Cyber compliance, regulations, and standards fact sheet

A quick guide to the key frameworks that organisations should be aware of

Get ready for new EU regulations

One of the biggest challenges for North American companies operating out of Ireland is adjusting to a very different regulatory environment to what they've known in the States. And it's about to become much more complicated. The EU Commission is on a mission to harmonise regulations across member States, to better protect citizen's personal data and to put guardrails around businesses to ensure operational resilience in the face of increasing cybersecurity threats.

The last few years have seen some of the biggest US tech companies pay heavy fines for breaching Europe's General Data Protection Regulation (**GDPR**), which should serve as a timely reminder for multinational with a footprint in Ireland to stay compliant with what's coming down the track.

The scope of new regulations like **NIS2** (an update on the Network and Information Security directive) is intented to strengthen cybersecurity requirements for medium and large businesses that operate and provide services in key sectors. It puts pressure on them to meet higher technical standards around IT systems and networks, demonstrating resilience and business continuity capabilities.

Right now, BT Ireland is working with customers to make sure they are ready for the NIS2 deadline of October 18, 2024. And we're already engaging with financial service clients about preparation for the **Digital Operational Resilience Act (DORA)**, which will pass into law on January 17, 2025.

Please feel free to reach out and join the conversation about these regulations and others listed in this factsheet. There are many areas where BT can help, not just in achieving regulatory readiness by the deadlines, but also for ensuring you have the processes in place to stay compliant in the future.

Dónal Munnelly,
CyberSecurity Proposition Manager, BT Ireland

4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years[1]

277 days

time taken to identify and contact a data breach[1]

$250,000

20% of organisations that experienced a data breach paid this much or more in fines [1]

Source 1: IBM Cost of Cybercrime report 2023

Stay secure and compliant with future-proof strategies

If your organisation is struggling to keep up with ever-changing cyber security measures, you're not alone. A recent BT survey found 61% of respondents were facing similar challenges. The good news is, we can help.

Compliance frameworks and why they matter

Compliance frameworks are most businesses' best friend. Offering sets of guidelines and best practices, they're developed in conjunction with hundreds of organisations with input from thousands of subject matter experts, to help you understand what 'good' looks like and where to focus your efforts.

Increasing your organisation's resilience should be more than simply a box-ticking exercise. Compliance helps you meet regulatory requirements, protects your finances, improves processes, and strengthens your security. It also builds industry and customer confidence.

You should see compliance as an opportunity to develop a future-proof strategy – highlighting weaknesses and prioritising resources. It's important to remember that achieving compliance within a regulatory framework is an ongoing process, as your organisation's needs are always changing and evolving.

We've pulled together some of the key frameworks for UK organisations, to help you find the ones most relevant to you.

What frameworks are relevant to your organisation?

The size of your organisation, the sector you work in and the geographical locations in which you operate, can all influence the frameworks relevant to your business.

The good news

You don't have to go it alone. Our Security Advisory Services can help. Book a security health check tailored to your organisation's industry of specialism. The advisory reports will identify priorities and where to head next.

Find out more about our Security Advisory Services here: **btireland.com/securityadvisoryservices**

Compliance frameworks: a brief guide

Best practices for optimising workflows, reducing risk and strengthening cyber security

Compliance framework	What it is	Who it's for	Find out more	Good to know
NIS Also known as the Network & Information Systems Regulations or 'NIS1'	NIS, the first EU cyber security law, came into force in May 2018 The Regulations intend to address the threats posed to network and information systems and therefore aim to improve the functioning of the digital economy across the EU.	Operators of Essential Services (OES) and Competent Authorities (CAs).	**NIS: Full document**	Do the regulations apply to your organisation? **The NIS Regulations website explains how to identify OES and Cas**
NIS2 The revised and updated version of the Network and Information Security legislation detailed above	NIS2 is an EU directive designed to build upon NIS1. This set of legal measures addresses NIS1's areas of weakness, to widen its remit and have a greater impact overall. NIS2 applies to a larger group of medium and large size organisations, with the aim of strengthening cyber resilience in the EU.	Operators of Essential Services (OES) and Competent Authorities (CAs) deemed 'Essential' or 'Important', as outlined below. **Essential**: Energy, Transport, Banking, Financial markets, Health, Drinking Water, Wastewater, Digital Infrastructure, ICT Service Manage-ment, Public Administration, Space **Important:** Postal and Courier Services, Waste Management, Chemicals, Food, Manufacturing, Digital Providers, Research Organisations.	**NIS2 Directive: Full document**	While under the old NIS directive member states were responsible for determining which entities would meet the criteria to qualify as operators of essential services, the new NIS2 directive introduces a size-cap rule. This means that all medium-sized and large entities operating within the sectors or providing services covered by the directive will fall within its scope. The text also clarifies that the directive will not apply to entities carrying out activities in areas such as defence or national security, public security, law enforcement and the judiciary. Parliaments and central banks are also excluded from the scope. As public administrations are also often targets of cyberattacks, NIS2 will apply to public administration entities at central and regional level. In addition, member states may decide that it applies to such entities at local level too.
EU cyber security certification framework Establishing the European Union Agency for Cybersecurity	The framework sets EU-wide parameters for the rules, technical requirements, standards and procedures surrounding risk-based certification schemes covering different categories of ICT products, processes and services.	Companies providing ICT (information and communications technology) products, services and processes.	**ENISA and ICT cybersecurity certification: Full document**	Organisations will be able to obtain certifications that are valid across the EU, reducing the compliance burden on those that currently maintain multiple certifications to meet requirements across different markets. This harmonised approach to cyber security certification will supersede member states' individual certification schemes such as the Dutch scheme for BSPA Baseline security Product Assessment and France's CSPN certification Sécuritaire de Premier Niveau.

Compliance frameworks: a brief guide (continued)

Best practices for optimising workflows, reducing risk and strengthening cyber security

Compliance framework	What it is	Who it's for	Find out more	Good to know
DORA Digital Operational Resilience Act	It introduces rules on ICT-related incident management, digital operational resilience testing, and managing third-party risk.	DORA applies to a wide range of financial entities regulated by the Central Bank of Ireland.	**Dora: Overview**	
GDPR General Data Protection Regulation (GDPR)	GDPR is the toughest privacy and security law in the world. 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.	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.	**GDPR: An overview** **GDPR: Full Document**	The European Union's General Data Protection Regulation (GDPR) was designed to apply to all types of businesses, from multi-nationals down to micro-enterprises. The fines imposed by the GDPR under Article 83 are flexible and scale with the firm. Any organization that is not GDPR compliant, regardless of its size, faces a significant liability. Infringements could result in a fine of up to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.
Digital Services Act	The Digital Services Act (DSA) is a new set of EU-wide rules for digital services acting as intermediaries for consumers and goods, services, and content. In the context of the DSA, digital services refer to intermediary services such as host providers, online marketplaces, and social media networks.	All online intermediaries and platforms in the EU, for example, online marketplaces, social networks, content sharing platforms, app stores, and online travel and accommodation platforms.	**The Digital Services Act**	Its main goal is too prevent illegal and harmful activities online and the spread of disinformation. It ensures user safety, protects fundamental rights, and creates a fair and open online platform environment.
CIS 18 Also known as 'CIS Controls' or CIS Critical Security Controls. CIS stands for Center for Internet Security. The 18 relates to the number of Critical Security Controls – a series of best practices for organisations to follow.	The Center for Internet Security (CIS) is a community driven non-profit organisation. Its CIS Controls (also known as 'CIS 18') and CIS Benchmarks are globally recognised best practices for securing data and IT systems.	Small, medium and large organisations in the public and private sector.	**CIS: An overview**	

Find out more about how BT can help you with navigating compliance, regulations and frameworks by visiting: **btireland.com/securityadvisoryservices**

Offices Worldwide

April 2024