

- [ ] Implement bias audits for AI systems (AI Act)
- [ ] Establish a framework defining roles and responsibilities, cybersecurity policies aligned with regulations
- [ ] Enhance CDD/EDD per FinCEN federal requirement
- [ ] Implement bias audits for AI systems (AI Act) (EU law with extraterritorial scope)

Incident response

- [ ] Test SOC 2 incident recovery plans quarterly
- [ ] Maintain breach reporting playbooks (SEC Rule 10b-5)
- [ ] Establish Incident Response Plan with clear communication protocols and post incident analysis process
- [ ] Maintain breach reporting playbooks (SEC federal requirement Rule 10b-5)

Risk assessment

- [ ] Catalog critical assets and data
- [ ] Analyze threats and vulnerabilities
- [ ] Prioritize risks based on likelihood and impact (consider regulatory focus)
- [ ] Develop risk treatment plans aligned with compliance requirements

Implement fundamental security controls

- [ ] Implement strong access management (MFA, Least privilege)
- [ ] Implement data security measures (Encryption, DLP)
- [ ] Deploy and maintain endpoint security (EDR)
- [ ] Implement network security (Firewalls, IDS/IPS, Segmentation)
- [ ] Establish a continuous vulnerability management program
- [ ] Conduct regular security awareness training

How do you know if you are properly evaluating your compliance framework as a CISO?

How do you actually gauge if your approach is working correctly? Well, you should start by tracking concrete metrics.

- **Measure your organization's cyberattack resilience using frameworks like MITRE CREF, focusing on mean time to detect (MTTD) and recover (MTTR).** Keep in mind that companies adhering to NIST CSF standards typically experience 40% fewer breaches.
- **Audit outcomes are another critical indicator:** firms that pass SOC 2 Type 2 audits resolve incidents 35% faster, thanks to alignment with ISO/IEC 27001 controls.
- **Regulatory alignment is another key tool:** Gartner® found that 78% of high-compliance organizations integrate at least three frameworks, such as DORA, PCI DSS 4.0, and GDPR.
- **Watch out for warning signs:** frequent audit delays often signal poor coordination between departments like legal and IT.
- **Another warning sign is rising IT spend without clear ROI:** IBM Security's 2024 'Cost of a Data Breach Report' tied excessive costs to fragmented tooling.. Third-party breaches are especially telling; 62% of incidents in 2024 stemmed from vendors lacking ISO 27001 certification.
- **To optimize, adopt AI-driven tools to automate control testing and cut manual workloads by half:** run tabletop exercises, such as Immersive Labs' ransomware simulations, to test real-world readiness. Benchmark annually against peers using maturity assessments like CAF or NIST CSF.

What are some strategic priorities to work on in 2025?

- **Adaptability:** Use RegTech for real-time regulatory updates
- **Unified frameworks:** Align NIST CSF with ISO 27001 to streamline audits.
- **Balanced AI adoption:** Innovate without compromising governance to avoid penalties.

By refining these layers—metrics, red flags, and optimizations—you can turn compliance from a checklist into a competitive advantage.

DORA
An outline and recommendations for CISOs

DORA

The Digital Operational Resilience Act (DORA) has applied since January 17, 2025, and imposes binding requirements on financial entities operating within EU member states, as well as on ICT service providers that supply critical services to those entities.

Why does it matter for cybersecurity professionals?

DORA regulations explicitly target ICT systems by introducing rules for ICT risk management frameworks, incident reporting, digital operational resilience testing, and oversight of ICT third-party risks. While NIS2 focuses broadly on network and information security across critical sectors, DORA goes further by embedding operational resilience requirements specifically for the financial sector, covering both ICT risk management and third-party dependencies.

New regulatory technical standards (RTS) were implemented by three European Supervisory Authorities (ESAs)—the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA) to ensure that all financial entities such as banks, insurance companies, investment firms and crypto-asset service providers in Europe are resilient in the face of rising cyberattacks.

When outsourcing critical functions, DORA regulation requires financial service providers to:

- **Comply with DORA regulations from day one.**
  Financial entities are required to critical vet third party ICT service providers according to DORA's standards. This means that contracts can only be entered into once these requirements are met.

- **Conduct ongoing audits.**
  Financial institutions must conduct regular audits to determine the risk of a third-party provider. Critical ICT third-party service providers must cooperate with all ongoing audits overseen by the competent authorities.

- **Update third-party contracts with DORA requirements.**
  Contracts with third-party service providers must include detailed information about the service provider and critical ICT security measures. Such information can include the location where the services will be provided, the locations of data storage, and data protection provisions in case of an attack.

- **Include third-party contractors in training programs.**
  Financial entities are required to include their critical ICT third party providers in training programs to improve cyber resilience.

- **Develop water-tight exit strategies.**
  When a contract between the critical ICT service provider and the financial institution is dissolved, there is still a responsibility to ensure protection against potential threats. Exit plans need to be documented, tested, and reviewed regularly to prove compliance.

- **Termination in case of non-compliance.**
  DORA explicitly states that if an critical ICT third-party provider is unwilling or unable to comply with the regulations, the financial entity must exit the contract.

The mutually collaborative oversight framework helps manage the business relationship between the third-party provider and the financial institution to better mitigate cyber risks such as supply chain vulnerabilities. DORA regulations require financial service providers to:

1. Vet third party critical ICT service providers according to DORA's standards before entering into contracts.
2. Conduct regular audits to determine the risk of a critical ICT third-party provider
3. Update critical ICT third-party contracts to include detailed information about the service provider and ICT security measures.
4. Include critical ICT third-party contractors in training programs to improve cyber resilience.
5. Develop and regularly test exit strategies to ensure protection against potential threats, even after the contract is dissolved.
6. Terminate the contract if the critical ICT third-party provider is unwilling or unable to comply with the regulations.
7. Terminate the contract if a critical ICT third-party provider is unwilling or unable to comply with regulations, and leverage CybelAngel's impact by proactively launching third-party management assessments. These include comprehensive EASM evaluations on your key providers to identify exposures, ensure compliance, and reduce business risk through rapid detection and actionable intelligence.

4 recommendations for you to meet

In order to meet and maintain compliance, focus on the following 5 areas.

Follow an ICT risk management framework

- [ ] Conduct a comprehensive risk assessment to identify vulnerabilities in ICT systems.
- [ ] Map critical ICT assets and their dependencies to business functions.
- [ ] Assign clear roles and responsibilities for managing ICT risks.

Third-Party risk management

- [ ] Vet all critical third-party ICT service providers to ensure they meet DORA standards before entering contracts.
- [ ] Update contracts to include detailed provisions on data security, storage locations, and incident response protocols.
- [ ] Conduct regular audits and ensure third-party providers participate in training programs on cyber resilience.
- [ ] Develop robust exit strategies to mitigate risks when terminating contracts with non-compliant providers.

Implement incident reporting mechanisms

- [ ] Set up standardized templates for reporting major ICT incidents to competent authorities.
- [ ] Notify clients promptly about incidents and outline mitigation measures.
- [ ] Perform root-cause analyses for all incidents to prevent recurrence.

Conduct regular resilience testing

- [ ] Schedule annual threat-led penetration testing (TLPT) to simulate real-world cyberattacks.
- [ ] Use the results of these tests to refine operational resilience strategies.

Reviewing NIS 2

On February 26, 2024, NIST released Cybersecurity Framework 2.0 in collaboration with stakeholders from organizations of all sizes. It guides organizations in managing cybersecurity risks with a taxonomy of high-level cybersecurity outcomes, useful for any organization regardless of size, sector, or maturity, to better understand, assess, prioritize, and communicate their cybersecurity efforts.

NIS 2 is a mandatory EU cybersecurity regulation for critical sectors, while NIST CSF 2.0 is a voluntary, globally applicable framework developed in the U.S. to guide organizations in managing cybersecurity risks.

NIST CSF 2.0 scope

The scope of NIST CSF 2.0 has expanded beyond U.S. critical infrastructure to address global cybersecurity challenges, making NIST practices usable by all organizations, regardless of sector. The framework includes:

- **CSF core**
  A taxonomy of high-level cybersecurity outcomes that helps organizations manage their cybersecurity risks, with a hierarchy of functions, categories, and subcategories detailing each outcome applying to all IT systems.

- **CSF organizational profiles**
  Details for describing an organization‘s target cybersecurity posture.

- **CSF tiers**
  Context for how an organization views its cybersecurity risks and the processes to manage those risks, including governance and management practices.

NIST CSF 2.0 is widely recognized as a critical resource for organizations seeking to improve their cybersecurity posture and is essential for cybersecurity compliance. Organizations can map various cybersecurity standards with the NIST framework to adhere to regulatory requirements for identifying, detecting, and recovering from cybersecurity incidents. NIST compliance provides a comprehensive foundation that aligns with many existing compliance standards, such as GDPR, HIPAA, ISO, and CIS Controls.

One significant change is the addition of a new Govern function. This helps organizations make informed decisions on policy and management practices aligned to a larger cybersecurity strategy, including organizational context, risk management strategies, and supply chain risk management.

The core functions of NIST CSF 2.0 are:

Govern
Provides outcomes for the organization‘s ability to achieve and prioritize the five other functions, considering the broader organizational context for sustainable results, including establishing a cybersecurity strategy, considering cybersecurity supply chain risk management, and cybersecurity compliance with regulatory bodies.

Identify
Asks organizations to consider their current cybersecurity threat landscape and identify areas for improvement within the policies, plans, processes, procedures, and management practices.

Protect
Addresses safeguards to manage the organization‘s cyber risk, preventing vulnerabilities from being exploited, including identity management, access control, data security, platform security, and infrastructure resilience.

Detect
Determines how quickly organizations can discover a potential threat and analyze adverse events that indicate cyberattacks, supporting successful incident response and recovery activities for enhanced mitigation of threats.

Respond
Provides guidelines for actions to take after a threat is uncovered to contain cyber threats, covering incident management, analysis, mitigation, reporting, and communication of cyber attacks.

Recover
Helps organizations identify assets and operations impacted by a cyber attack and supports the organization’s return to normal operation.

Implementing NIST CSF 2.0 can help organizations meet regulatory requirements, improve supply chain transparency, build a resilient cyber risk management strategy, be adaptive and flexible, and future-proof the organization.

Recommendations for implementing NIST CSF 2.0

ICT risk management

- [ ] Follow an ICT cybersecurity risk management framework.
- [ ] Conduct a comprehensive risk assessment to identify vulnerabilities in ICT systems.
- [ ] Map critical ICT assets and their dependencies to business functions.
- [ ] Assign clear roles and responsibilities for managing ICT risks.

Third-Party risk management

- [ ] Vet all third-party ICT service providers to ensure they meet standards before entering contracts.
- [ ] Update contracts to include detailed provisions on data security, storage locations, and incident response protocols.
- [ ] Develop robust exit strategies to mitigate risks when terminating contracts with non-compliant providers.
- [ ] Conduct regular audits and require third-party providers to participate in cyber resilience training programs, while leveraging CybelAngel's capabilities to continuously assess and monitor your key vendors. This ensures ongoing compliance, strengthening cyber defenses, and reducing risk through actionable intelligence and rapid exposure detection.

Incident reporting

- [ ] Set up standardized templates for incident response and communication with relevant internal and external stakeholders.
- [ ] Notify clients promptly about incidents and outline mitigation measures.
- [ ] Perform root-cause analyses for all incidents to prevent recurrence.

Resilience testing

- [ ] Schedule regular penetration testing, red teaming, and risk-based security assessments to simulate real-world cyberattacks in line with NIST guidance.
- [ ] Use the results of these tests to refine operational resilience strategies.

Businesses without an existing cybersecurity strategy can start with templates and information provided by NIST, such as the Small Business Quick Start Guide, which makes suggestions for each of the core functions.

To protect critical infrastructure as cyber threats continue to evolve, organizations must take an adaptive approach to their cybersecurity posture. NIST CSF 2.0 represents a vital advancement in cybersecurity practices with a proactive approach to managing risks and ensuring compliance.

COMPLIANCE AT CYBELANGEL

We align our services and expertise with leading frameworks and regulations, including NIST CSF 2.0, the EU's Digital Operational Resilience Act (DORA), and the NIS 2 Directive, to empower organizations to achieve and maintain a robust security posture.

NIST CSF 2.0

The NIST Cybersecurity Framework 2.0 provides a comprehensive and adaptable structure for managing cybersecurity risks. Its six core functions—Govern, Identify, Protect, Detect, Respond, and Recover—offer a clear roadmap for organizations of all sizes and sectors. By aligning with NIST CSF 2.0, companies can improve their risk management, enhance compliance with various standards (like GDPR, HIPAA, ISO), and build resilience against cyber threats. CybelAngel's platform directly supports the implementation of NIST CSF 2.0 by providing external risk visibility and actionable threat intelligence across each of these functions. Addressing European Regulatory Requirements: DORA and NIS 2

CybelAngel also helps organizations address the specific requirements of key European regulations:

DORA (Digital Operational Resilience Act)

DORA aims to strengthen the digital operational resilience of the financial sector in the EU. It mandates that financial entities implement robust ICT risk management frameworks, conduct regular resilience testing, and establish incident reporting mechanisms. CybelAngel's external risk monitoring capabilities provide critical visibility into third-party risks and vulnerabilities, enabling financial institutions to meet DORA's requirements for supply chain security and incident detection.

NIS 2 Directive

The NIS 2 Directive expands the scope of cybersecurity regulations to a wider range of critical sectors across the EU. It sets out minimum cybersecurity standards and incident reporting obligations for essential and important entities. CybelAngel's proactive threat detection and vulnerability management capabilities help organizations comply with NIS 2 by identifying and mitigating cyber risks before they can impact essential services.

The EU's regulatory landscape has reached a critical inflection point.

With DORA now enforceable since January 2025 and NIS 2's entity lists due on April 17, 2025, organizations face a clear mandate: comply or confront escalating risks. As ENISA Executive Director Juhan Lepassaar warns, "NIS 2 isn't just about rules—it's a cultural shift. Entities must embed resilience into their DNA, or face systemic vulnerabilities." This cultural shift is reflected in the way DORA and NIS 2 intersect. Financial entities follow DORA's ICT risk management and incident reporting requirements instead of NIS 2's parallel provisions, a critical "lex specialis" exemption that streamlines compliance for the sector.

Meanwhile, NIS 2's expanded scope now covers over 100,000 EU entities across energy, healthcare, transport, and other critical sectors, with non-compliance fines reaching up to €10 million or 2% of global turnover, underscoring the high stakes involved.

The numbers tell a compelling story.

According to Gartner, 82% of compliance leaders prioritize third-party risk management, yet a BBC Cyber Report reveals that 68% of organizations still lack real-time vendor monitoring capabilities. DORA further raises the bar by requiring financial firms to conduct annual penetration tests and threat-led simulations, ensuring that resilience is tested and proven regularly. To meet these demands, organizations must automate governance processes, as manual efforts cannot scale to satisfy NIS 2's 24-hour incident reporting or DORA's rigorous ICT third-party audits. Leveraging established frameworks like ISO 27001 can accelerate compliance, covering approximately 85% of NIS 2 and DORA requirements. Moreover, external attack surface monitoring is no longer optional; as Kroll's 2025 Cyber Forecast highlights, 60% of breaches originate from unmanaged digital assets, making continuous external visibility critical to reducing risk.

The verdict is clear: compliance in 2025 is no longer a mere cost center but the currency of trust. The price of inaction far outweighs the investment required to build resilient, compliant operations. Organizations that embrace this shift will not only avoid penalties but also gain a competitive edge in an increasingly risk-averse market.

For those ready to take the next step, CybelAngel will help you to navigate these complex requirements and future-proof your cybersecurity strategy.

How to leverage CybelAngel to maximise NIS 2 and DORA Compliance

Compliance Goal / Regulatory Requirement	Clarified Contribution	CybelAngel Modules
Comprehensive ICT Asset Inventory & Exposure Visibility DORA Art. 5(1)(c); NIS2 Art. 21(2)(b)	Identifies exposed Shadow IT, IoT, RDP, cloud assets, and their vulnerabilities;	Attack Surface Management
External Credential Leak Monitoring & Access Control DORA Art. 6; NIS2 Art. 21(2)(c)	Detects leaked credentials on open/dark web; supports internal IAM enforcement	Credential Intelligence
Sensitive Data Protection & Data Loss Prevention DORA Art. 5(1)(d); NIS2 Art. 21(2)(d); GDPR Art. 32	Detects exposed sensitive data in cloud, S3 buckets, and databases; complements encryption and access controls	Data Breach Prevention
Threat Intelligence & Early Warning DORA RTS (Threat Intelligence); NIS2 ID.RA-3	Provides actionable external threat insights, including threat actor activity and ransomware trends	Threat Intelligence Dark Web Monitoring
Phishing & Impersonation Detection DORA Art. 5(1)(e); NIS2 Art. 21(2)(e)	Detects phishing attempts, fraudulent and impersonation domains; strengthens incident detection	Domain Protection
API Security & Vulnerability Management DORA Art. 5(1)(d); NIS2 Art. 21(2)(b,d)	Identifies unsecured or unknown APIs exposed to the internet; supports attack surface discovery and risk reduction	API Exposure Monitoring

Brand Protection & Executive Impersonation **(Indirectly related to DORA/ NIS2 reputation and phishing response)**	Detects fake brand or personnel profiles on social media; supports brand protection and executive impersonation detection	Social Media Impersonation
Third-Party Risk Assessment & Due Diligence **DORA Art. 28; NIS2 Art. 21(2)(f)**	Assesses compliance and cyber resilience of key third-party providers through EASM and due diligence	Third Party Assessment / Due Diligence

CybelAngel

Detect, Anticipate, Control External Threats

CybelAngel is the world's leading platform for external threat intelligence.

Secure your digital activities with CybelAngel, the only comprehensive threat Intelligence provider.

START NOW