

UK Cyber Security Regulation, What Your Organisation Needs to Know

A plain English guide to the changes coming in 2026 and how to prepare

Why this matters now

The UK cyber security regulatory landscape is entering its biggest period of change in almost a decade. The Cyber Security and Resilience Bill is expected to become law during 2026, widening the scope of regulation well beyond critical national infrastructure. If your organisation operates in a regulated sector, provides digital services, or supplies organisations that do, these changes are likely to affect you, regardless of whether you consider yourself in scope today.

The good news is that 2026 is a preparation year, not a deadline. Organisations that start reviewing their position now will be in a far stronger place than those who wait for the regulations to be finalised.

The current and emerging framework

Framework	Status	Applies to	Key obligation
UK GDPR / Data Protection Act 2018	In force	All organisations processing personal data	Appropriate technical and organisational measures; 72-hour breach reporting
NIS Regulations 2018	In force, being superseded	Operators of essential services, digital service providers	Proportionate security measures; incident reporting to competent authority
Cyber Essentials / Cyber Essentials Plus	In force, v3.3 update expected April 2026	Any organisation, often mandatory for public sector contracts	Baseline technical controls; MFA to become mandatory across all cloud services
FCA / PRA operational resilience rules	In force	Regulated financial services firms and their supply chains	Map important business services, set impact tolerances, test resilience to disruption
UK Cyber Security and Resilience Bill	Before Parliament, expected Royal Assent in 2026	MSPs, data centres, large load controllers, designated critical suppliers, and their supply chains	Mandatory incident reporting on tight deadlines; turnover based penalties up to GBP 17 million or 4 percent of global turnover

What is changing, in brief

A new Cyber Security and Resilience Bill

- Expands regulation to cover managed service providers, data centres, and critical suppliers, on top of the existing NIS Regulations
- Introduces mandatory incident reporting on tight deadlines
- Brings in penalties of up to GBP 17 million or 4 percent of global turnover for serious breaches, with daily penalties for ongoing non compliance

A tougher Cyber Essentials standard

- An updated version is expected in April 2026
- Multi factor authentication will become mandatory across all cloud services, not only higher risk systems
- All internet connected devices will be confirmed as within scope

Wider exposure if you work with the EU or in financial services

- If you serve EU customers or operate EU subsidiaries, the EU NIS2 Directive already applies, with personal liability for senior management
- If you are a regulated financial services firm, the FCA, PRA, and DORA all expect demonstrable operational resilience testing, including penetration testing

How Akita can help

Akita Cyber Security works with organisations across financial services, professional services, and technology to translate regulatory change into a practical, prioritised plan. Depending on where you are today, that might mean:

- A GRC assessment to establish exactly which frameworks apply to you and where the gaps are
- CISO as a Service, giving you board level ownership of cyber risk without a full-time hire
- Penetration testing and continuous testing through our unique solution, to meet resilience testing expectations and keep pace with a changing threat landscape
- Cyber intelligence to manage supply chain risk, a theme that runs through every framework above

Not sure where your organisation stands?

Book a free, no obligation discovery call with Akita Cyber Security. We will listen to your current set up, talk through which of these frameworks apply to you, and share what we are seeing work well for organisations like yours. This is a conversation, not a sales pitch.

Andy Lowy, VP Sales and Marketing

Email: andy.l@akitacyber.com

Phone: +44 7537 158632

Book directly: [UK Cyber Security Regulation Consultation](#)