



Cyber Essentials Update: Key changes from April 2026 for the engineering sector

From 27th April 2026, a new set of refinements to the Cyber Essentials and the Cyber Essentials Plus certifications will officially come into effect.

It is important to note that these changes do not rewrite the five core technical controls: firewalls, secure configuration, user access control, malware protection, and patch management. These remain the foundational pillars of the scheme.

Instead, the [IASME 2026](#) update focuses on strengthening organisational proof of compliance, mandatory protections for cloud services, and ways to collect stronger, more reliable evidence for assessments. By tightening these requirements, the update provides an increase in credibility of the Cyber Essentials scheme and ensures it remains as important and as valuable as ever.

For engineering organisations, these updates arrive at a time when digital transformation is rapidly reshaping how manufacturing and production environments operate.

The evolving cyber threat landscape for engineering businesses

Engineering businesses, especially here in Scotland, sit at the heart of the nation's manufacturing strength, yet they also carry some of the most exposed operational risk when it comes to cyber threats.

The shift toward digitally connected workshops, automated production lines and data-driven engineering processes means that systems once isolated on factory floors and workshops are now deeply integrated across entire organisations.

That connectivity is powerful, but it also widens the attack surface. A single compromised controller, outdated PLC, or unpatched engineering workstation can act as an entry point for attackers looking to disrupt production, tamper with calibration data or compromise design files.

In engineering environments where precision, safety and uptime are non-negotiable, even a small cyber incident can quickly escalate into lost output, compliance issues, or reputational damage.

Scottish engineering firms operate within a uniquely interconnected ecosystem. Many supply into critical national infrastructure, energy, transport, defence and aerospace sectors, where resilience isn't simply a desirable feature but an operational requirement.

At the same time, Scotland's engineering sector is dominated by SMEs who often juggle ageing specialist equipment, limited downtime windows and complex supplier relationships. This creates a perfect storm where legacy technology meets modern cyber risk.

Against this backdrop, structured cyber security frameworks such as Cyber Essentials have become increasingly important.

What are Cyber Essentials and Cyber Essentials Plus?

[Cyber Essentials](#) is a UK government-backed certification scheme designed to help organisations protect themselves against the most common cyber threats. At its core, the framework focuses on essential technical controls that significantly reduce the likelihood of a successful attack. These include firewalls, secure configuration, user access control, malware protection, and patch management.

For many engineering organisations, Cyber Essentials provides a practical baseline for securing the everyday systems that underpin operations, including office IT networks, cloud services, remote access systems, and connected engineering workstations.

Cyber Essentials certification is achieved through a verified self-assessment questionnaire that confirms these controls are correctly implemented across the organisation's IT environment.

Cyber Essentials Plus goes a step further. It includes an independent technical audit carried out by an external assessor who verifies the security controls in practice through vulnerability scans and device testing.

For engineering businesses supplying into sectors such as energy, defence, aerospace, or infrastructure, Cyber Essentials Plus is often requested by customers or procurement frameworks as evidence that robust cyber security standards are in place.

Beyond compliance, certification demonstrates to partners, regulators, and customers that cyber security is treated as a core part of operational resilience.

Key changes

Leaving no grey areas or room for interpretation, here are the coming 2026 updates to the Cyber Essentials scheme.

High risk and critical patches must be applied within 14 days

This is arguably the most significant shift for IT teams. Previously, the 14-day rule was a strong guideline – now it is a strict requirement.

If a vendor releases a patch for a critical or high-risk vulnerability, you have exactly 14 days to apply it to every device, server, and application in your scope. If an assessor finds even one device missing a critical update older than two weeks, the organisation automatically fails the assessment.

Multi-factor authentication (MFA) must be enabled for all cloud services

Account takeovers are one of the most common ways businesses are breached. To combat this, multi-factor authentication is now mandatory for all cloud services.

If a service provider offers MFA, whether it's included for free or requires a paid upgrade, you must enable it for all users and not just administrators. If it is available but not active, the result will be automatic failure.

This update removes cost or inconvenience as excuses for leaving accounts protected by only a password.

Cloud services cannot be excluded from scope

In previous years, some organisations tried to narrow their scope to exclude certain cloud platforms. The 2026 update closes this loophole.

The new definition of a cloud service is simple – if it stores or processes your organisational data and is accessed via business credentials, it is in scope. This includes everything from Microsoft 365 and Google Workspace to your CRM, HR platforms, and cloud storage. If your data lives there, the service must meet CE standards.

CE+ introduces stricter retesting rules

For those pursuing Cyber Essentials Plus (the audited version of the scheme), the spot check just got harder. In the past, if an assessor found a flaw on a specific device, the organisation might fix just that one device to pass.

Under the new rules, if a device in the initial sample fails the update check, the assessor must test a second random sample. If the second sample also fails, the organisation fails the entire certification. This ensures that your security fixes are applied across the whole company and not just to the devices the auditor happens to look at.

Organisations must now provide clearer scoping definitions and stronger evidence

The days of providing a one-sentence description of your network are over. The 2026 update demands transparency. Organisations must now provide detailed descriptions of their infrastructure, including every legal entity included in the certification.

Furthermore, if you choose to exclude a part of your network, you must provide strong evidence of how it is segregated from the rest of the business. Assessors will now require more documentation to prove that your boundaries are real and secure.

Why strong cyber fundamentals matter for engineering firms

Ensuring strong technical controls, secure configurations, and clear access boundaries in engineering environments protects not only the plant, but the extended supply chain these organisations support.

Independent validation of your security posture helps demonstrate that essential safeguards are in place, operating effectively and aligned with industry best practice; giving customers, partners and regulators confidence that security is embedded from the workshop to the boardroom.

For the engineering community, resilience isn't just about preventing downtime. It is about ensuring continuity in sectors where Scotland has deep heritage and global reputation.

Whether producing precision components, supporting energy transition projects or innovating in advanced manufacturing, engineering businesses must treat cyber security as a core part of operational excellence.

Simple, robust security fundamentals reduce the likelihood of attacks entering through the most common routes such as phishing, misconfigurations or human error, while also providing a foundation for safe, sustainable growth as digital transformation accelerates.

By taking a proactive, structured approach to cyber resilience, Scotland's engineering sector can protect its talent, its intellectual property and its contribution to the wider Scottish economy.

Steps to help organisations prepare

With the deadline fast approaching, the best strategy is to begin reviewing your current setup now. Here is how you can get ahead of the curve:

Review all cloud services and enforce MFA

Your first step should be a comprehensive cloud audit. You need to list every platform your employees use to conduct business, from major suites like Microsoft 365 to smaller, more niche tools. Once identified, you must confirm that multi-factor authentication is active for every single account without exception – from the CEO to the newest employee.

It is important to distinguish between MFA being available and being enforced. Many platforms allow users to opt in, but to pass the new criteria, your administrative settings must require the second factor at every login. Don't forget the smaller SaaS tools like marketing platforms or project management apps; if they hold organisational data, they must be protected.

Strengthen asset management

You cannot secure what you do not know exists, so make asset management the foundation of your compliance. You should maintain an accurate and up to date master inventory that includes every device capable of connecting to your network or accessing business data.

If you have out of scope areas, such as a guest Wi-Fi network or legacy systems used for specific tasks, you must provide clear documentation and technical evidence of how they are segregated. For instance, via a robust firewall or a separate VLAN.

Furthermore, pay close attention to 'bring your own device' policies. If staff use personal phones for work emails or Teams, those devices are officially in scope and must meet the same security standards as company-owned hardware.

Tighten patch management

To meet the strict new 14-day window for critical updates, your team likely needs to move beyond manual checks. We recommend implementing automated solutions, such as Mobile Device Management (MDM) or central patching tools, which can push updates to all devices simultaneously the moment they are released.

It is also wise to assign a specific team member to monitor security bulletins, so your organisation is alerted the second a high-risk vulnerability is announced. To ensure you are ready for the live assessment, consider enacting a test run; if a critical patch were released today, could your current processes realistically deploy it to every single device in the company within two weeks?

Review and restrict administrative privileges

While this isn't a brand-new requirement for 2026, the updated standard places renewed emphasis on strengthening identity and access controls across the organisation, particularly around admin privileges and modern authentication.

The most important rule to enforce is that no user, including IT staff, should use an account with administrative rights for everyday tasks like reading emails or browsing the web. Instead, administrators should maintain two separate accounts: a standard one for daily work and a separate, highly secured admin account used exclusively for specific technical changes.

Finally, establish a routine to audit these permissions at least once a quarter. This ensures that access is revoked for employees who have changed roles or left the company, keeping your attack surface as small as possible.

OT security for engineering

Operational Technology (OT) security has become one of the most critical challenges for engineering and manufacturing firms, particularly those running mixed environments where legacy machinery meets modern connectivity.

Unlike traditional IT systems, OT environments are built for safety, precision, and uptime, not security, making them uniquely vulnerable when connected to corporate networks or remote access systems.

Many Scottish engineering businesses operate equipment that is decades old, irreplaceable, or no longer supported, yet now integrated into digital workflows for monitoring, maintenance or data capture.

This creates a situation where a single exposed interface or compromised remote connection can lead directly to disruption of physical processes. Strengthening OT security means applying robust access controls, monitoring for unexpected behaviour on production networks, and ensuring engineering teams and IT teams work together rather than in silos.

With Scotland's engineering sector contributing to critical national infrastructure, energy transition projects, and advanced manufacturing, protecting OT is no longer optional, it's essential to maintaining safe operations, safeguarding intellectual property and ensuring continuity across the wider Scottish supply chain.

Need support preparing for Cyber Essentials certification?

The 2026 Cyber Essentials updates represent a shift toward a more resilient UK business landscape, moving away from tick-box compliance to genuine operational security. While the 'auto-fail' criteria might seem daunting, they are designed to protect you from the very real, very common tactics used by cyber criminals today.

With our team of specialists, we can guarantee thorough and efficient analysis of your business – closing gaps and emitting vulnerabilities to keep your network up to date with the latest Cyber Essentials and Cyber Essentials Plus regulations.

[Get in touch](#) today to maximise cyber resilience for your business.