A CISO's Compliance Playbook

Strategies to meet NIS2, DORA, and PS21/3 requirements

BITSIGHT

Table of Contents

CISOs Leading the Charge Amid New Regulations 3

The Regulatory Trinity: NIS2, DORA, and PS21/3 5

Lessons Learned from the State of Supply Chain Cybersecurity 13

Leveraging Compliance as a Strategic Advantage 16

Five Strategies Every CISO Should Prioritize Now 19

Checklist: 30 Questions to Self-Assess Compliance Readiness 23

Strategizing for Success Beyond Compliance 26

Legal Disclaimer: *This ebook does not constitute legal advice, and you should consult your own legal counsel with respect to the applicability of laws and regulations to your own business operations.*

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

01

CISOs Leading the Charge Amid New Regulations

01 CISOs Leading the Charge Amid New Regulations

Tim Grieveson
Senior Vice President -
Global Cyber Risk Advisor, Bitsight

The emergence of significant and important changes in cyber risk regulations like NIS2, DORA in the EU, or PS21/3 in the UK, signals a seismic shift toward strengthening cyber resilience and enforcing accountability—whilst improving incident response to combat the knock-on impact of cyber threats to our digital economy.

As governments and regulatory bodies formally recognize the importance of cybersecurity in safeguarding critical infrastructure, CISOs can turn defencive functions into business differentiators that enable growth and protect revenue.

Championing regulations is not just a matter of checking compliance boxes: it's an opportunity to become a business leader. With more critical and visible roles, CISOs are responsible for measuring and reducing exposure, improving cybersecurity postures, building resilience, allocating resources for compliance, understanding third-party risks, and activating governance processes to maintain executive sponsorship.

Organisations that demonstrate strong cybersecurity governance and leadership are better positioned to build and maintain trust with shareholders, regulators, and customers. The ability to articulate an understanding of risks—and their impact on business operations—will prove to be competitive advantages.

This playbook offers helpful definitions, practical advice, and recommendations from our global team of cyber risk advisors to use throughout your journey towards regulatory compliance.

> **"Key to success is ensuring your programme is security led as opposed to compliance led. When this is aligned to measurable frameworks such as NIST, ISO27001, or SOC2 it builds executive and customer trust."**

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

02

The Regulatory Trinity: NIS2, DORA, and PS21/3

02 The Regulatory Trinity

NIS2, DORA, and PS21/3—these acronyms carry the weight of a new era in cybersecurity, just like GDPR did for personal data a few years ago. The genesis of these regulations lies in the imperative need for resilience. In a world where digital disruptions can cripple nations and economies, the industry needed a shift from reactive defence to proactive fortification.

The Network and Information Systems 2 Directive (NIS2)

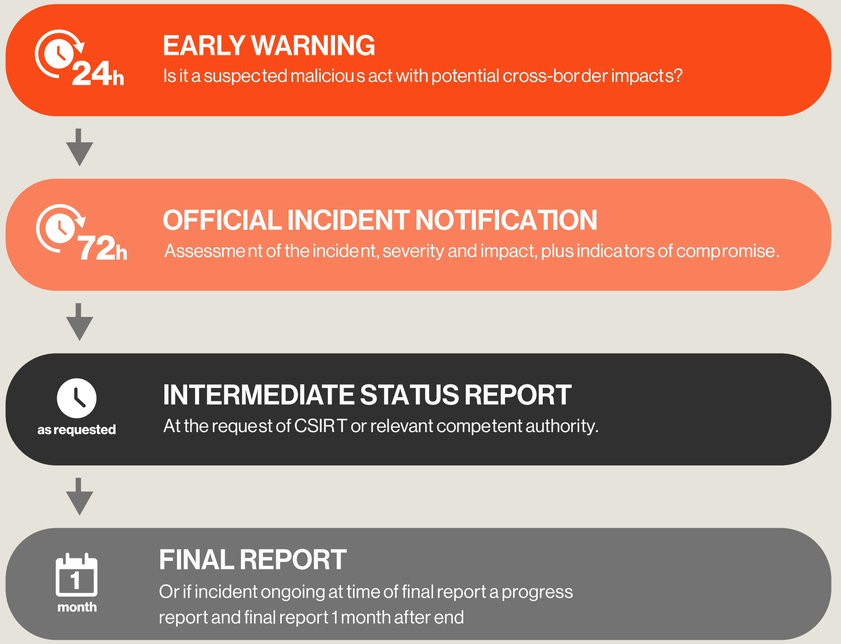
NIS2 aims to get organisations up to speed and establish a higher level of cybersecurity and resilience within organisations of the European Union. Subject entities need to implement robust cybersecurity measures, incident response plans, and reporting mechanisms.

Under NIS2, risk management means:

- Management is accountable for non compliance
- Essential and important entities must take security measures
- Organisations must notify incidents within a given time frame

One of the important requirements in NIS2 will be the very short reporting obligation notice for incidents. This involves maintaining continuous monitoring and establishing a skilled emergency response team capable of swift and accurate reactions—with active participation from suppliers.

The phased process to notify the relevant competent authority or CSIRT (Computer Security Incident Response Team) looks like this:

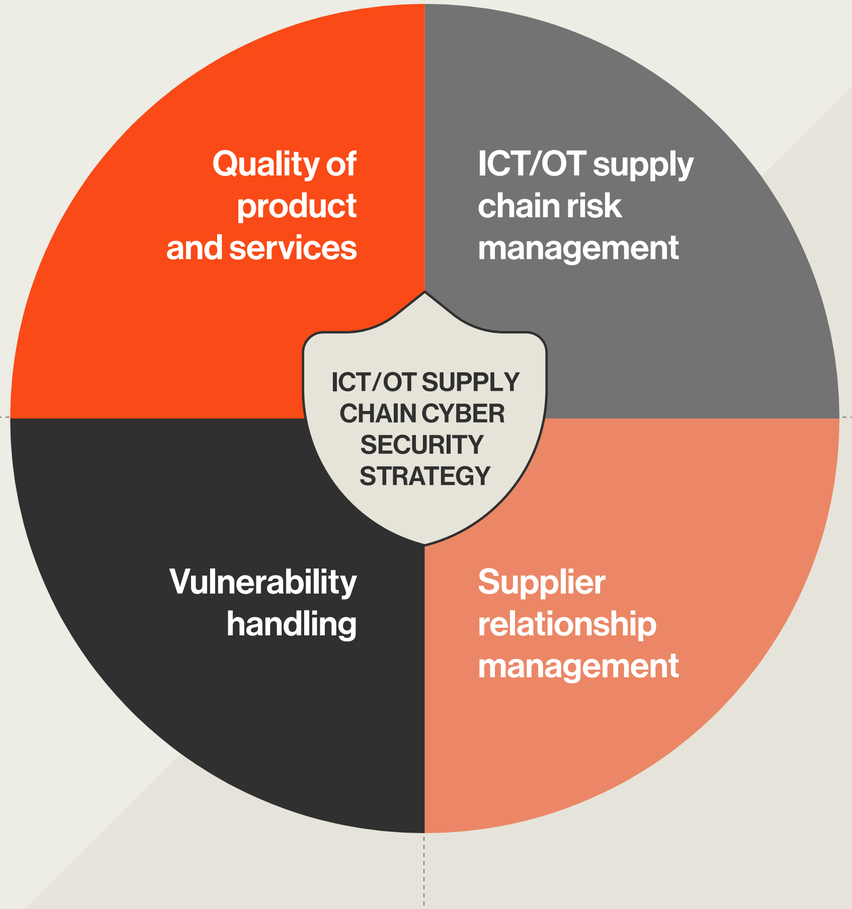


Source: National Cyber Security Centre

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

With a strong focus on supply chain cybersecurity, NIS2 entails a risk-based approach to four key areas: supply chain risk management, supplier relationship management, vulnerability handling, and quality of products and practices of suppliers and service providers.

- Provide secure products and services
- Have the infrastructure protected
- Have secure processes in place
- Have technical measures implemented
- Create transparency in ICT/OT supply chain
- Measure the quality of products and services



- Understand the supply chain
- Identify suppliers and providers
- Understand the potential risks for the own organisations and for end customer

- Manage vulnerabilities
- Know your assets
- Understand risks of vulnerabilities
- Patch vulnerabilities
- Have a defined maintenance policy

- Manage ICT/OT supply chain
- Have policies and agreements in place
- Have cybersecurity requirements defined Monitor supplier and service provider performance
- Manage changes

Source: ENISA

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

Who is NIS2 meant to target?

NIS2 defines two categories for entities in scope: important and essential. Entities in both categories will have to meet the same requirements. However, the distinction will be in the supervisory measures and penalties:

- Essential entities will be required to meet supervisory requirements as of the introduction of NIS2—both preventively and after verification of an incident.
- Important entities will only be subject to ex-post supervision—that is, in case authorities receive evidence of non-compliance.

Smaller organisations are not necessarily excluded: Member States can extend these requirements if an enterprise fulfills specific criteria that indicate a key role for society, the economy, or for particular sectors or types of services.

Essential

- Energy
- Transport
- Banking
- Health
- Drinking water
- Wasting water
- Financial market infrastructures
- Digital infrastructure and ICT service management
- Public administration
- Space

Inspection ex-ante

Important

- Postal and courier services
- Waste management
- Manufacturing
- Chemicals
- Food production
- Digital providers
- Research

Inspection ex-post

Regardless of size, the NIS2 Directive also applies to public administration entities of central governments and public administration entities at a regional level. Exempt from this are public administrations whose activities are in the areas of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences.

Quick facts

Who:
Large enterprises (headcount over 250 or more than 50M turnover) or medium (headcount over 50 or more than 10M turnover) from impacted sectors. Public administration entities of central governments and at a regional level, regardless of size.

What:
Implement effective measures to secure their network and information systems, report significant incidents to national authorities, and contribute to a collective effort to enhance the overall cyber resilience of critical sectors.

When:
Published January 16, 2023.
Local legislations to be created and adopted by Member States as of October 17, 2024.

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

Cyber risks and threats impacting critical infrastructure systems range anywhere from ransomware to supply chain attacks and cyber espionage. By setting common standards and requirements, NIS2 aims to mitigate these risks and enhance the overall cybersecurity posture of organisations.

The potential risks extend across the supply chain. NIS2 indicates in Article 21.(3)[1] that entities must consider the security practices of their third-parties:

"(...) take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures."

[1] Source: NIS2 Directive, Article 21

A real-world example of critical infrastructure risk

Bitsight identified nearly 100,000 exposed industrial control systems (ICS) across 96 countries, including the United Kingdom, Italy, France, the Netherlands, Germany, and Spain. This could allow an attacker to control physical infrastructure such as power grids, traffic light systems, and security and water systems.

Read the research →

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

The Digital Operational Resilience Act (DORA)

DORA aims to address risks affecting information and communication technology (ICT) by establishing a framework for enhanced operational resilience across the financial sector—including holistic cyber risk management, incident reporting, and coordination among financial entities and regulatory authorities.

Who is DORA meant to target?

DORA will specifically focus on 20 types of regulated EU financial entities. These include banks and providers of other financial services such as credit or payment, electronic money institutions, investment firms, and crypto-asset service providers. It will also encompass service providers in areas such as security depositories, central counterparties, trading venues, trade repositories, alternative investment funds and management, data reporting, insurance and reinsurance, occupational retirement pensions, credit rating, statutory auditing, or crowdfunding.

With a shared set of rules across the EU, DORA creates a comprehensive approach to ensuring organisations can withstand, respond, and recover from the impacts of ICT incidents, thereby continuing to deliver critical and important functions and minimizing disruption for customers and the financial system.

This set of technical standards must be adopted by financial entities and their critical third-party service providers in their ICT systems by January 17, 2025.

The number and severity of cyber threats associated with ICT risks has been growing steadily over the last years. The cases where organisations have dealt with attacks targeting ubiquitous software and products—including SolarWinds Orion and Microsoft Exchange—further prove that cyber threats continue to evolve.

Quick facts

Who:
Service providers within the EU financial sector.

What:
Establish effective risk management, incident response, and reporting practices to ensure and enhance operational resilience.

When:
Published January 16, 2023.
In effect by January 17, 2025.

What are examples of ICT risks?

- DDoS attacks
- Malware attacks, including ransomware
- Hardware or software vulnerabilities
- Third-party or supply chain attacks
- Data manipulation attacks
- Cloud service outages
- Human errors or insider threats

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

DORA Key Tenets

DORA requirements span across five pillars:

If a company is part of the financial sector and falls under both DORA and NIS2 scopes, which EU law takes precedence?

DORA. As a specific law for the financial sector, it takes precedence over NIS2 as a general law.

- **Governance** (accountable management body)
- **Risk management framework and associated activities** (identification, protection and prevention, detection, response and recovery, learning and evolving, crisis communication)

- **Standardized incident classification**
- Compulsory and standardized **reporting of major incidents**
- **Anonymized EU-wide reports**

- **Comprehensive testing program**, with a focus on technical testing
- Large-scale, **threat-led live tests** performed by independent testers every three years

- **Guidelines on information sharing arrangements** for cyber threats and vulnerabilities

- **Strategy, policy, and standardized register of information**
- **Guidelines** for pre-contract assessment, contract contents, termination, and stressed exit
- **Create oversight framework for critical providers** across the EU with clear requirements and penalties

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

The UK's Prudential Standard (PS21/3)

PS21/3 shares the overarching goal of enhancing digital resilience with DORA, but with a broader scope. It encompasses critical entities in the ICT sector, including a broader range of financial entities such as banks, building societies, and designated investment firms in the United Kingdom.

The policy recognizes the importance of the ICT sector in supporting the functioning of essential services across various industries, and seeks to establish measures to prevent and respond to cybersecurity incidents.

Similar to DORA, PS21/3 demands subject organisations to elevate their cyber risk management initiatives across:

- Risk management and prevention to enhance their overall cybersecurity posture.
- Incident response and recovery to ensure swift and effective responses to cybersecurity incidents and minimize potential disruptions.
- Information sharing and cooperation with other organisations and with competent authorities.

Regulatory oversight and enforcement from authorities with the power to conduct audits and impose penalties for non-compliance.

Quick facts

Who:
Firms deemed critical within the financial ICT sector.

What:
Implement robust cybersecurity and incident response capabilities, and cooperate with authorities to enhance the overall resilience of the ICT sector.

When:
Published March 31, 2022.
In effect by March 31, 2025.

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

03

Lessons Learned from the State of Supply Chain Cybersecurity

03 Lessons Learned from the State of Supply Chain Cybersecurity

Establishing good practices for supply chain cybersecurity at the EU level is now more important than ever.
But how are organisations doing in this front? And what can we learn from the current situation?

Based on findings from the European Union Agency for Cybersecurity (ENISA), we observe the following trends and implications.

The growing significance of third-party risk management (TPRM) in ensuring supply chain resilience—covering risk assessments, supplier relationship management, and vulnerability management.

86% of organisations implement (ICT/OT) supply chain cybersecurity **policies.**

Company Size

0-100	101-1000	> 5000
62%	83%	100%

Sector

Banking	98%	Transport	92%
Healthcare	93%	Drinking water	74%
Energy	92%	Digital Infrastructure	60%

Only holistic, integrated cyber risk management can account for sector-specific regulations while contributing to collective resilience.

Continuous monitoring and automation can augment capabilities in threat detection, response, and mitigation.

Source: Good Practices for Supply Chain Cybersecurity Report, ENISA

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

03 Lessons Learned from the State of Supply Chain Cybersecurity

Businesses begin to recognize supply chain cybersecurity as a business enabler and competitive advantage instead of an operational expenditure.

47%
allocate budget

Sector

Banking	**71%**	Healthcare	**61%**
Healthcare	**61%**	Transport	**53%**

24%
have dedicated **roles and responsibilities** for ICT/OT supply chain cybersecurity.

Cybersecurity leaders face increased accountability, and view regulatory compliance as a baseline requirement for building a robust cybersecurity posture.

61%
require **security certification** from suppliers

43%
use **security rating** services.

37%
demonstrate **due diligence** or risk assessments.

It's interesting to see that while 83% of organisations conduct initiatives for supply chain security, only 47% of them allocate budget specifically for those activities. This also illustrates the challenges of addressing supply chain risk as an independent process.

Source: Good Practices for Supply Chain Cybersecurity Report, ENISA

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

04

Leveraging Compliance as a Strategic Advantage

04 Leveraging Compliance as a Strategic Advantage

The foundations for one regulation often serve other regulations, as many strive to ensure the same goals: transparency, enabling business securely, establishing accountability, and providing appropriate governance and reporting.

When a new directive emerges, you are probably already doing some of the work. Organisations that have Vendor Risk Management (VRM) and Third-Party Risk Management (TPRM) programs in place already have a solid start to comply with the new supply chain resilience and reporting requirements as they have governance, process, and metrics or reports needed for the regulation.

Likewise, most multinational banks already have strategies in place to cope with enhancing operational resilience and therefore the new regulations in the financial sector build upon the foundations already in place.

While some may view this as another obligation that diverts attention away from their day-to-day responsibilities, many cybersecurity leaders are embracing this momentous occasion as strategic advancement to **cement their critical role in the business.**

> **“Security leaders, Legal, and Procurement professionals already have a tsunami of workload. However, these upcoming regulations tightly align with business objectives and industry standards. Finding partners and solutions that make the task easier is key.”**

Tim Grieveson
Senior Vice President -
Global Cyber Risk Advisor, Bitsight

©2024, BitSight Technologies, Inc. and its affiliates (“Bitsight”). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

Rather than seeing these initiatives as challenges, think of them as strategic opportunities. These are some common misconceptions and how they could be viewed from a different perspective:

Traditional Belief	Strategic Opportunity
Cybersecurity management —and leadership— is perceived as solely focused on reducing risk.	By taking ownership of compliance initiatives, CISOs showcase their commitment to not just securing the organisation but also being accountable stewards of its digital assets. This enhances their credibility as business leaders.
Compliance is simply a checkbox exercise with no tangible business benefits.	Regulatory alignment supports broader business goals for competitive advantage, enhances market positioning, and increases credibility by demonstrating robust cybersecurity practices. This attracts customers who prioritize security-conscious partners.
Meeting regulatory requirements is not critical to business continuity.	Security teams ensure resilience by integrating compliance efforts with effective incident response and continuity planning, fostering cross-functional collaboration.
Executives and boards do not engage with cybersecurity talk.	The CISO can effectively communicate insights and benchmarks on cybersecurity maturity, becoming an indispensable advisor to top-level decision-makers.

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

05

Five Strategies Every CISO Should Prioritize Now

05 Five Strategies Every CISO Should Prioritize Now

1. Holistic Cyber Risk Management

Strategy: Develop a comprehensive framework that covers risk, performance, and exposure management workflows across your organisation and your supply chain—from governance and cyber risk quantification to External Attack Surface Management (EASM) and Third-Party Risk Management (TPRM).

Implication: Streamline compliance efforts by identifying commonalities across regulations, ensuring a unified, risk-based approach that covers risk management, incident response, data protection, and reporting.

2. Continuous Monitoring and Adaptive Security

Strategy: Implement continuous monitoring practices to detect and respond to cybersecurity threats in real-time, and adopt an evolving security model based on emerging threats and regulatory requirements.

Implication: Proactively identify and mitigate risks, emerging vulnerabilities, and changes in your security posture—or that of your vendors. Respond swiftly to ensure ongoing compliance and resilience.

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

3. Benchmarking and Transparent Reporting

Strategy: Provide accurate and timely information about cybersecurity incidents, potential risks, and the measures taken to address them. As executive boards and regulators become increasingly involved in risk discussions, they appreciate quantifiable metrics that communicate how your company performs—both absolutely and relative to industry benchmarks, especially as regulatory expectations vary across industries.

Implication: Build trust with Boards and regulators by sharing independent, comparable, and consistent benchmarking data—an objective analysis of your organisation's cybersecurity performance based on quantitative data.

4. Accountability and Management Responsibility

Strategy: Management now needs to take responsibility for the organisation's cybersecurity maturity. Implement a robust framework for accountability that includes risk assessments, approval of risk treatment plans, and cybersecurity training.

Implication: Embedding accountability into management responsibilities contributes to a cultural shift where cybersecurity is not just an IT concern, but a fundamental aspect of overall governance. This fosters a collective responsibility for cybersecurity at all levels of the organisation.

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

5. Cybersecurity Training and Culture

Strategy: Train management and all levels of employees for more in-depth cybersecurity knowledge. Make cybersecurity everyone's job by ensuring they understand their role in maintaining compliance and resilience. This will reduce the risk of insider threats and human error.

Implication: Boards and regulators will notice that the organisation is fostering a cybersecurity-aware culture through regular training and awareness programs.

How to Disclose Benchmarking Data: Real-World Examples

- Equifax includes cybersecurity performance benchmarks in its Annual Security Report. Equifax focuses on its performance compared to peers in the Finance and Technology sectors, noting that its security capabilities "ranked in the top 1% of Technology companies and top 3% of Financial Services companies analyzed."
- Darling Ingredients leverages cybersecurity performance benchmarks in its Annual ESG Report, describing its cyber program as "being in the top 10% of the Energy/Resource Industry."
- Schneider Electric and AVEVA include cybersecurity performance benchmarks in their Annual Sustainability Report, describing their programs as being ranked "in the Top 25% in external ratings for Cybersecurity performance."

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

06

Checklist: 30 Questions to Self-Assess Compliance Readiness

06 Checklist: 30 Questions to Self-Assess Compliance Readiness

The answers to the following questions can guide the development of action plans and improvements to ensure ongoing compliance and resilience against cybersecurity threats.

Regulatory Landscape:

- Are we up-to-date with the latest regulatory requirements in our industry and region?
- Have we identified and analyzed the specific compliance requirements relevant to our organisation?

Governance and Policies:

- Do we have a comprehensive set of cybersecurity policies and procedures in place?
- Are these policies aligned with regulatory standards and industry best practices?

Cyber Risk Management:

- Have we conducted a recent and thorough cybersecurity risk assessment?
- Are we actively monitoring and managing identified risks, including third-party risk, emerging threats, and zero day events?

Vendor and Third-Party Risk Management:

- Do we have a centralized and up-to-date vendor inventory, with a drill-down view into vendors across Business Units?
- Do we perform risk assessments and continuously monitor the cybersecurity practices of our vendors?

Incident Response:

- Do we have a well-defined incident response plan in place that meets business continuity and disclosure expectations?
- Have we conducted tabletop exercises or simulations to test the effectiveness of our incident response capabilities?

Business Continuity and Resilience:

- Is there a business continuity plan in place that considers cybersecurity incidents?
- Have we tested the organisation's ability to recover from a cybersecurity incident and overall resilience strategy?

Security Controls and Technologies:

- Are our security controls and technologies in line withregulatory requirements?
- Have we implemented encryption, firewalls, intrusion detection/prevention systems, and other relevant security measures?

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

Access Controls and Identity Management:

- Are access controls aligned with the principle of least privilege?
- Is identity and access management robust, including regular reviews and updates?

Critical Assets:

- Have we identified, documented, and classified critical infrastructure assets or business services?
- Is there a tailored cybersecurity strategy based on sector-specific requirements?

Training and Awareness:

- Do employees receive regular cybersecurity training and awareness sessions?
- Are employees aware of their roles and responsibilities in maintaining compliance?

Documentation and Recordkeeping:

- Is there proper documentation of our cybersecurity policies, risk assessments, and incident response activities?
- Are records maintained to demonstrate compliance efforts?

Legal and Regulatory Reporting:

- Do we have mechanisms in place for timely and accurate reporting to regulatory authorities?
- Have we established communication protocols for notifying relevant stakeholders in the event of a data breach or cybersecurity incident?

Continuous Monitoring:

- Is there a strategy for leveraging cyber risk analytics for continuous compliance monitoring?
- How is the continuous monitoring data used in our compliance reporting?

Continuous Improvement:

- Do we have a process for continuous improvement of our cybersecurity program?
- Are lessons learned from incidents and audits used to enhance our cybersecurity posture?

Cross-Functional Collaboration:

- Do we have effective communication and collaboration with other departments, such as legal, procurement, HR, and IT?
- Are compliance efforts integrated into broader organisational strategies?

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

07

Strategizing for Success Beyond Compliance

07 Strategizing for Success Beyond Compliance

NIS2, DORA, and PS21/3 are not just legal frameworks; they are industry catalysts. The journey can be challenging, but with confidence and the right tools, it's easier to navigate.

To comply with increasingly complex cybersecurity regulations, organisations need clear visibility into their digital ecosystem and attack surface. They must also be able to identify risks and assess the controls they have in place to mitigate them, ultimately empowering them to measure and improve security performance over time.

CISOs should now prioritise six main areas:

1. **Frameworks:** Align security and risk programmes to industry best practice frameworks, such as NIST, ISO27001, or SOC2.
2. **Resilience Testing:** Perform regular digital operational resilience testing and use feedback to continuously improve.
3. **Third-Party Risk:** Urgently prioritise third-party risk management governance, vendor risk assessments, and remediation.
4. **Awareness Training:** Ensure employees and contractors receive security awareness training and know how to report incidents in a timely manner.
5. **Measurement & Reporting:** Ensure metrics of security posture and vulnerabilities are provided to executive members regularly.
6. **Roles & Responsibilities:** Ensure procedures for detection, notification, and reporting of security incidents are clearly defined and understood.

With a suite of solutions powered by objective data—which pioneered the security ratings industry in 2011—Bitsight arms organisations to identify risk in their digital ecosystems and supply chains, so they can focus on remediation and continuous improvements.

Bitsight capabilities that enable compliance include:

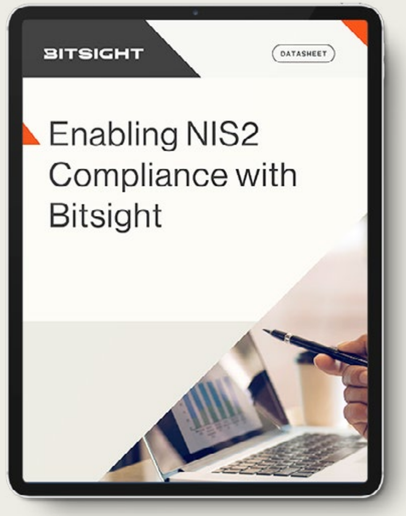
- Mapping risk vector data to control frameworks and questionnaire-based assessments so you can 'trust but verify' risk assessments.
- Data-driven insights on how to meet internal standard and regulatory requirements.
- Continuous monitoring of your attack surface and third-party security controls to track performance over time and remediate gaps.
- Sound governance over your organisation's expanding digital footprint, including third- and fourth-party risk.
- Streamlined and scalable vendor management to improve collaboration and information sharing across the supply chain.

To learn more about these capabilities,
get a personalized consultation with a Bitsight expert.

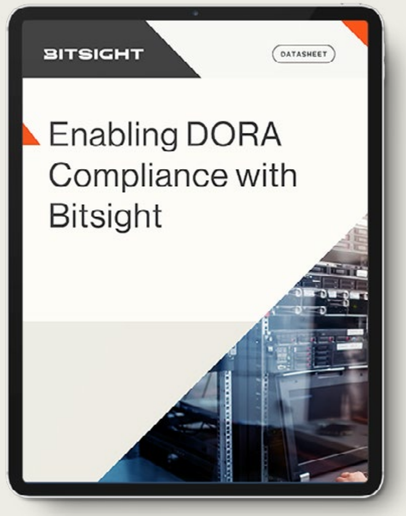
©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

Additional Resources

Watch on demand →



Download your copy →



Download your copy →

©2024, BitSight Technologies, Inc. and its affiliates ("Bitsight"). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

©2024, BitSight Technologies, Inc. and its affiliates (“Bitsight”). BITSIGHT® is a registered trademark of Bitsight. All rights reserved.

BITSIGHT