GP IT Services
POWERED BY IT AUXILIUM
SUPPORTING YOU AND YOUR PATIENTS

HEALTH IT Services
POWERED BY IT AUXILIUM
SUPPORTING YOU AND YOUR PATIENTS

CYBER ESSENTIALS AND CYBER ESSENTIALS PLUS CONSULTANCY & AUDIT

Service Overview

The Cyber Essentials and Cyber Essentials **Plus** Consultancy & Audit service provides structured, end-to-end support to help organisations achieve and maintain certification under the UK Government–backed Cyber Essentials scheme, including Cyber Essentials Plus.

The service is designed to reduce certification risk, simplify technical and administrative requirements and provide assurance that controls are implemented in line with National Cyber Security Centre (NCSC) guidance.

Our approach combines technical consultancy, remediation guidance and audit readiness support, enabling organisations to improve their cyber security posture while achieving recognised certification.

Service Objectives

The objectives of this service are to:

- Support successful Cyber Essentials and Cyber Essentials Plus certification
- Reduce the risk of certification failure or delays
- Improve baseline cyber security controls
- Align organisational security practices with NCSC guidance
- Provide clear evidence and audit readiness
- Support ongoing compliance and re-certification

01223 827 410

hello@healthitservices.co.uk | healthitservices.co.uk
hello@gpitservices.co.uk | gpitservices.co.uk

Intended Customers

This service is suitable for:

- Public sector organisations
- NHS and health and care organisations
- Small and medium-sized enterprises
- Third sector organisations
- Suppliers required to meet Cyber Essentials as part of contractual obligations

The service is scalable and can be tailored to organisations of varying size, complexity and technical maturity.

Scope of Service

The Cyber Essentials Consultancy & Audit service supports both initial certification and annual re-certification and may be delivered as a one-off engagement or as part of an ongoing managed security service.

The scope include:

- Cyber Essentials readiness assessment
- Gap analysis against the five Cyber Essentials control areas
- Remediation planning and advisory support
- Assistance with self-assessment submission
- Cyber Essentials Plus audit preparation and coordination
- Post-certification improvement planning

Detailed Service Activities

Discovery and Scoping

- Initial discovery call to understand organisation size, sector and technical environment
- Confirmation of certification target: Cyber Essentials or Cyber Essentials Plus
- Identification of key stakeholders and systems in scope
- Agreement of scope, timelines and responsibilities

Readiness Assessment

- Review of current security controls and configurations
- Assessment against the five Cyber Essentials control areas:
    - o Firewalls and internet gateways
    - o Secure configuration
    - o User access control
    - o Malware protection
    - o Patch management
- Identification of gaps and non-conformities

Gap Analysis and Risk Prioritisation

- Detailed gap analysis mapped to Cyber Essentials requirements
- Risk-based prioritisation of remediation actions
- Clear identification of mandatory versus recommended controls

Remediation Support

- Practical guidance to address identified gaps
- Configuration advice aligned with NCSC best practice
- Support developing policies and procedural controls where required
- Clarification of evidence requirements

Cyber Essentials Plus Audit Preparation

- Technical preparation for independent assessment
- Support coordinating the Cyber Essentials Plus audit
- Validation of system configurations and evidence
- Remediation guidance for any pre-audit findings

Self-Assessment Submission Support

- Assistance completing the Cyber Essentials self-assessment questionnaire
- Review of responses for accuracy and consistency
- Pre-submission validation to reduce risk of rejection

Post-Certification and Ongoing Support

- Review of certification outcomes
- Recommendations for continuous improvement
- Support planning for annual re-certification

Key Features

The service delivers end-to-end consultancy and audit readiness support for both Cyber Essentials and Cyber Essentials Plus. It combines structured readiness assessments with practical, risk-based remediation guidance aligned to National Cyber Security Centre best practice. Rather than focusing solely on certification, the service helps organisations implement sustainable baseline security controls that can be evidenced confidently during assessment.

Support includes validation of technical configurations, clarification of scheme requirements and guided completion of the Cyber Essentials self-assessment. For Cyber Essentials Plus, the service provides targeted preparation for the independent technical audit, ensuring systems, policies and evidence are aligned ahead of assessment and reducing the risk of failure or rework.

Benefits

By providing clear structure and expert oversight, the service significantly increases the likelihood of successful certification at the first attempt. Organisations benefit from reduced uncertainty around technical requirements, improved confidence in audit readiness and a clearer understanding of where security controls need to be strengthened.

Beyond certification, the service helps establish a stronger cyber security baseline, improving protection against common threats and enhancing assurance for customers, partners and regulators. The outcome is not only compliance with the Cyber Essentials scheme but a more resilient and well-governed security posture.

Support Levels

Support is available at different levels to reflect organisational size, complexity and risk appetite.

Standard Support is delivered remotely during UK business hours and includes consultancy, evidence guidance and submission support. This is typically provided as a fixed price engagement based on organisation size and DSPT level. Enhanced Support offers accelerated delivery, extended availability and additional assurance for complex environments. Pricing is agreed based on scope and timelines. All engagements include a named technical consultant acting as a technical account manager, providing continuity, specialist guidance and oversight throughout the service.

Pricing Model

Pricing is based on:

- Organisation size and number of users
- Complexity of the technical environment
- Certification level required
- One-off or recurring engagement

Pricing is provided as a fixed project cost or fixed annual fee, ensuring transparency and cost predictability. All pricing is agreed prior to service commencement.

Security and Compliance

The service aligns with:

- NCSC Cyber Essentials scheme requirements
- NCSC Cyber Security Guidance
- UK GDPR and Data Protection Act 2018 where applicable
- Government supply chain security expectations

All customer information is handled securely and confidentially.

Onboarding and Offboarding

Onboarding

- Formal service initiation
- Confirmation of scope and systems in scope
- Delivery plan and timeline agreement

Offboarding

- Handover of findings and recommendations
- Certification evidence summary
- Optional transition to managed compliance

Service Availability

- UK-wide remote service delivery
- Business hours support as standard
- Enhanced availability by prior agreement

Service Outcomes

- Successful Cyber Essentials or Cyber Essentials Plus certification
- Improved cyber security baseline
- Clear evidence and audit trail
- Defined improvement roadmap

Contact and Escalation

Customers are provided with clear contact details, named resources and escalation routes at service commencement to ensure effective support throughout the engagement.

Service Constraints and Dependencies

- Customers retain responsibility for implementing agreed remediation actions
- Timely access to systems and documentation is required
- Certain technical remediation may fall outside the scope of consultancy services
- Certification bodies operate independently for Cyber Essentials Plus audits

About Us

IT Auxilium Ltd is a UK technology services provider delivering secure, dependable IT solutions where reliability is critical.

Healthcare is a core specialism. Through our dedicated divisions, GP IT Services and Health IT Services, we support General Practices, Primary Care Networks and independent healthcare providers with IT designed for clinical environments and aligned to NHS frameworks and UK security standards.

Beyond healthcare, IT Auxilium applies the same disciplined, security-led approach to all businesses we support. From managed IT and cybersecurity to cloud services and digital transformation, we provide proactive monitoring, clear accountability and responsive UK-based support, acting as a trusted extension of our customers' teams.

Health IT Services & GP IT Services are trading names of IT Auxilium Ltd.

Additional Support Services

NHS Data Security and Protection Toolkit (DSPT) Support
Our NHS Data Security and Protection Toolkit (DSPT) Support service provides structured guidance to achieve and maintain compliance. We assess readiness, address gaps, prepare evidence and support submissions, ensuring alignment with NHS requirements while reducing risk and administrative burden.

Artificial Intelligence (AI) Readiness Assessment and Advisory Service
Our Artificial Intelligence Readiness Assessment and Advisory Service helps organisations evaluate capability, risk and governance before adopting AI. We assess data maturity, security and compliance, providing clear recommendations to enable responsible, safe and value-driven AI adoption.

IT Managed Service Provider
Our Managed IT Service offering delivers proactive, fully supported IT management. We provide 24/7 monitoring, security, patching and responsive UK-based support, ensuring systems remain secure, reliable and optimised while you focus on your core operations.

Microsoft 365 Migration & Onboarding
Our Microsoft 365 Migration and Onboarding service ensures a smooth, secure transition with minimal disruption. We plan, migrate and configure your environment, apply security best practice and support user adoption, enabling organisations to realise value quickly and confidently.

Backup & Disaster Recovery
Our Backup and Disaster Recovery services provide comprehensive protection across endpoints, Entra ID, Microsoft Azure, Microsoft 365 and Google Workspace. We deliver secure, automated and monitored backups with clearly defined recovery options, helping organisations restore systems and data quickly following cyber incidents, accidental deletion or service disruption. Our approach is designed to support business continuity, regulatory expectations and operational resilience, ensuring critical data remains protected, accessible and recoverable when it matters most.

Medical-Grade Cloud Based Temperature/Environmental Monitoring Data Logger System
Our medical-grade, cloud-based temperature and environmental monitoring service provides continuous automated monitoring, real-time alerts and auditable records for regulated environments. It replaces manual checks, reduces risk and supports compliance, inspections and operational assurance across single or multi-site estates.