

WHICH BUSINESS CERTIFICATION IS RIGHT FOR YOU?

ISO 9001 • ISO 27001 • ISO 14001 • Cyber Essentials • Cyber Essentials Plus

Certification is evidence — not a guarantee.

ISO 9001 Quality Management System Covers: Documented processes, customer satisfaction, continual improvement, quality objectives OK: Any organisation wanting to demonstrate consistent quality and customer focus 3-year cycle • Annual surveillance audits	ISO 27001 Information Security Management Covers: Information security risks, confidentiality, integrity, availability, controls (Annex A) OK: Finance, legal, technology, healthcare — any organisation handling sensitive data 3-year cycle • Annual surveillance audits
ISO 14001 Environmental Management System Covers: Environmental impacts, energy use, waste reduction, emissions, continual improvement OK: Manufacturing, construction, logistics, organisations with sustainability commitments 3-year cycle • Annual surveillance audits	Cyber Essentials UK Government-backed cyber scheme Covers: Firewalls, secure configuration, user access control, malware protection, patching OK: Any UK business — mandatory for many government supply chains Annual renewal • Self-assessment reviewed by accredited assessor
Cyber Essentials Plus Independent technical verification of the five Cyber Essentials controls	OK: Technology companies, MSPs, regulated sectors, higher-value government contracts • Annual renewal • Assessor performs hands-on testing of devices and systems

AT A GLANCE COMPARISON					
	ISO 9001	ISO 27001	ISO 14001	CE	CE+
Covers quality	YES				
Covers security		YES		YES	YES
Covers environment			YES		
UK Government				YES	YES
Independent technical					YES
Annual renewal				YES	YES
3-year cycle with audits	YES	YES	YES		
Risk assessment required		YES	YES		

Which Certification Fits Your Business?

RECOMMENDED STARTING POINT BY BUSINESS TYPE

Accountancy / Finance	Cyber Essentials, ISO 27001	Client financial and personal data
Construction / Engineering	ISO 9001, ISO 14001	Quality of work and environmental impact
Manufacturer	ISO 9001, ISO 14001	Quality management and sustainability
Legal / Solicitor	Cyber Essentials, ISO 27001	Client confidentiality and data handling
Technology company / MSP	Cyber Essentials Plus, ISO 27001	Technical customers expect verified security
Healthcare	Cyber Essentials, ISO 27001, ISO 9001	Patient data, care quality, regulation
Charity	Cyber Essentials, ISO 9001	Donor trust, grant eligibility, governance
School / Education	Cyber Essentials, ISO 9001	Safeguarding data, quality of provision
Government supply chain	Cyber Essentials (mandatory)	Required for contracts involving personal data
Professional services	Cyber Essentials, ISO 27001	Client data and supply chain confidence

COMMON MYTHS

Certification means we are completely secure

FALSE — Certification confirms you met requirements at the time of assessment. Threats evolve and certification is a baseline, not a finish line.

Certified organisations never make mistakes

FALSE — Certified organisations have processes to identify and prevent recurrence. They still experience incidents.

Certification replaces management

FALSE — Management systems require ongoing leadership commitment, audit and review. Certification tests whether this is happening.

Once certified, we don't need to renew

FALSE — ISO certifications need annual surveillance audits. Cyber Essentials requires annual renewal. Lapsing is itself a risk.

CERTIFICATIONS NEED AN OPERATIONAL HEARTBEAT

OK: Policies reviewed and updated

OK: Risk register current

OK: Security controls tested

OK: Internal audits on schedule

OK: Supplier reviews completed

OK: Training current for all staff

OK: Management review conducted

OK: Corrective actions closed and verified

Businesses don't earn trust through logos or marketing slogans. They earn it through consistent good practice, with independent certification providing evidence of that commitment.



itclub.work/
knowledge-centre