Cyber Essentials Readiness Diagnostic

Score Your Readiness in 5 Minutes

This diagnostic identifies your current readiness for Cyber Essentials certification based on the seven most common failure points we see in SME submissions.

How to use this diagnostic: For each statement below, give yourself 4 points if it's fully true, 2 points if it's partially true, or 0 points if it's not true. Total your score at the end to see where you stand.

1. SCOPE UNDERSTANDING (Max 12 points)

■ We have mapped our complete digital estate including office devices, remote workers, mobile phones, cloud services, and all internet-connected systems (4 points)

■ We understand that BYOD devices, home-working laptops, and cloud infrastructure must be included in scope (4 points)

■ We have documented our scope definition clearly and can explain what's included and why (4 points)

2. MSP & DOCUMENTATION READINESS (Max 12 points)

■ If we use an MSP, we have confirmed they can provide certification-ready documentation (firewall configs, patch management evidence, access control policies) (4 points)

■ We understand which controls are our MSP's responsibility vs. our organisational responsibility (4 points)

■ We have documented policies and processes for security controls, not just verbal assurances (4 points)

3. PATCH MANAGEMENT (Max 12 points)

■ We have visibility into patch status across our entire estate (not just relying on 'automatic updates') (4 points)

■ We can demonstrate that critical security patches are applied within 14 days of release (4 points)

■ We have a documented process for managing patch exceptions and tracking compliance (4 points)

4. MULTI-FACTOR AUTHENTICATION (Max 12 points)

■ MFA is enabled for all remote access to our systems and all administrator accounts (4 points)

■ We use app-based or hardware token MFA (not just SMS codes) (4 points)

■ Any MFA exceptions are documented with clear business justification (4 points)

5. USER ACCESS & SHARED ACCOUNTS (Max 12 points)

■ Every user has their own unique account—we have eliminated all shared logins (4 points)

■ User access rights are appropriate to roles, with admin privileges limited to those who genuinely need them (4 points)

■ We have a process for promptly disabling/removing accounts when people leave and regularly review access rights (4 points)

6. FIREWALL & NETWORK BOUNDARIES (Max 12 points)

■ Our boundary firewall is configured with deny-by-default rules and we can export/explain our ruleset (4 points)

■ Default credentials have been changed and unnecessary services (UPnP, remote management) are disabled (4 points)

■ Guest WiFi and IoT devices are properly segmented from our business network (4 points)

7. PREPARATION & PLANNING (Max 12 points)

■ We are starting this process at least 4-6 weeks before we need certification (4 points)

■ We have gathered evidence for our controls (screenshots, config exports, policy documents) before submission (4 points)

■ We have conducted an honest gap assessment and addressed weaknesses before formal certification (4 points)

YOUR SCORE & NEXT STEPS

Add up your points from all seven sections. Your total score (out of 84 possible) indicates your certification readiness:

68-84 POINTS: CERTIFICATION READY

You're in strong shape for Cyber Essentials certification. Your controls are largely implemented and documented. You likely just need a quick validation to confirm everything aligns with CE requirements before formal submission.

Recommended next step: Book a Readiness Validation Call (from £950) to confirm you're ready and identify any minor gaps before submission.

40-67 POINTS: GAPS IDENTIFIED

You have foundational controls in place but there are clear gaps in implementation or documentation. These gaps will cause problems during formal assessment—likely resulting in back-and-forth clarifications or failed submission.

Recommended next step: Book a Structured Assessment & Readiness Package (from £1,750) to identify all gaps, get guidance on fixing them, and prepare your evidence pack properly.

0-39 POINTS: FOUNDATION NEEDED

You're starting from low maturity and attempting certification now would likely fail or require extensive rework. You need comprehensive support to build controls properly before formal assessment.

Recommended next step: Book a Cyber Assurance Pathway consultation (from £3,500) for end-to-end support implementing controls, documenting processes, and preparing for certification.

Ready to Move Forward?

At Idela, we match support to your actual readiness level—no over-engineering, no under-investing. Our readiness-first approach means you only submit for formal certification when you're genuinely ready.

READINESS VALIDATION	STRUCTURED ASSESSMENT	COMPREHENSIVE PATHWAY
68-84 points	40-67 points	0-39 points
Quick validation call + minor gap identification	Full gap assessment + documentation guidance	End-to-end implementation support
From £950	From £1,750	From £3,500

Start with a Free 15-Minute Readiness Call

We'll discuss your score, identify your biggest gaps, and recommend the best path forward.

No obligation. No sales pressure. Just honest guidance.

■ letstalk@idelaonline.com | ■ +44 20 7946 0958

■ www.idelaonline.com

Idela is an IASME-approved Certification Body specialising in Cyber Essentials and IASME Cyber Assurance for UK organisations. We believe certification should be clear, achievable, and built on genuine capability—not confusion or box-ticking.