Cyber Essentials Renewal Checklist

Incorporating the April 2026 Scheme Revisions

Context for UK organisations

From April 2026, Cyber Essentials introduces several important updates that directly affect small and medium-sized UK solicitor practices. These changes strengthen expectations around cloud security, device management, vulnerability handling, and governance. Firms preparing for renewal must ensure their systems, processes, and documentation align with the revised requirements.

This checklist provides a clear, practical overview of what your organisation must now consider ahead of your next assessment.

---

1. Cloud Services (Now Fully in Scope)

- Identify all cloud services used to store, process, or access organisational or client data.
- Confirm each service meets Cyber Essentials technical controls.
- Ensure secure configuration settings are applied and documented.
- Verify MFA is enabled for all cloud accounts.
- Review vendor responsibilities vs. firm responsibilities (shared responsibility model).

---

2. Mandatory Multi-Factor Authentication (MFA)

- Enable MFA for all users and administrators on every cloud platform where supported.
- Ensure MFA is enforced, not optional.
- Review and remove legacy authentication methods.
- Document MFA policies and user guidance.

---

3. Vulnerability Management & 14-Day Patching Requirement

- Implement a structured vulnerability management process.
- Patch all vulnerabilities rated CVSS 7.0+ within 14 days.
- Maintain evidence of patching timelines and approvals.
- Ensure automated update mechanisms are enabled where possible.

---

4. Firewall & Router Firmware Updates

- Identify all firewalls, routers, and boundary devices.
- Track firmware versions and vendor security advisories.
- Apply high/critical firmware updates within 14 days.
- Document firewall rule changes and approval processes.

---

5. Windows 10 Devices (Post-October 2025)

- Identify all Windows 10 devices still in use.
- Upgrade, replace, or enrol devices into Microsoft Extended Security Updates (ESU).
- Maintain evidence of ESU coverage for all in-scope devices.

---

6. BYOD (Bring Your Own Device) Requirements

- Identify all personal devices accessing organisational data.
- Ensure BYOD devices meet the same security standards as firm-owned devices.
- Enforce MFA, screen locks, supported OS versions, and patching.
- Update BYOD policies and user agreements.

---

7. Stricter Governance & Administrative Controls

- Maintain a register of all administrator accounts.
- Review admin access regularly and remove unused accounts.
- Document firewall rule approvals and configuration changes.
- Ensure governance processes are auditable and consistently applied.

---

8. Evidence & Documentation Readiness

- Ensure all policies reflect April 2026 requirements.
- Maintain logs, screenshots, and configuration evidence.
- Review incident response and access control documentation.
- Prepare a clear asset inventory covering devices, cloud services, and network equipment.

---

9. Pre-Renewal Internal Review

- Conduct an internal readiness check 4–6 weeks before renewal.
- Validate that all April 2026 changes are implemented.
- Address any gaps in patching, MFA, device support, or governance.

---

10. Final Preparation for Assessment

- Ensure all evidence is up to date and accessible.
- Confirm all staff understand any new requirements (e.g., MFA, BYOD rules).
- Review the full April 2026 question set to ensure alignment.

Summary

The April 2026 Cyber Essentials updates introduce more rigorous expectations across cloud services, authentication, patching, device support, and governance. For UK organisations, early preparation will ensure a smooth renewal and help maintain strong protection for client data and operational systems.

This checklist can be used internally or shared with your IT provider to support a structured, compliant renewal process.

Additional Support from JDI-UK Limited

Companies seeking assistance with their Cyber Essentials renewal process can get in touch with JDI-UK Limited. We offer a range of solutions tailored to help organisations navigate their renewal smoothly, from supporting customers to manage the renewal themselves, to providing a fully managed service including recertification, or a one-off managed renewal service. Whatever your needs, JDI-UK Limited can provide expert guidance and practical support to ensure compliance and ease the renewal journey.

W: https://jdi-uk.com/

T: 01138 715023

M: 07486 860990