Whitepaper

Endress+Hauser
People for Process Automation

How Endress+Hauser and Netilion support your regulatory compliance

By Steve North, Quality Manager Information Security Endress+Hauser Digital Solutions

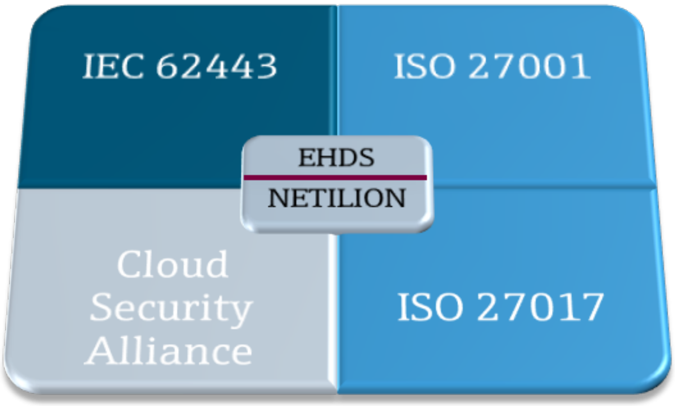
In 2016, the European Commission proposed the European Union's Network and Information Security (NIS) directive as the first piece of union-wide cybersecurity legislation, and member states quickly began adopting it. In 2022, the US enacted the Strengthening American Cybersecurity Act to increase its own level of national cyber-defense.

These two examples are only a fragment of the global efforts to create, standardize and enforce cybersecurity measures across multiple countries, industries, and agencies. These regulations primarily address operators of essential services (OES), to protect Critical Infrastructure – energy, water, health, etc. – against cyber-attacks.

Endress+Hauser is fully aware of the burden customers bear in complying with such legislation and provides a cybersecurity certification strategy to contribute to that compliance.

Note: This document mainly addresses using the Netilion cloud service in an industrial context. Endress+Hauser Digital Solutions does not qualify as an operator of essential service (OES), nor a digital service provider (DSP) as defined in the NIS.

Endress+Hauser Cybersecurity Certification Strategy (CS2)



Endress+Hauser, through its Digital Solutions (EHDS), has created a comprehensive Cybersecurity Certification Strategy (CS^2). It ensures information security with ISO/IEC 27001:2013, for which EHDS has held certification since 2021.
Furthermore, for the Netilion cloud service provided by EHDS, a third-party certification body confirmed its compliance with ISO/IEC 27017:2015, a control catalog for cloud applications.

Endress+Hauser also has group-wide certification of the secure development life cycle (SDLC) according to IEC 62443-4-1, ensuring that product development processes follow strict security practices.

Lastly, the Consensus Assessment Initiative Questionnaire (CAIQ) of the Cloud Security Alliance provides full transparency with regards to the security controls implemented in Netilion. The current status of Endress+Hauser certifications are available on a dedicated page of the official site.

Requirements of cybersecurity legislation

Across countries and industries, cybersecurity regulations share a similar structure. All OES must protect their IT infrastructure, properly manage their networks, and have processes to handle incidents. These requirements must also cover every link of the information supply chain. The details vary by region and industry, but the structure remains the same.

Let's take the NIS directive as an example. Chapter IV Article 14 states

1. *Member States shall ensure that operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed*
2. *Member States shall ensure that operators of essential services take appropriate measures to prevent and minimize the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services*

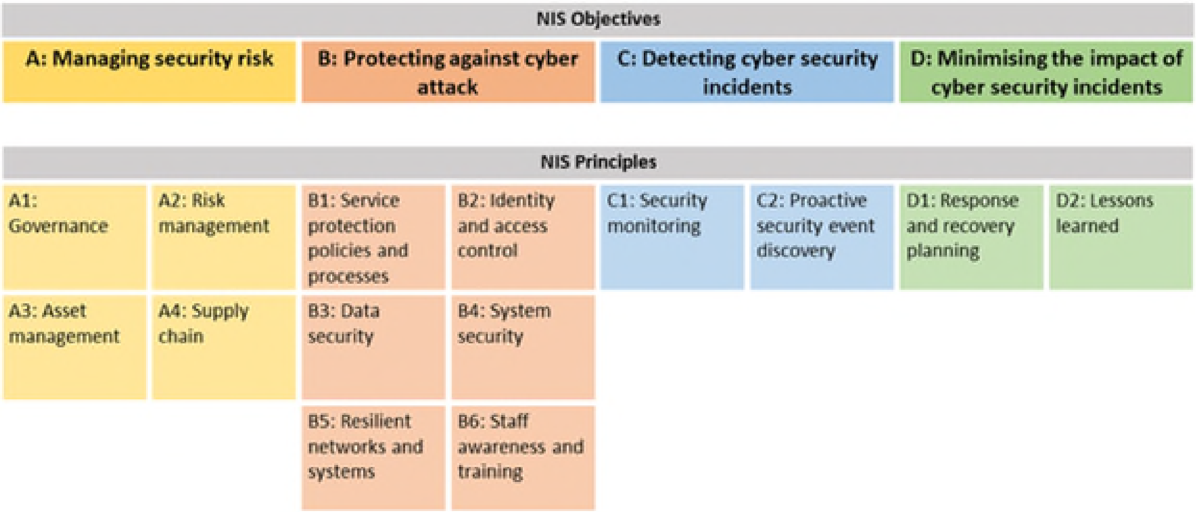
To provide guidance on "appropriate and proportionate technical and organizational measures" for "state of the art" technology, Chapter VI Article 19 states

1. *In order to promote convergent implementation of Article 14(1) and (2) and Article 16(1) and (2), Member States shall, without imposing or discriminating in favor of the use of a particular type of technology, encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.*

CS2 coverage of cybersecurity legislation

In providing cloud applications for customers, Endress+Hauser and Netilion play an important role in supporting cybersecurity. Many users qualify as OES and must remain compliant while using Netilion.

With its Cyber Assessment Framework, the UK National Cyber Security provides an overview of NIS principles.



NIS Objectives							
A: Managing security risk		B: Protecting against cyber attack		C: Detecting cyber security incidents		D: Minimising the impact of cyber security incidents	

NIS Principles							
A1: Governance	A2: Risk management	B1: Service protection policies and processes	B2: Identity and access control	C1: Security monitoring	C2: Proactive security event discovery	D1: Response and recovery planning	D2: Lessons learned
A3: Asset management	A4: Supply chain	B3: Data security	B4: System security				
		B5: Resilient networks and systems	B6: Staff awareness and training				

Source: *UK National Cyber Security Center*

We can then use this framework to outline Endress+Hauser's Cyber Security Certification Strategy, especially the security controls stemming from ISO/IEC 27001:2013

NIS principles	Endress+Hauser CS^2 controls
A1 – Governance	A6. Organization of information security
A2 – Risk Management	P1. Risk management policy
A3 – Asset Management	A8. Asset management
A4 – Supply Chain	A15. Supplier relationship
B1 – Service Protection Policies and Processes	A5. Information security policies
B2 – Identity and Access Control	A9. Access control
B3 – Data Security	A10. Cryptography
B4 – System Security	A12. Operations security
B5 – Resilient Network and Systems	A13. Communication security
B6 – Staff Awareness Training	A7. Human resource security
C1 – Security Monitoring	A12. Operations security
C2 – Proactive Security Event Discovery	A16. Information security incident management
D1 – Response and Recovery Planning	A17. Business continuity management
D2 – Lessons Learned	P3. Non-conformity handling

Conclusion

Complying with cybersecurity legislations and regulations can challenge OES within their own structures, so third-party suppliers of network devices and cloud systems must support that compliance as much as possible.

By entrusting data and network access to external players, OES only maintain partial control of their systems, making them vulnerable to non-compliance and cyber-attacks. The best digital service providers hold relevant and valid certifications, like ISO/IEC 27001:2013 and/or IEC 62443-4-1:2018, to reduce those risks dramatically.

Certification provides independent confirmation that digital service providers follow internationally accepted standards and industry best practices. Through its Cybersecurity Certification Strategy, Endress+Hauser Digital Solutions provides all the security necessary to support customers in cybersecurity compliance, particularly in the context of using cloud systems like Netilion.