DPS

NIS2 Compliance
Deadline Has Passed

Protect Your Critical Infrastructure

Industrial control systems are under constant threat. Meet your compliance obligations under NIS2, the UK Cyber Security Bill, and IEC 62443 with our full lifecycle cybersecurity services.

- Comprehensive OT/IT security assessments
- Full regulatory compliance support
- Minimal operational disruption

Why DPS?

25+
Years Experience

500+
OT Environments Secured

12+
Industries Served

30+
Countries

€10M maximum NIS2 Fines
or 2% of global turnover

83% of OT environments
experienced a breach in 2024

21 days average downtime
after a ransomware attack

€25K Cost per minute
of unplanned downtime

Digital Process Solutions
dp-sgroup.co.uk

Regulatory Landscape

Critical Compliance Requirements

Industrial operators face an increasingly complex regulatory environment. Understanding your obligations is the first step toward compliance.

Effective 2025

UK Cyber Security & Resillience Bill

New legal obligations for critical national infrastructure operators with mandatory incident reporting and enhanced regulatory oversight.

- Mandatory incident reporting within 24 hours
- Enhanced powers for regulatory bodies
- Criminal liability for non-compliance
- Annual security assessments required

Effective October 2024

NIS2 Directive

The expanded EU directive covering more sectors and supply chains with stricter enforcement mechanisms across all member states.

- Risk management policies mandatory
- Supply chain security requirements
- Incident reporting within 24-72 hours
- Management accountability provisions

Industry Best Practice

IEC 62443 Standard

The international standard for industrial automation and control systems security throughout the entire lifecycle.

- Security levels for zones and conduits
- Risk assessment methodology
- Security lifecycle requirements
- Component security requirements

Consequences of Non-compliance

The Cost of Inaction

Non-compliance and security breaches carry severe consequences across legal, operational, and strategic dimensions.

Legal & Financial Penalties

- **€10M** or 2% of global annual turnover, whichever is higher for essential entities
- **Personal** director accountability under UK Cyber Security & Resilience Bill
- **24 hrs** mandatory notification for significant incidents under NIS2

Operational Impact

- **€25,000+ Unplanned Downtime**
  Average cost per minute of downtime in manufacturing environments
- **21 days Extended Recovery**
  Average time to recover from a ransomware attack on OT systems
- **73% Supply Chain Impact**
  of breaches affect downstream customers and partners
- **Critical Safety Compromise**
  OT breaches can directly impact physical safety and operations

Strategic Risks

- **Reputational Damage**
  Loss of stakeholder confidence and public trust following a breach disclosure
- **Insurance Implications**
  Non-compliance may void coverage or result in significantly increased premiums
- **Competitive Disadvantage**
  Security-conscious markets increasingly require proven compliance credentials
- **National Security**
  Critical infrastructure breaches can impact public safety and national security

Who Must Comply?

The international standard for industrial automation and control systems security throughout the entire lifecycle.

- Energy & Utilities
- Water Treatment
- Manufacturing
- Transport
- Healthcare
- Chemical Processing
- Oil & Gas
- Food & Beverage

Don't wait for an incident or regulatory action. Proactive compliance is significantly less costly than reactive remediation.

Digital Process Solutions

dp-sgroup.co.uk