WISE IT SOLUTIONS

UK compliance guide for IT

What the security and resilience rules UK businesses most often face mean for your systems, in plain English.

Last reviewed: November 2026 · Current version: wise-its.uk/compliance

Please read first. This guide summarises; it is not legal advice. Regulations apply to your business and only you can sign the declarations. Rules change: check the current version online at **wise-its.uk/compliance**, and ask your legal or compliance adviser to confirm what applies to you.

Contents

Cyber Essentials and Cyber Essentials Plus	Any UK organisation
UK GDPR and the Data Protection Act 2018	Any organisation handling personal data about people in the UK
NIS Regulations and the CSR Bill	Currently operators of essential services (such as energy, transport, water and health) and certain digital service providers
FCA operational resilience	Many FCA-regulated firms, including banks, insurers and larger investment firms
DORA (EU Digital Operational Resilience Act)	EU financial entities since 17 January 2025, and in practice UK businesses that supply them with technology services
NHS Data Security and Protection Toolkit	Organisations with access to NHS patient data and systems, including many suppliers and care providers
PCI DSS (card payments)	Any business that takes, processes or stores card payments

Cyber Essentials and Cyber Essentials Plus

Who it applies to

Any UK organisation. Required for some government contracts, and increasingly asked for by customers and insurers.

What it requires

A government-backed scheme covering five technical controls: firewalls, secure configuration, security update management, user access control and malware protection. Cyber Essentials is a verified self-assessment; Plus adds hands-on technical testing. Certification is renewed every year.

What it means for your IT

- Every in-scope device supported and updated within the scheme's timescales
- Multi-factor authentication on cloud services
- Administrator rights kept to a minimum
- Evidence ready for the certification body

Full guide: wise-its.uk/compliance/cyber-essentials/ · **Related:** Cyber Essentials readiness · Cyber Essentials explained

UK GDPR and the Data Protection Act 2018

Who it applies to

Any organisation handling personal data about people in the UK.

What it requires

Requires "appropriate technical and organisational measures" to keep personal data secure, and certain personal data breaches to be reported to the Information Commissioner's Office within 72 hours of becoming aware of them.

What it means for your IT

- Access to personal data limited to people who need it
- Encryption on laptops and phones
- Backups that can be restored, and records of tests
- A way to detect, assess and record incidents quickly

Full guide: wise-its.uk/compliance/uk-gdpr/ · **Related:** Cyber security and incident response · Evidence register

NIS Regulations and the CSR Bill

Who it applies to

Currently operators of essential services (such as energy, transport, water and health) and certain digital service providers.

What it requires

The NIS Regulations 2018 require in-scope organisations to manage cyber risk and report significant incidents. The Cyber Security and Resilience Bill, introduced to Parliament in November 2025, proposes extending this to managed service providers, data centres and critical suppliers. Check the current status, as the detail may change.

What it means for your IT

- Supplier security reviewed, including your IT provider
- Incident detection and reporting routes agreed in advance
- Risk management documented and reviewed
- Evidence that controls are working, not just written down

Full guide: wise-its.uk/compliance/nis-and-cyber-security-resilience-bill/ · **Related:** How we access your IT · Cyber maturity model

FCA operational resilience

Who it applies to

Many FCA-regulated firms, including banks, insurers and larger investment firms.

What it requires

In-scope firms must identify their important business services, set impact tolerances for how much disruption they can tolerate, and show they can stay within them, including through severe but plausible scenarios. The FCA's deadline for firms to be able to remain within tolerance was 31 March 2025.

What it means for your IT

- Systems mapped to the business services they support
- Recovery tested against impact tolerances
- Third-party and outsourcing risk managed
- Scenario testing recorded, with lessons acted on

Full guide: wise-its.uk/compliance/fca-operational-resilience/ · **Related:** Backup and disaster recovery · Tabletop exercise

DORA (EU Digital Operational Resilience Act)

Who it applies to

EU financial entities since 17 January 2025, and in practice UK businesses that supply them with technology services.

What it requires

DORA sets requirements for ICT risk management, incident reporting, resilience testing and the management of ICT third parties. UK suppliers to EU financial firms may be asked for contractual commitments on security, incident notification, audit access and exit plans.

What it means for your IT

- Clear contractual terms on incident notification and exit
- Evidence of security controls and testing
- Documented subcontractors and delivery partners
- A tested exit plan for the service

Full guide: wise-its.uk/compliance/dora/ · **Related:** Trust centre · Contracts and switching

NHS Data Security and Protection Toolkit

Who it applies to

Organisations with access to NHS patient data and systems, including many suppliers and care providers.

What it requires

An annual online self-assessment of data security and protection. NHS England has been moving the toolkit to align with the National Cyber Security Centre's Cyber Assessment Framework, so requirements for some organisations are changing.

What it means for your IT

- Staff training and access controls evidenced
- Devices and systems supported and updated
- Backups and business continuity tested
- Incidents reported through the right routes

Full guide: wise-its.uk/compliance/nhs-dspt/ · **Related:** Cyber security · IT manager cover checklist

PCI DSS (card payments)

Who it applies to

Any business that takes, processes or stores card payments.

What it requires

The card industry's security standard. Version 4.0.1 is current, and its future-dated requirements became mandatory on 31 March 2025. Your payment provider tells you which self-assessment applies.

What it means for your IT

- Card systems kept separate from the rest of the network
- Multi-factor authentication for access to card data environments
- Updates and malware protection on payment devices and systems
- Logs kept and reviewed

Full guide: wise-its.uk/compliance/pci-dss/ · **Related:** Networks and communications · Cyber security

Where do you stand?

Take the free five-minute cyber maturity self-assessment at **wise-its.uk/resources/cyber-maturity-model**, or ask us for an evidence review at **wise-its.uk/contact**. Wise IT Solutions provides the technical controls, the evidence and the advice; compliance decisions stay with you.

© Wise IT Solutions. Free to share in full with this notice. Last reviewed November 2026.