Talanos
cybersecurity

www.talanoscybersecurity.com

The UK Cybersecurity Regulatory Landscape: An Overview for Medium-Sized Enterprises

Mandatory Regulations

UK GDPR & DPA 2018

Key focus: Personal data protection requirements.

Max penalty: £17.5M or 4% annual turnover

NIS Regulations

Key focus: Network security for essential services.

Max penalty: £17M

FCA Regulations

Key focus: Operational resilience requirements.

Max penalty: Variable fines + activity restrictions

PECR Regulations

Key focus: Electronic communications security.

Max penalty: £500,000

Key Standards

Cyber Essentials

Basic security requirements: firewall, secure configuration, access control, malware protection, patch management.

Benefits: Government contract eligibility, basic protection

Cyber Essentials Plus

Includes the same requirements as Cyber Essentials, with additional independent testing.

Benefits: Independent verification, enhanced credibility

NIST CSF v2

Risk-based cybersecurity framework designed to help organisations identify, protect against, respond to, and recover from cyber threats.

Benefits: Risk-focused, regulatory alignment

ISO 27001:2022

International standard for information security management systems. Specific monitoring, threat intelligence, and incident response requirements.

Benefits: International recognition, extensive coverage

PCI-DSS

For businesses that handle payment card data, compliance with PCI DSS is mandatory. This standard is set by the major card schemes (Visa, Mastercard, etc.) rather than by legislation.

Industry-Specific Requirements

Financial Services

PSD2 (Payment Services Directive 2)

SYSC (Senior Management Arrangements, Systems and Controls)

EU Digital Operational Resilience Act (DORA)

Healthcare

NHS Digital Data Security

Medical Device Regulations

Data protection specifics

Public Sector

Government Supplier Assurance

Minimum Cyber Security Standard

Procurement requirements

Telecomms

Telecommunications (Security) Act 2021

European Electronic Communications Code (EECC)

Ofcom Security Framework

Coming soon...

UK Cyber Security and Resilience Bill: Announced in July 2024 and currently undergoing legislative processes.

EU Artificial Intelligence Act (AI Act): Expected in 2025

EU Cyber Resilience Act (CRA): Expected in 2025

Need help navigating the Cybersecurity compliance landscape? Contact our team of experts here.

This infographic provides general information about UK cybersecurity regulations and standards as of March 2025 and is intended for educational purposes only. While every effort has been made to ensure accuracy, this document should not be considered comprehensive legal advice or a substitute for professional consultation.