SecurityHQ

Compliance Requirements Report

Dissecting NIS 2, NIST, DORA, and other Security Standards

Contents

NIST, NIS, and DORA In a Sentence

National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF) – This is a risk-based framework to help businesses manage and protect their critical infrastructure and empower companies to take proactive steps to mitigate cyber risks.

Network & Information Security Directives (NIS 2) EU Directive - A framework created to support and protect critical infrastructure specifically within the European Union (EU).

Digital Operation Resilience Act (DORA) - The European Union's (EU) act sets a standard for managing operational risks, such as cyber threats, system failures, and other operational disruptions posed by digital information and communication technologies.

What is the NIS 2 Directive?

The Network and Information Security Directive (NIS 2) is a legal framework designed to improve cyber security and critical infrastructure throughout the European Union (EU). Based on the NIS Directive, NIS 2 has expanded its scope of security requirements from businesses, as well as business capabilities regarding crisis management and reporting. A further objective of NIS 2 is to ensure a more uniform application of the directive into national laws across EU member states.

Deadline for NIS 2 Compliance

> "By 17 October 2027 and every 36 months thereafter, the Commission shall review the functioning of this Directive, and report to the European Parliament and to the Council."
>
> - NIS Directive 2

What is DORA?

In addition to NIS 2, financial entities in the European Union and their IT providers must comply with DORA by January 17, 2025.

> "As a part of the legislative framework of the European Union, the Digital Operational Resilience Act (DORA) aims to set a common standard for managing operational risks, such as cyber threats, system failures, and other operational disruptions posed by digital information and communication technologies. With an aim to foster the potential of digital finance, the act ensures that financial entities, including banks, crypto asset providers, data reporting providers, and cloud service providers have robust and effective risk management practices to manage, mitigate, and prevent these risks."

- The Digital Operational Resilience Act (DORA); Challenges and Solutions

What Does NIS 2 Mean for Business?

According to the European Commission, the Directive on measures for a high common level of cybersecurity across the Union (the NIS 2 Directive) provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

Member States preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority, cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic collaboration and the exchange of information among Member States. A culture of security across sectors vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare, and digital infrastructure.

What Entities are Affected?

NIS 2 expands the range of industry categories subject to the directive, categorizing them into 'essential' and 'important' groups. Essential entities are subject to proactive compliance monitoring by regulatory authorities, while important entities may undergo compliance checks in response to incident reports or other significant events.

EU member states can modify the list of essential entities, so organizations operating in multiple countries must confirm their classification in each country. However, one of NIS 2's key aims is to standardize classifications across EU member states, so entities should generally fall into the same category regardless of location.

Below are the baseline essential entities as defined by the EU.

Essential Entities

The sectors designated as essential under the NIS 2 directive are deemed foundational to the functioning of society. The size threshold for a critical entity under NIS 2 varies by sector, with typical minimums of 250 employees, an annual turnover of 50 million Euros, or a balance sheet total of 43 million Euros. It's important to note that essential organizations that don't meet these size criteria are still considered important entities.

They include:

- Banking
- Digital Infrastructure – Including internet exchange points, DNS services, TLD name registries, cloud computing, data centers, content delivery networks, trust services, public communications networks, and electronic communications services.
- Drinking Water
- Energy - All primary energy sources, such as electricity production and distribution, district heating and cooling, oil production, refining, storage, and stockholding, as well as natural gas production, supply, and distribution, and hydrogen production, storage, and transmission.
- Financial Infrastructure
- Health
- IT Service Management - Includes business-to-business managed service providers and managed security service providers.
- Transport
- Public Administration (newly added)
- Space (newly added)
- Wastewater (newly added)

Important Entities

NIS 2 significantly broadens the list of important entities compared to NIS 1, covering a diverse array of key manufacturing and service sectors. The size thresholds for important entities under NIS 2 also vary by sector, with typical minimums being 50 employees, an annual turnover or balance sheet total of 10 million Euros.

The important sectors include:

- Digital Service Providers
- Research Organizations
- Chemical Manufacturing & Distribution (newly added)
- Durable Goods Manufacturing (newly added) - A broad category that includes medical device manufacturing, computers, electronics, optics, electrical equipment, machinery, vehicles, trailers, and other transport equipment.
- Food Manufacturing & Distribution (newly added)
- Pharmaceutical Manufacturing (newly added)
- Postal & Courier Services (newly added)
- Waste Management (newly added)

Read more from the European Commission, **here.**

Benefits of Being NIS 2 Compliant

1. Enhanced Risk Management and Reduction

The SHQ Response Platform, which integrates the NIST and **MITRE** framework, calculates the impact of security threats, and the likelihood of risks happening, all from a single location.

- Conduct risk assessments and implement security policies
- Manage incidents
- Secure the supply chain
- Ensure network security
- Control access
- Utilize cryptography and, where applicable, encryption
- Implement multi-factor authentication
- Protect data
- Oversee system procurement and operational security (including vulnerability management and reporting)
- Conduct testing and auditing
- Provide cybersecurity training and promote basic computer hygiene

2. Enhanced Risk Mitigation

SecurityHQ's Risk Management makes the creation of risks easy with a simple 3-click process, and a library of threat profiles available to readily use.

- Document, track, and mitigate your risks. Within the risk itself, use individual mitigation trackers.
- Easily create risks, identify suspected risks, and assign risks to specific actions.
- Gain access to a library of threat profiles, with relevant and generic mitigations and threat mapping.
- Create, manage, track, and mitigate risks

3. Incident Response and Recovery Capabilities

SHQ Response is a unified security management platform to orchestrate and enable collaboration, prioritize incidents, visualize risks, and empower integration.

- Reporting security incidents that have significant impacts within specified deadlines
- Perform forensic analysis

4. Business Continuity and Easy Collaboration with 3rd Parties and Supply Chains

Understanding your supply chain is critical to securing it effectively. Start by creating a list of all suppliers and partners and identify which ones are the highest priority in terms of risk. Look for information published by your suppliers to understand how they provide services securely, and make sure you understand each party's security responsibilities under your contract or licensing agreement.

- Crisis response
- Crisis management
- Implement emergency procedures
- Plan for business continuity

Preparing for NIS 2 Compliance in Six Steps

Organizations identified as essential or important under NIS 2 should begin their preparation immediately, as implementing the required internal measures will take time. The following guideline outlines how to assess and achieve readiness for specific NIS 2 requirements.

Step One: Gap Analysis

The requirement to conduct a risk assessment and review security policies necessitates a structured evaluation of the organization's current security stance and defense capabilities compared to industry best practices.

A gap analysis should be the first step in the organization's NIS 2 compliance journey, producing a dashboard that displays the organization's current level of cyber resilience, including both strengths and gaps that need to be addressed.

Step Two: Detailed Recommendations Are Essential

An executive overview should be complemented by detailed initiatives to enhance resilience, providing clear instructions for security implementation teams. Each enhancement initiative should include a detailed description of the recommendation and its implementation process.

Step Three: Supply Chain Security and Ongoing Monitoring.

With the increasing digital integration of supply chain partners, supply chain cybersecurity has become a critical aspect of cyber resilience for many organizations. The EU has recognized this, making supply chain security a key mandate in NIS 2.

Organizations with digital connections to supply chain partners must expand their security posture analysis to include those partners, regardless of their location within or outside the EU. This analysis should produce a security roadmap with actionable, measurable recommendations that can drive structured and accelerated improvements in supplier security and reduce supply chain risk.

The cyber posture and risk analysis applied to the digital supply chain should cover data storage and processing services, software, and managed security services. The security posture and practices of supply chain partners should be evaluated against industry best practices.

A common challenge is the lack of proactive monitoring of critical suppliers, which can undermine NIS 2 compliance. It's essential to follow up a supplier posture analysis and risk reduction program with ongoing monitoring to ensure sustained improvements.

Step Four: Incident Management and Reporting

Incident management is a core security requirement for NIS 2 compliance. This includes any actions and procedures aimed at preventing, detecting, analyzing, containing, responding to, and recovering from incidents.

In practice, when an incident occurs, an organization must simultaneously work on multiple fronts to rapidly contain the incident, minimize damage, and collect the necessary data to meet reporting requirements. In addition to technical and operational tasks, executive-level crisis management is essential during major incidents.

NIS 2 places a strong emphasis on incident reporting, with stricter requirements than NIS 1.

> An organization experiencing a significant cyber-attack must notify its national cybersecurity agency within 24 hours and submit a detailed incident report within 72 hours. This report should assess the impact on operations, customers, and supply chain partners, and ideally include indicators of compromise. A final, detailed report on the incident and response must be submitted within 30 days.

Reporting is also required at the national level. Each EU country's Computer Security Incident Response Team (CSIRT) must submit a quarterly summary report to the European Union Agency for Cybersecurity (ENISA) on cyber incidents from the previous three months, using anonymized data. ENISA must also report to the EU biannually. The goal of these reporting requirements is to enable organizations and member states to learn from each other and benefit from a collective cybersecurity approach.

Step Five: Leadership Accountability

Organizations must prepare a crisis management and business continuity plan. Under NIS 2, executive leaders will be held accountable for significant external impacts resulting from breaches. Crisis management and business continuity planning outlines how executive and operational teams should respond during a crisis.

To prepare for an NIS 2 audit, organizations should review their cyber playbooks and allocate time to update or develop them before the NIS 2 compliance deadline. Tabletop exercises, or "wargames," are an effective way to test crisis preparedness and should be conducted early in the NIS 2 preparation timeline.

Step Six: Adversarial Simulations

NIS 2 acknowledges that cyber defenses and crisis preparedness need to be tested. Adversarial simulations (red teaming) should be used to test an organization's cyber defenses, mimicking real threat actor tactics, techniques, and procedures. These simulations can identify security system gaps, misconfigurations, and vulnerabilities that can then be addressed with appropriate mitigations.

How SecurityHQ Can Support Your NIS 2 Compliance Journey

> By working with SecurityHQ, you can enhance your cybersecurity maturity and confidently prepare for NIS 2 compliance, safeguarding your organization in an increasingly complex regulatory landscape."
>
> - Assad Bahar, Regional Solution Lead, SecurityHQ

SecurityHQ understands that NIS 2 brings new, more stringent requirements that vary by sector. To help our clients get ready for these regulations, we offer the following services:

Sector-Specific Workshops

'We organize workshops tailored to your specific industry, designed to identify the exact NIS 2 requirements and any gaps in your current cybersecurity setup. These workshops focus on the unique regulatory challenges that your sector faces.'
– Assad Bahar

Tailored Analysis

'Following the workshops, we conduct an in-depth analysis to determine how your existing practices measure up against NIS 2 requirements, identifying where improvements are needed. This analysis is specific to your sector, ensuring your organization is fully compliant.'
– Assad Bahar

Actionable Implementation Plans

'Based on our findings, we provide a detailed action plan with clear steps to address any gaps. This plan is customized to align with your business goals while ensuring that you meet NIS 2 compliance standards.'
– Assad Bahar

Continuous Support and Adaptation

'We don't just help you plan; we offer ongoing support to ensure your organization can adapt to evolving regulations and cybersecurity threats, making sure your compliance strategy remains effective over time.'
– Assad Bahar

Boosting Cybersecurity Maturity and Achieving NIS 2 Compliance with Our Risk Centre

"At SecurityHQ, we know how important it is for our clients to continually improve their cybersecurity practices. That's why we've created our Risk Centre, a platform designed to provide a maturity evaluation into vital areas like Governance and Risk Management, Incident Response and Reporting, Access Control, and Monitoring and Detection.

By leveraging the NCSC Cyber Assessment Framework (CAF), we can help you understand your current cybersecurity maturity and set targets for ongoing enhancement. Our assessments utilizing the NCSC framework are closely aligned with well-established international standards such as ISO 27001 and NIST CSF. This ensures that your organization's cybersecurity measures are not only comprehensive but also meet global best practices. This approach also lays a strong foundation for NIS 2 compliance, as there are considerable similarities between these frameworks."

- Assad Bahar, Regional Solution Lead, SecurityHQ

How We Can Support You Technically

Gap Analysis

Evaluate your existing cybersecurity policies, procedures, and technical controls against the NIS 2 requirements.

Risk Assessment

Identify the vulnerabilities, threats, and potential impact on your critical assets.

Compliance Report

Receive a detailed outlined report outlining areas of compliance and non-compliance, and associated risks.

Prioritized Recommendations

Receive the recommended actions to take to address any identified gaps.

Management Presentation

Offer a briefing to senior management, summarizing the assessment findings, risks, and recommended actions.

2-hour Workshop

To review the incident response plan or, if one is not in place already, a session to provide a structured incident response plan document for the client to adopt.

Regulatory Obligations Overview

A walkthrough of the legal implication of NIS 2 non-compliance to emphasize the importance of acting.

What is NIST?

The National Institute of Standards and Technology (NIST) is a U.S. federal agency that operates under the Department of Commerce. Established in 1901, NIST's mission is to promote American innovation and industrial competitiveness by advancing measurement science, standards, and technology.

> "NIST plays a crucial role in various fields, including cybersecurity, manufacturing, and healthcare, by developing and maintaining standards that ensure the quality and reliability of products and services. NIST's Cybersecurity Framework helps organizations manage and reduce cybersecurity risks and publishes cybersecurity guides aligned with specific controls to help organizations achieve their cyber goals."

- Alan Cizenski, Pre Sales Engineer, SecurityHQ

'NIST SP 800-30, titled **"Guide for Conducting Risk Assessments,"** lays the groundwork for conducting risk assessments by offering a catalog of security and privacy controls to organizations to allow them to implement those practices to fortify their defenses. The document is a comprehensive outline for conducting risk management that entails defining vulnerabilities, interpreting the level of risk in the infrastructure, monitoring the potential threats, and implementing remediation strategies.' - Read more, **here.**

'NIST 800-53, provides a comprehensive record of security and privacy controls, curated by the Information Technology Laboratory (ITL), for federal information systems in the United States. Titled "**Security and Privacy Controls for Information Systems and Organizations,"** the publication assists federal agencies and organizations in effectively securing their information systems and protecting sensitive information from various security threats and vulnerabilities. With an aim to maintain secure information systems, NIST 800-53 also outlines the importance of continuous monitoring and regular updates to the security controls to confront the evolving threat landscape.' – Read more, **here.**

NIST Benefits to Business

> A risk-based, structured approach to enhance businesses' cybersecurity posture through identifying, managing, and mitigating cyber risks. By adopting the NIST guidance, businesses can improve their resilience against cyber threats and streamline compliance, ensuring the protection of critical assets and maintaining customer trust."

- Alan Cizenski, Pre Sales Engineer, **SecurityHQ**

The five functions of the NIST Framework include:

1. **Identify** – To achieve an understanding and identification of all assets.
2. **Protect** – To outline the right measures to safeguard to make sure that the delivery of key infrastructure/ services is achieved.
3. **Detect** – To implement the right mechanisms to identify occurrences of cyber security incidents.
4. **Respond** – To conduct the right approach/activities about an identified cyber security incident.
5. **Recover** – To identify the right activities to maintain resilience and restore impacted capabilities/services.

How SecurityHQ Aligns with the NIST Framework

SHQ Response Platform acts as the Emergency Room, and the Risk Centre provides the Wellness Hub for all cyber security monitoring and actions. This has included a complete rewrite of how risks are visualized and how customers work with their security team.

The Risk Centre is designed to prevent emergencies before they arise. To make this possible, SecurityHQ has combined its intellectual property and knowledge on risk mitigation and cybersecurity, and merged with several recognized sources in the industry, including the National Institute of Standards and Technology (**NIST**), the National Cyber Security Centre (NCSC), and **MITRE** Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK), to provide actions on how to identify, map, and raise risks.

> ‘SHQ Response Platform is unique in the industry as it follows a combination of different sources and is always viewed within the context of the customer. The Risk Centre itself is what makes this such a unique offering, as the user is now able to calculate the impact of security threats to the business, the likelihood of risks happening, identify all the different tactics and techniques, and highlight how best to mitigate these risks, all from a single location”
>
> - Chris Cheyne, SOC Director and CTO, SecurityHQ

SecurityHQ, NIST, MITRE, & NCSC Intelligence Combined

With **SHQ Response Platform,** users are now able to:

- Map Threats, Assets, and Vulnerabilities to Derive Risks.
- Manage Risks in Accordance with NIST 800-30.
- Identify Maturity and Impact Mitigations, Linked to NIST 800-53.
- Track Mitigations, Task Assignments, and Progress.
- Link Compliance Incidents to Risk, to Reduce Repetitive Incidents Creating Noise.
- Receive Monthly Tailored Executive Reports, Delivered by Data Analytics Team, to Prioritise Actions.
- View the Incident Graphic Card, which Showcases Real-time Incident Information, Including the Time-line Perspective Tab, Graphical Representation Tab, and MITRE Tactics Tab.
- Investigate & Prioritise Incidents. Categorize incidents against MITRE ATT&CK, and Assign Risk Levels, Based on CIA Attributes, Asset Criticality, and Possible Impact.

> We have not seen any platforms out there that are doing this. We see a lot of risk management platforms, but they don't deal with the details of cyber security risks in a very good way. The SHQ Response Platform has simplified cyber security, by enabling customers to be part of their security journey. It was built so that businesses could learn more about potential threats, and solve cyber-related issues, together with their designated security experts."

- Feras Tappuni, CEO, SecurityHQ

And this is just the beginning. SHQ Response Platform is continuously evolving its **Incident Response capabilities,** to meet market demands and enhance customer experience. For more information on the developments of the SHQ Response Platform, talk with a security expert, **here.**

Next Steps

While the NIS 2, DORA, NIST, and other cybersecurity frameworks are curated to streamline cybersecurity strategies, it can be challenging for organizations to achieve compliance and fortify their defenses alone.

At SecurityHQ, we are committed to empowering businesses to build a secure future by simplifying cybersecurity. This is why we offer a wide range of comprehensive solutions tailored to the unique needs of each organization.

To embark on the journey of a resilient digital future, **contact us today.**

Additional Compliance Requirements – Global Requirements

Payment Card Security Data Security Standard (PCI-DSS)

Industries Impacted: **Finance, Merchants, Payment Card Issuing Banks, Processors, Developers, Vendors**

Applicable Locations: **Global**

Objective: The PCI DSS is a set of security standards created to minimize card fraud by tightening security controls and the use of data and is monitored by the PCI SSC (Payment Card Industry Security Standards Council).

'All merchants and service providers that process, transmit, or store cardholder data must comply with the PCI DSS. Merchants accept debit or credit card payments for goods or services. Note that the PCI DSS applies to merchants even if they have subcontracted their payment card processing to a third party. Service providers are directly involved in processing, storing or transmitting cardholder data on behalf of another entity.' **– IT Governance**

Environmental, Social, and Governance (ESG)

Industries Impacted: **All. This is an assessment of how a Business Treats and Protects its Employees, Suppliers, Customers, and the Public.**

Applicable Locations: **Global**

Objective: The environmental elements look at the impact of a business on the natural world. The social element assesses how the people involved in the business are treated. The governance elements analyze how the business policies itself.

'ESG stands for environmental, social, and governance, and is a holistic framework that measures the sustainable and ethical behavior of a business. The criteria ensure that a business is being socially responsible and held accountable, which is in the best interest of shareholders and potential investors.' **– Climate Partner**

Payment Card Security Data Security Standard (PCI-DSS)

Industries Impacted: **Finance, Merchants, Payment Card Issuing Banks, Processors, Developers, Vendors**

Applicable Locations: **Global**

Objective: The PCI DSS is a set of security standards created to minimize card fraud by tightening security controls and the use of data and is monitored by the PCI SSC (Payment Card Industry Security Standards Council).

'All merchants and service providers that process, transmit, or store cardholder data must comply with the PCI DSS. Merchants accept debit or credit card payments for goods or services. Note that the PCI DSS applies to merchants even if they have subcontracted their payment card processing to a third party. Service providers are directly involved in processing, storing or transmitting cardholder data on behalf of another entity.' **– IT Governance**

Soley Payments of Principles and Interest (SPPI Rules)

Industries Impacted: **Finance**

Applicable Locations: **All: The SPPI Rules are part of the International Financial Reporting Standard. IFRS Standards are required or permitted in 132 jurisdictions across the world.**

Objective: 'The SPPI test requires that the contractual terms of the financial asset (as a whole) give rise to cash flows that are solely payments of principal and interest on the principal amounts outstanding i.e. cash flows that are consistent with a basic lending arrangement. Unlike the business model test, this assessment must be carried out on an instrument-by-instrument basis.' **- BDO UK**

Payment Card Industry Security Standards Council (PCI SSC)

Industries Impacted: **Finance, Merchants, Payment Card Issuing Banks, Processors, Developers, Vendors**

Applicable Locations: **Global: Headquartered in the US**

Objective: 'The PCI Security Standards Council (PCI SSC) is a global forum for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection.' **- PCI SSC**

'The Council is responsible for the development, management, education, and awareness of the actual Payment Card Industry Standards (PCI), including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.' **- PCI Policy Portal**

ISO/IEC 27001

Industries Impacted: **All. This is a set of Standards used to Ensure Companies have Adequate Data Protection Services**

Applicable Locations: **Global: Relies on companies meeting the ISO standard**

Objective: 'The ISO/IEC 27001 standard provides companies of any size, and from all sectors of activity, with guidance on establishing, implementing, maintaining, and continually improving an information security management system. Conformity with ISO/IEC 27001 means that an organization has put in place a system to manage risks related to the security of data owned or handled by the company.' **- ISO**

Additional Compliance Requirements – US Specific

Gramm-Leach-Bliley Act (GLBA)

Industries Impacted: **Finance, Insurance**

Applicable Locations: **US**

Also known as the Financial Services Modernization Act of 1999, 'the Gramm-Leach-Bliley Act required the Federal Trade Commission (FTC) and other government agencies that regulate financial institutions to implement regulations to carry out the Act's financial privacy provisions (GLB Act).' **- Federal Trade Commission**

Sarbanes-Oxley Act (SOX)

Industries Impacted: **Finance**

Applicable Locations: **US**

Objective: The Sarbanes–Oxley Act was established in 2002 and is a United States federal law. SOX was created to mandate practices in financial record keeping and reporting. It contains eleven requirements that all US-based accounting firms must comply with.
Read the full Act, **here.**

Health Insurance Portability and Accountability Act (HIPAA)

Industries Impacted: **Finance, Healthcare, Claims Processing**

Applicable Locations: **US as well as companies that have access to the health information of United States residents.**

Objective: Although related to healthcare, rather than finance, HIPAA is a requirement for the handling of healthcare data of employees within financial organizations.

'The HIPAA Privacy Rule regulates the use and disclosure of protected health information (PHI) by "covered entities." These entities include healthcare clearinghouses, health insurers, employer-sponsored health plans, and medical providers.' **- National Library of Medicine**

California Consumer Privacy Act (CPA)

Industries Impacted: **Technology, Media and Entertainment, and Telecommunications (TMT) Industries.**

Applicable Locations: **California: The CCPA applies to the data of California residents only, though any company collecting data on California residents are subject to CCPA regardless of location**

Objective: 'The California Consumer Privacy Act (CPA) gives customers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law.'
- State of California Department of Justice

Health Insurance Portability and Accountability Act (HIPAA)

Industries Impacted: **Finance, Healthcare, Claims Processing**

Applicable Locations: **US as well as companies that have access to the health information of United States residents.**

Objective: Although related to healthcare, rather than finance, HIPAA is a requirement for the handling of healthcare data of employees within financial organizations.

'The HIPAA Privacy Rule regulates the use and disclosure of protected health information (PHI) by "covered entities." These entities include healthcare clearinghouses, health insurers, employer-sponsored health plans, and medical providers.' **- National Library of Medicine**

Personal Information Protection and Electronic Documents Act (PIPEDA)

Industries Impacted: **Banks, Airlines, Telecommunications Companies, Media and Entertainment**

Applicable Locations: **Canada: All privately owned businesses in Canada, employees of federally regulated businesses, and oversees organizations using Canadians' data.**

Objective: PIPEDA aims to strike a balance between an individual's right to the privacy of personal information and the need of organizations to collect, use, or disclose personal information for legitimate business purposes. 'The Personal Information Protection and Electronic Documents Act (PIPEDA) sets the ground rules for how private-sector organizations collect, use, and disclose personal information in the course of for-profit, commercial activities across Canada.' **- Office of the Privacy Commission of Canada**

American Bar Association Model Rules (ABA Model Rules)

Industries Impacted: **Legal Services**

Applicable Locations: **US: The ABA Model Rules have only come into effect when states choose to adopt them – attached is a list of willing states**

Objective: 'The ABA Model Rules of Professional Conduct were adopted by the ABA House of Delegates in 1983. They serve as models for the ethical rules of most jurisdictions.' The Model Rules of Professional Conduct are not inherently binding but have come into effect only when states choose to adopt certain rules.' **- ABA (American Bar Association)**

New York State Department of Financial Services (NYDFS)

Industries Impacted: **Finance, Insurance, Healthcare**

Applicable Locations: **New York**

Objective: The New York State Department of Financial Services (NYDFS) is responsible for regulating financial services and products in New York. It oversees areas such as insurance, banking, and financial services laws. NYDFS aims to build an equitable, transparent, and resilient financial system that benefits individuals and supports businesses. Read more **- Department of Financial Services**

Health Information Technology for Economic and Clinical Health Act (HITECH)

Industries Impacted: **Finance, Healthcare, Claims Processing**

Applicable Locations: **US: Companies that have access to the health information of United States residents, as well as Business Associates of Covered Entities**

Objective: The HITECH Act is part of the American Recovery and Reinvestment Act of 2009 that incentivized the meaningful use of Electronic Health Records (EHRs) and strengthened the privacy and security provisions of HIPAA. Among other measures, the HITECH Act extended the reach of the HIPAA Security Rule to Business Associates of Covered Entities, who also had to comply with certain Privacy Rule standards and the new Breach Notification Rule. The Act also introduced tougher penalties for HIPAA compliance failures. Read more **- HIPPA Journal**

Additional Compliance Requirements Regulations- India Specific

IT Act 2000

Industries Impacted: **Finance, Technology, Media and Entertainment**

Applicable Locations: **India, as well as Indian citizens committing acts outside the country or foreign citizens within India**

Objective: 'The IT Act aims to provide a legal framework for electronic governance in matters related to cybercrime and e-commerce by giving recognition to electronic records and digital signatures. 'An Act to provide legal recognition for transactions carried out using electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce' **- find the full act here**

The Digital Personal Data Protection Bill (PDPB) IT Act 2022

Industries Impacted: **Finance, Technology, Media and Entertainment**

Applicable Locations: **India, as well as any data processed outside of India, provided such processing is in connection with any profiling of, or activity of offering goods or services to data principals within India.**

Objective: 'The new Digital Personal Data Protection Bill, 2022 released on Friday (November 18) is focused on personal data, as compared to an earlier unwieldy draft.' **- The Indian Express**

'The purpose of this Act is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their data and the need to process personal data for lawful purposes and matters connected therewith or incidental thereto.' **- Read the full act here: Ministry of Electronics & Information Technology**

Sensitive Personal Data or Information (SPDI Rules)

Industries Impacted: **Finance, Technology, Media and Entertainment**

Applicable Locations: **India, as well as Indian citizens committing acts outside the country**

Objective: 'In India, SPDI is expressly defined and dealt with under the SPDI Rules. Such rules require entities that hold user-related SPDI to maintain certain security standards. These rules also prescribe the specific protocols necessary for storing personal information electronically, including in respect of SPDI.' **- S&R Associates**

Find definitions and regulations under the 2011 Act **here**

Bar Council of India (BCI)

Industries Impacted: **Legal Services, Educational Institutions Teaching Law**

Applicable Locations: **India**

Objective: 'The Bar Council of India is a statutory body created by Parliament to regulate and represent the Indian Bar. We perform the regulatory function by prescribing standards of professional conduct and etiquette and by exercising disciplinary jurisdiction over the bar.' **- BCI**

Digital Information Security Health Care Act (DISHA)

Industries Impacted: **Healthcare, Insurance, and any Companies Dealing with Digital Health Data**

Applicable Locations: **The Data Protection Rules apply to any corporate entity that in some way deals with the SPDI of a person.**

Objective: 'The DISHA (Digital Information Security in Healthcare Act) will serve as the framework for the development of digital health records in India and will enable the digital sharing of individual health records with and between hospitals and clinics.' **- estartIndia**

Additional Compliance Requirements – UAE Specific

The Personal Data Protection Law (PDPL) of the United Arab Emirates

Industries Impacted: **Technology, Media and Entertainment, Telecommunications, or any Company that Processes Data**

Applicable Locations: **UAE, as well as any company that processes personal data of people residing within the UAE**

Objective: 'The Personal Data Protection Law constitutes an integrated framework to ensure the confidentiality of information and protect the privacy of individuals in the UAE. It provides proper governance for data management and protection and defines the rights and duties of all parties concerned.' **- UAE Government**

Dubai International Finance Center (DIFC) Data Protection

Industries Impacted: **Finance**

Applicable Locations: **'This Law applies to the Processing of Personal Data by a Controller or Processor incorporated in the DIFC, regardless of whether the Processing takes place in the DIFC or not.'**

Objective: 'The law prescribes rules and obligations regarding the collection, handling, and use of personal data as well as rights and remedies for individuals who may be impacted by such processing. It is designed to balance the legitimate needs of businesses and organizations to process personal information while upholding an individual's right to privacy.' **- DIFC**

Read the full law **here**

Abu Dhabi Global Market (ADGM) Data Protection

Industries Impacted: **Finance**

Applicable Locations: **Any Processing of Personal Data in the context of the activities within ADGM, regardless of whether the Processing takes place in ADGM or not.**

Objective: 'Regulations to make provision for the protection of personal data processed or controlled from within the Abu Dhabi Global Market.' **- ADGM Data Protection Regulations**

Health Data Law UAE

Industries Impacted: **Healthcare, Insurance, Finance**

Applicable Locations: **UAE: All entities operating in the UAE and the Free Zones that provide healthcare, or handle health data**

Objective: 'The Health Data Law in the UAE regulates the processing of electronic health data originating in the country. It imposes obligations on healthcare providers, medical insurance providers, and other entities related to the collection, processing, and transfer of health data. The law formalizes the requirement that health data must be processed and stored within the UAE, with limited exceptions for data transfer.' **- PricewaterhouseCoopers**

UAE IE Regulation

Industries Impacted: **Healthcare, Insurance, Finance**

Applicable Locations: **UAE**

Objective: 'The purpose of the UAE IA Regulation is to provide requirements to raise the minimum level of protection of information assets and supporting systems across all implementing entities in the UAE' **- UAE**

Additional Compliance Requirements – UK and Europe Specific

General Data Protection Regulation (GDPR)

Industries Impacted: **Finance, eCommerce, Social Media Platforms, Tech, Medical, Healthcare**

Applicable Locations: **EU**

Objective: 'The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.' **– GDPR.EU**

Digital Security Sandbox (DSS)

Industries Impacted: **Financial**

Applicable Locations: **UK: Only UK-Established Entities may Participate in the DSS as a Sandbox Entrant**

Objective: 'The DSS is a regime that will allow firms to use developing technology, such as distributed ledger technology (DLT), in the issuance, trading, and settlement of securities such as shares and bonds. In doing so, the Bank and FCA will pursue three overarching aims: Facilitating innovation to promote a safe, sustainable, and efficient financial system; protecting financial stability and finally, protecting market integrity and cleanliness.'
- Bank of England

Financial market participants should be able to interact with firms inside DSS as normal whilst benefiting from the new technology.

ePrivacy Directive

Industries Impacted: **Electronic Communications Sector**

Applicable Locations: **EU: No longer applies to the UK**

Objective: 'The ePrivacy Directive specifies that people have to opt in before a company can send communications to them. This applies to not just email marketing, but also calls, texts, and any other form of electronic communication. Unsolicited emails or calls are not allowed.' **- Cloudflare**

'The ePrivacy Directive came into force in May 2011. The directive concerns the processing of personal data and the protection of privacy in the electronic communications sector.'

Find the full act **here.**

Data Protection Act 2018

Industries Impacted: **Social media, eCommerce, Finance, Technology, Healthcare**

Applicable Locations: **UK: Primarily applies to UK-based companies with some exceptions**

Objective: 'The Data Protection Act 2018 controls how your personal information is used by organizations, businesses, or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Under the Data Protection Act 2018, citizens have the right to find out what information the government and other organizations store about you.' **- UK government**

Solicitors Regulation Authority (SRA)

Industries Impacted: **Legal Services**

Applicable Locations: **England and Wales**

Objective: 'It is responsible for regulating the professional conduct of solicitors and other authorized individuals, as well as those working in-house at private and public sector organizations.' **- SRA**

Additional Compliance Requirements – UK and UAE Specific

Cyber Essentials

Industries Impacted: **Social media, eCommerce, Finance, Technology, Healthcare**

Applicable Locations: **UK companies**

Objective: 'Cyber Essentials is a government-backed, industry-supported scheme to help organizations protect themselves against common online threats. Cyber Essentials is a set of basic technical controls organizations should have in place to protect themselves against common online security threats.' **- UK Government**

The Caldicott Principles

Industries Impacted: **Health and Social Care**

Applicable Locations: **England**

Objective: 'Eight principles to ensure people's information is kept confidential and used appropriately. The principles are intended to apply to all data collected for the provision of health and social care services where patients and service users can be identified and would expect that it will be kept private.' **- UK Government**

Health and Social Care Act 2012

Industries Impacted: **Healthcare**

Applicable Locations: **UK**

Objective: 'The main aims of the Act are to change how NHS care is commissioned through the greater involvement of clinicians and a new NHS Commissioning Board; to improve accountability and patient voice; to give NHS providers new freedoms to improve quality of care; and to establish a provider regulator to promote economic, efficient and effective provision. It also addresses public health, regulation of health and social care services, public involvement, and cooperation between local authorities and commissioners of health care services.' **- UK Government**

Protection Today,
Preparation for
Tomorrow

About SecurityHQ

Report a Cyber Security Incident

If you are experiencing a current security breach or possible incident and require immediate assistance, please complete the form and a member of our Security Operations Team will aim to be in contact within 15 minutes.

Are You Experiencing An Incident?

Having conducted incident response investigations across a wide range of industries, SecurityHQ are best placed to work with businesses large and small, and across numerous technical environments to reduce the impact of a cyber security incident.

If you suspect a security incident, you can also report an incident by phone by contacting us 24/7 for immediate support at +442033270698 or email forensics@securityhq.com

SecurityHQ

Join us on Socials:

SHQ Underground Podcast:

Get in Touch

sales@securityhq.com
www.securityhq.com

Americas:	+1 312 544 0538
APAC:	+91 842 119 8100
Europe:	+44 20 332 70699
Middle East:	+971 4354 9535
Africa:	+27 11 702 8555