**2025 Cyber Insurance Renewal Checklist**

*A Comprehensive Guide for UK Organisations*

**Developed by ProCheckUp** | **Based on 25+ Years of Cybersecurity Excellence**

**How to Use This Checklist**

This checklist has been designed to align with the latest UK cyber insurance underwriter requirements, incorporating the **UK Cyber Governance Code of Practice (April 2025)**, **Cyber Essentials** standards, and emerging regulatory requirements from the **Cyber Security and Resilience Bill**.

**Key Symbols:**

✅ Essential — Required by most underwriters

🔸 Recommended — Improves premium rates and coverage

📋 Document Required — Evidence must be provided

⚠️ Critical Gap — Common cause of renewal rejection

**Section 1: Multi-Factor Authentication (MFA) Evidence** ✅

**Basic MFA Requirements**

* FA enforced on all administrative accounts and privileged service accounts 📋
* MFA implemented for remote access to corporate networks 📋
* MFA active on cloud services (Office 365, Azure, AWS, etc.) 📋
* MFA enabled for privileged user accounts 📋
* MFA configured for backup, remote management, and third-party access systems 📋
* Ensure MFA exemptions reviewed quarterly and board-approved 🔸

**Evidence Documentation Required 📋**

* Screenshots of MFA configuration dashboards
* MFA enrollment reports showing coverage percentages
* Policy documents defining MFA requirements
* Exemption logs with risk assessments (if any exceptions exist)
* MFA bypass procedures documentation

**Advanced MFA Considerations** 🔸

* Conditional access policies configured based on risk
* Hardware security keys for high-privilege accounts
* MFA fatigue protection measures implemented
* Regular MFA effectiveness audits conducted

**Common Underwriter Questions:**

*"Provide evidence that MFA is enforced across all remote access points, including VPNs, cloud services, and administrative interfaces. Include screenshots of configuration settings and user enrollment statistics."*

**Section 2: Backup and Recovery Evidence** ✅

**Backup System Requirements**

* Automated backup systems operational 📋
* Air-gapped or immutable backups implemented ✅
* Geographic separation of backup locations 🔸
* Encrypted backups (at rest and in transit) ✅
* Regular backup integrity testing performed 📋

**Recovery Testing Documentation 📋**

* Monthly backup restore test logs
* Recovery time objective (RTO) test results
* Recovery point objective (RPO) validation records
* Full system restore exercise documentation
* Business-critical application recovery tests

**Evidence Package Required 📋**

* Backup success/failure logs (last 6 months)
* Restore test results with timestamps
* Recovery playbook documentation mapped to critical services and tested under FCA/NHS continuity standards
* Backup retention policy and compliance records
* Third-party backup provider security attestations

**Critical Backup Questions** ⚠️

*"Demonstrate that backups can be restored within your stated RTO. Provide logs showing successful monthly restore tests for critical systems. Include evidence that backups are protected from ransomware encryption."*

**Section 3: Incident Response and Tabletop Exercise Records** ✅

**Incident Response Plan Requirements**

* Written incident response plan exists 📋
* Plan updated within last 12 months ✅
* Clear roles and responsibilities defined 📋
* Escalation procedures documented 📋
* Legal and regulatory notification procedures included 📋

**Tabletop Exercise Documentation 📋**

* Tabletop exercises completed at least annually with insurer-aligned ransomware scenario testing ✅
* Exercise report with findings and improvements 📋
* Board or senior management participation recorded 🔸
* Post-exercise action plan implementation 📋
* External facilitator involvement (recommended) 🔸

**Required Tabletop Exercise Evidence 📋**

* Exercise scenario details and methodology
* Participant attendance records with job roles
* Timeline of response decisions during exercise
* Identified gaps and remediation plans
* Plan updates implemented post-exercise
* Board reporting on exercise outcomes

**Regulatory Alignment** 🔸

* Procedures align with upcoming Cyber Security and Resilience Bill
* NCSC reporting channels incorporated
* ICO notification procedures (72-hour requirement)
* Industry-specific reporting requirements addressed

**Sample Tabletop Exercise Documentation:**

*"Exercise Date: [Date], Scenario: Ransomware attack on critical systems, Participants: [List with roles], Key Findings: [Summary], Action Items: [List with owners and due dates], Board Briefing: [Date and attendees]"*

**Section 4: Vendor Due Diligence Essentials** ✅

**Vendor Risk Assessment Framework**

* Vendor risk classification system implemented 📋
* Due diligence questionnaires for critical vendors 📋
* Security attestations from key suppliers 📋
* Regular vendor security reviews scheduled 📋
* Vendor incident notification procedures established 📋

**Critical Vendor Documentation 📋**

* Vendor security attestations (SOC 2, ISO 27001, or Cyber Essentials Plus for UK SMEs)
* Cloud suppliers to evidence \*\*UK GDPR / Data Protection Act 2018\*\* compliance ✅
* Financial services vendors must show \*\*FCA/PRA compliance evidence\*\* 🔸
* Data processing agreements (DPAs) with security clauses
* Vendor business continuity plans and testing results
* Right-to-audit clauses in vendor contracts
* Vendor cybersecurity insurance verification

**Supply Chain Risk Management** 🔸

* Fourth-party (sub-vendor) risk assessment process
* Vendor security incident response coordination
* Regular vendor security posture monitoring
* Vendor offboarding security procedures
* Alternative vendor identification for critical services

**High-Risk Vendor Categories** ⚠️

* Cloud service providers
* Payment processors
* Data hosting providers
* Remote access solution vendors
* Software-as-a-Service (SaaS) platforms

**Evidence Requirements for Insurers 📋**

*"Provide vendor risk register including security ratings, due diligence documentation for top 10 critical vendors, and evidence of regular security reviews. Include contracts showing cybersecurity requirements and right-to-audit clauses."*

**Section 5: Board-Level Cyber Governance Requirements** ✅

*Aligned with UK Cyber Governance Code of Practice (April 2025)*

**Board Governance Structure**

* Designated board-level Senior Information Risk Owner (SIRO) or equivalent accountable for cyber security ✅
* Cyber security as standing agenda item (quarterly minimum) 📋
* Evidence of board training mapped to UK Cyber Governance Code of Practice (April 2025) 📋
* Proof of cyber risk integration into annual Companies Act 2006 Section 172 reporting 📋
* Board oversight explicitly tied to cyber insurance renewal conditions 📋

**Required Board Documentation 📋**

* Board meeting minutes showing cyber risk discussions
* Cyber security training certificates for board members
* Annual cyber risk assessment presented to board
* Board-approved cyber security strategy and budget
* Incident escalation procedures approved by board

**UK Cyber Governance Code Compliance** ✅

* **Risk Management**: Cyber risk ownership and appetite defined
* **Strategy**: Cyber strategy aligned with business objectives
* **People**: Cyber security culture and capabilities assessed
* **Incidents**: Response and recovery plans regularly tested
* **Assurance**: Regular cyber security reporting to board

**Board Reporting Metrics 📋**

* Cyber risk dashboard with key performance indicators
* Security incident trend analysis
* Vulnerability management statistics
* Security awareness training completion rates
* Third-party security assessment results

**Evidence Package for Insurers 📋**

*"Provide board meeting minutes demonstrating regular cyber risk oversight, training records for board members, and documented integration of cyber risk into enterprise risk management framework. Include evidence of board involvement in major cyber security decisions."*

**Section 6: External Attack Surface & Continuous Monitoring** 🔸

**Attack Surface Visibility**

* Comprehensive asset inventory (internet-facing systems) 📋
* Regular CHECK or CREST-accredited penetration tests 📋
* Quarterly CyberSnapshot or equivalent insurer-ready posture scans ✅
* Domain and subdomain monitoring 🔸
* Third-party security ratings monitoring 🔸

**Monitoring and Assessment Evidence 📋**

* Quarterly external vulnerability scan reports
* Penetration testing reports (annual minimum)
* Asset discovery scan results
* Remediation tracking for identified vulnerabilities
* Continuous monitoring service reports (if applicable)

**Section 7: Compliance and Certification Alignment** ✅

**Required Certifications and Standards**

* **Cyber Essentials Plus certification** (\*\*mandatory for UK Gov supply chain SMEs\*\*)✅
* **ISO 27001 certification** (expected baseline for enterprises; premium reductions apply)🔸
* **Alignment with UK Cyber Assessment Framework (CAF)** outcome statements📋
* Industry-specific compliance (PCI DSS, HIPAA, etc.) as applicable 📋

**Cyber Essentials Plus Requirements** ✅

* Firewalls configured and maintained (14-day patch window)
* Secure configuration of systems and software
* User access control with principle of least privilege
* Malware protection on all devices
* Security patch management (critical patches within 14 days)

**Documentation Required 📋**

* Current certification certificates
* Internal audit reports
* Compliance gap analysis and remediation plans
* Policy documents aligned with chosen frameworks

**Section 8: Quick Win Implementation Guide** 🔸

**30-Day Priority Actions**

1. **Document MFA deployment** - Screenshot current configuration
2. **Test backup restore** - Conduct \*\*insurer-witnessed or auditor-validated restore\*\* with logs
3. **Schedule tabletop exercise** - Book with board member participation
4. **Audit vendor list** - Identify and assess top 10 critical vendors, mapped against UK critical national infrastructure dependencies
5. **Board cyber training** - Enroll board members in NCSC training

**90-Day Strategic Actions**

1. **Obtain Cyber Essentials Plus** - Complete certification process
2. **Implement continuous monitoring** - Deploy external attack surface monitoring
3. **Enhance vendor contracts** - Add security clauses and audit rights
4. **Board governance integration** - Establish regular cyber risk reporting
5. **Incident response testing** - Conduct comprehensive tabletop exercise

**Section 9: Evidence Package Preparation 📋**

**Insurer Submission Format**

* Executive summary with key security achievements, explicitly referencing UK insurer questionnaires (WTW, Marsh, Aon, Hiscox models)
* Technical appendix with timestamped screenshots, audit logs, and board minutes cross-referenced
* Board governance documentation package
* Vendor risk management portfolio
* Incident response and testing records

**Common Documentation Gaps** ⚠️

* Screenshots without timestamps or context
* Policies without evidence of implementation
* Outdated assessments (over 12 months old)
* Missing board oversight documentation
* Incomplete vendor due diligence records

**Section 10: Sector-Specific Considerations**

**Financial Services**

* PCI DSS compliance (SAQ-D / ROC as applicable) with **QSA attestation**
* Additional MFA for trading platforms
* Enhanced vendor due diligence for fintech partners
* FCA-mandated operational resilience reporting alignment ✅
* Cloud services evidencing PRA/FCA Third-Party Outsourcing Policy compliance

**Healthcare**

* NHS DSPT evidence pack ✅
* CQC cyber safety compliance mapped to patient safety
* Proof of medical device patching cycles aligned to MHRA guidance
* Care Quality Commission cyber security requirements

**Local Government**

* PSN Code of Connection or equivalent compliance evidence
* NCSC GovAssure external assessment results (if available)
* Citizen data protection measures
* Supply chain security for public services
* Emergency response coordination procedures

**Manufacturing**

* IEC 62443 alignment for OT/ICS environments
* Industrial control system protection
* Demonstrated business continuity resilience against supply chain disruption ✅
* Business continuity for manufacturing operations

**Action Checklist Summary**

**Essential Documentation Package 📋**

* MFA evidence with screenshots and policies
* Backup testing logs and recovery procedures
* Tabletop exercise report with board participation
* Vendor due diligence documentation for critical suppliers
* Board meeting minutes showing cyber governance oversight

**Certification Requirements** ✅

* Cyber Essentials Basic (minimum for SMEs)
* ISO 27001 (preferred for large enterprises)
* Industry-specific certifications as applicable PCI ASV/QSA

**Regulatory Alignment** 🔸

* UK Cyber Essentials
* UK GDPR
* NCSC Pentenst/Check Greenlight
* Data protection and privacy compliance

**ProCheckUp Support Services**

**Need help implementing this checklist?** ProCheckUp offers comprehensive support to help UK organisations meet cyber insurance requirements:

* **CyberSnapshot Rapid Assessments** - 48-hour external posture reviews
* **CyberEssentials Plus** - minimum for SMEs selling to UK government
* **Board Governance Support** - Compliance with PCI QSA/ASV, ISO27001
* **Tabletop Exercise Facilitation** - Expert-led incident response testing
* **ASV scans/CyberSnapshot** - Ongoing security posture validation

**Contact ProCheckUp:**

* 📞 **Phone**: 020 7612 7777
* 📧 **Email**: [sales@procheckup.com](mailto:sales@procheckup.com)
* 🌐 **Web**: www.procheckup.com

*This checklist is based on ProCheckUp's 25+ years of cybersecurity experience and current UK cyber insurance market requirements as of September 2025. Requirements may vary by insurer and should be verified with your specific insurance provider.*

**Version**: 2025.1 | **Last Updated**: September 2025 | **Next Review**: January 2026