ALVAO

Empowering UK organizations with Cyber Essentials compliance

Cyber Essentials is a UK government-backed cybersecurity certification, governed by the NCSC (National Cyber Security Centre), the United Kingdom's official authority for cyber security, operating as part of GCHQ (Government Communications Headquarters) who define the baseline of technical defenses—firewalls, secure configurations, access controls, malware protection and patch management—capable of shielding organizations from around 80% of common Internet-borne cyber threats.

Index

1. Cyber Essentials and its importance for UK Businesses

Why is it important?

Regulatory and purchasing requirement

It is a procurement prerequisite for government contracts involving personal or sensitive data. Certification is mandatory for suppliers bidding on many UK government contracts, especially those handling sensitive or personal data.

Insurance and market confidence

Build stakeholder trust by demonstrating visible commitment to cyber hygiene. Certification may lead to reduced cyber insurance premiums and serves as a visible declaration to stakeholders that the organization takes cyber security seriously.

Risk reduction

It supports insurance credibility, often lowering cyber premiums for certified entities. By implementing the five core controls, organizations significantly reduce their exposure to common, commoditized threats.

Who should comply?

Any UK organization seeking contracts with government bodies and/or public sector, handling personal data and contracts, or wishing to strengthen basic cyber defenses should prioritize Cyber Essentials certification.

2. Understanding Cyber Essentials and Cyber Essentials Plus

A. Cyber Essentials (Base level)

The base level involves a self-assessment process covering the five key technical controls. Submissions are reviewed by accredited certification bodies to verify accuracy and adherence.

- **Self-assessment process with five technical controls:**
  - Boundary firewalls
  - Secure configurations
  - User access control
  - Malware protection
  - Patch management
- **An independent review by an accredited certification body.**
- **Certification lasts for 12 months and must be renewed annually.**

B. Cyber Essentials Plus (Enhanced level)

Cyber Essentials Plus includes all the requirements of the base level but adds an independent technical audit. This includes external and internal vulnerability scans, malware detection testing, verification of secure configurations, and mandatory multi-factor authentication for cloud services. Pass criteria are stricter, and remediation is required within 30 days.

- **Includes everything from Cyber Essentials, plus an independent technical audit.**
- **The audit includes external and internal vulnerability scans, malware protection checks, and verification of MFA on cloud services.**
- **Companies must hold the Cyber Essentials certification first;** Cyber Essentials Plus must be pursued within three months of gaining the Cyber Essentials certification.
- **Stricter pass criteria: remediation must occur within 30 days.**

3. Benefits comparison

FEATURE	CYBER ESSENTIALS	CYBER ESSENTIALS PLUS
Self-assessment questionnaire	✓ Yes	✓ Yes +independent validation
External vulnerability scan	✓ Yes	✓ Yes
Internal device audits	✓ No	✓ Yes
Malware protection testing	✗ No	✓ Yes
Cloud service MFA verification	✗ Not enforced	✓ Yes
Assurance level	Basic	Higher – technical audit verifies actual implementation
Typical cost (SME)	£300–£600 + VAT	£1,500–£2,500 + VAT

4. How ALVAO supports compliance with Cyber Essentials (Plus)

4.1 Asset and software inventory

Keeping an accurate and up-to-date inventory of IT assets is fundamental to Cyber Essentials. Organizations must demonstrate that all hardware and software are supported, regularly updated, and patched against known vulnerabilities.

ALVAO IT Asset Management (ITAM) provides a single source of truth for all devices and applications in the environment. Assets are automatically discovered and recorded in the CMDB, along with details such as version numbers, configurations, and licensing status. When software or firmware is out of date, ALVAO generates alerts and links them to Service Desk workflows, ensuring patching is prioritized and tracked through to completion. This creates a clear, auditable process that satisfies Cyber Essentials' patch-management control and helps prevent security gaps caused by unmanaged assets.

4.2 CMDB risk and threat management

ALVAO's Configuration Management Database (CMDB) goes beyond simple asset tracking by enabling organizations to manage risks in context. Each risk can be directly linked to primary and secondary items, providing clear visibility of dependencies and potential cascading impacts across the infrastructure.

The CMDB also calculates an automatic security score for assets and services, highlighting the most vulnerable or high-risk areas. This prioritization helps IT teams focus resources where they will have the greatest impact in reducing risk.

For Cyber Essentials compliance, this capability ensures that vulnerabilities are not only recorded but also quantified, linked to real business assets, and addressed in a structured, evidence-driven way, strengthening both the certification process and overall operational resilience.

4.3 Real-time alerts & application control

Cyber Essentials requires organizations to use effective malware protection and ensure only approved applications are allowed to run. ALVAO supports this by enabling administrators to create allowlists and denylists of software.

Through its ITAM data, ALVAO shows exactly which applications are installed on which devices. If unapproved or potentially malicious software is detected, ALVAO triggers alerts and automatically raises Service Desk tickets to investigate and resolve the issue.

This means organizations can prove to auditors that they have an ongoing process to manage malware protection and application control across their estate.

4.4 Access control & secure configuration

Limiting user access and securing system configurations are critical Cyber Essentials requirements. ALVAO helps by combining asset visibility with role-based permissions.

Access rights can be linked to specific devices, applications, or services in the CMDB. Workflows ensure that when staff join, move roles, or leave,

access is provisioned or revoked in a consistent and auditable way. ALVAO also ensures that departing employees return all equipment, thereby reducing the security risks associated with data leaks.

In addition, secure configuration standards can be documented within ALVAO and checked against assets, allowing IT teams to demonstrate that systems are not running with unnecessary services, default settings, or open ports—all key points under the Cyber Essentials scheme.

4.5 Incident management and governance

Cyber Essentials Plus requires clear evidence of how organizations identify, record, and resolve security incidents. ALVAO's integrated approach, with ITAM-backed data and AI-enhanced ITSM workflows, helps organizations meet and exceed these expectations with efficiency and precision.

- **Structured incident capture:** ALVAO's Service Desk centralizes all security-relevant requests and incidents, linking them to relevant assets in the CMDB and applying predefined workflows to enforce escalation and resolution procedures.
- **End-to-end audit trails:** Every ticket, from detection through inference to closure, is auditable. Timestamped logs demonstrate consistent governance, which is essential for Cyber Essentials auditing.
- **AI-powered major incident detection:** ALVAO's AI Assistant, powered by Azure OpenAI, provides real-time support in the ticket interface—summarizing communications, surfacing similar historical tickets, and offering proposed solutions. Crucially, it calculates a major incident score for each ticket using service-level and asset-linked scoring metadata, raising awareness automatically when critical issues arise.
- **Improved awareness and response speed:** By flagging high-scoring tickets as potential major incidents, ALVAO ensures key personnel are alerted rapidly. Agents receive AI-generated recommendations, enabling faster root cause analysis and consistent resolution workflows, streamlining incident management for audit readiness.

This combination of AI, asset-aware service design, and robust ITSM workflows ensures that organizations can demonstrate not only incident handling, but proactive detection, structured response and continual governance, precisely aligning with Cyber Essentials Plus standards.

4.6 Built-in compliance credentials of ALVAO

ALVAO runs on Microsoft Azure, inheriting world-class security controls and compliance standards such as ISO 27001 and SOC 2. It is also listed on the UK G-Cloud framework, meaning it has already passed stringent government security assessments.

For organizations pursuing Cyber Essentials certification, using ALVAO provides assurance that the underlying ITSM/ITAM platform itself meets recognized security benchmarks. This not only supports compliance efforts but also reassures auditors, partners, and customers that ALVAO is a trusted, secure foundation for IT operations.

5. Getting started: ALVAO as a Cyber Essentials partner

ALVAO simplifies certification by embedding compliance directly into daily IT operations:

1

Deploy ALVAO modules for Asset Management and Service Desk.

2

Define asset inventories, software management alerts, and secure configuration policies.

3

Implement access controls and approval workflows with full audit logging.

4

Enable application allowlisting and alerts on attempts to run malware.

5

Conduct readiness checks using ALVAO Power BI integrated dashboards and reports.

6

Maintain evidence for base and Plus audits with minimal manual effort.

7

Streamline annual recertification by leveraging automated processes.

6. Conclusion

Cyber Essentials is vital for UK organizations looking to manage government requirements which meet common cyber security risks. Cyber Essentials Plus adds technical audits for deeper assurance, validating the implementation of security measures and ensuring customer and government trust in a company's compliance.

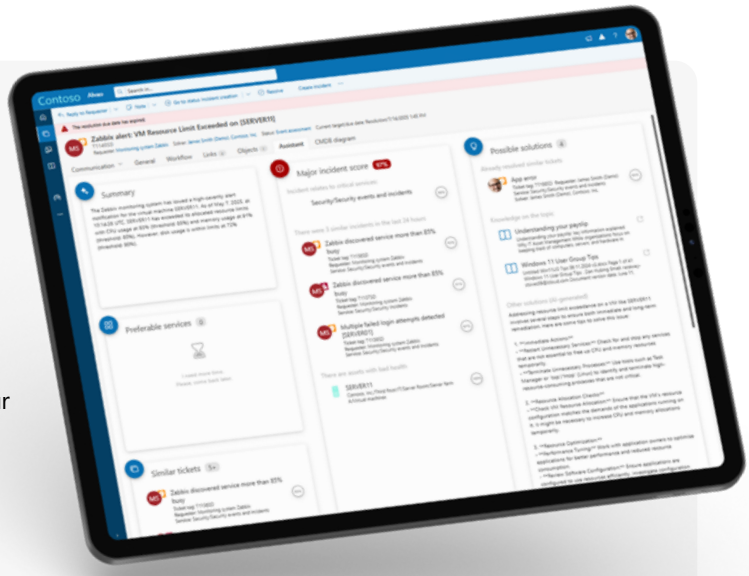
ALVAO's ITSM and ITAM platform supports asset tracking, patch management, incident handling, and access governance into a single platform. This ensures audit-ready, continuous compliance, turning Cyber Essentials certification into a natural by-product of robust IT operations while boosting long-term cyber resilience and operational efficiency.

Book a free ALVAO demo

What to expect:

- A personalized, interactive demo built around your needs.
- See how the solutions scale and sync with your tools and workflows.
- Answers to all your questions from our ITSM expert.

Request a demo at
alvao.com/en/demo



ALVAO

www.alvao.com