We are Ireland online

Tech

NIS2 Fact Sheet

For Technical staff, CISOs, Risk Managers

Cyber: Risk management

Obligations: Risk management measures should include measures to identify, protect, detect, respond, recover (Recital 40).

FAQs

Q: My small Registrar business is ISO-aligned. Isn't that secure enough for the NIS2 regulator?

A: No. Our Impact Assessment concludes that NIS2 is "High impact" for non-ISO aligned entities, because regulatory compliance is widely regarded as costly, resource intensive and administratively burdensome for SME companies (esp. providing audit evidence of controls).

Q: How do they expect NCSC, the "national competent authority" to regulate companies designated as "Essential Entities"?

A: Not yet confirmed, but looking at NIS1-designted **Operators of Essential Services (OES)**, we expect the NIST framework will be used.

Q: What is the NIST cyber security framework (CSF) ? Is it like ISO certification ?

A: No, it's benchmarking, not certification. The NIST CSF consists of the *Framework* ***Core***, the *Framework Implementation* ***Tiers***, and the *Framework* ***Profiles***. The ***Core*** consists of five concurrent and continuous functions; *Identify*, *Protect*, *Detect*, *Respond* & *Recover.*

Q : I'm just a supplier. Why must my regulated customer take account of vulnerabilities specific to each supplier, per Article 18(3) ?

A: The rationale is helpfully provided in Recital 43 (see below, right).

Key articles

- **Article 18 (1)** - Manage the risks – to prevent and minimise the IMPACT of incidents on recipients of their services. Take "appropriate" and "proportionate" measures.
- **Article 18 (2)** - must take an "all-hazards" approach to protect.
- **Article 18 (2a)** - supply chain security - must take account of vulnerabilities specific to each supplier 18(3). The rationale is helpfully provided in Recital 43.
- **Article 18 (4)** - corrective measures required without undue delay - must be appropriate and proportionate.

Recital 43

- Addressing cybersecurity risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security services and software editors, is ***particularly important*** given the prevalence of incidents where entities have fallen victim to attacks against network and information systems and where malicious actors were able to compromise the security of an entity's network and information systems ***by exploiting vulnerabilities*** affecting third party products and services.

Although voluntary and not intended to be an exhaustive checklist, the **NIST framework*** covers **five functions**, being critical areas of **data.**

**NIST*
National Institute of Standards and Technology (NIST) guidelines issued by *the US Dept of Commerce.*

Click here to se an example of NIST CSF in action.

	Function		Category
1.	**Identify**	Identify: looking at current data use and then evaluate and identify risk;	Asset Management
			Business Environment
			Governance
			Risk Assessment
			Risk Management Strategy
2.	**Protect**	Protect: the elements that help protect a business;	Access Control
			Awareness & Training
			Data Security
			Information Protection Processes & Procedures
			Maintenance
			Protective Technology
3.	**Detect**	Detect: being aware of problems as they happen;	Anomalies & Events
			Security Continuous Monitoring
			Detection Processes
4.	**Respond**	Respond: the bases needing to be covered to make an adequate response to a problem;	Response Planning
			Communications
			Analysis
			Mitigation
			Improvements
5.	**Recover**	Recover: the steps needed to make an effective recovery of lost data.	Recovery Planning
			Improvements
			Communications

Definitions

- **"TLDs"** = top level domain registries. This includes .com in addition to national country codes (like .ie .uk etc).
- **"EPRS"** = entities providing domain name registration services.
- "**Appropriate**" and "**proportionate**" security measures must take due account of severity of exposure, size, likelihood of occurrence, severity and societal/economic impact. Measures will be technical, operational and organisational. Article 18(1)
- "**All hazards**" approach includes theft, fire, flood, telecoms failures as well as unauthorised physical access/damage and malicious actions.
- **"NIST"** = One of the main ways in which businesses measure their preparedness in managing cyber-related security risks is to benchmark themselves against the Cybersecurity Framework developed by the NIST (National Institute of Standards and Technology, U.S. Department of Commerce).
- "**Essential Entities**" = *includes* Digital infrastructure (IXP; DNS; Top Level Domain (TLD) registries; cloud; data centre service providers; CDN; trust service providers; electronic communications)
- "**Important Entities**" = *include* digital providers such as online marketplaces; search engines; and social networks.

Nov 2022