



Service Definition Document

Assisted Cyber
Essentials Certification

Contents

Solution Overview.....	2
What is Assisted Cyber Essentials Certification?	2
Key Features.....	2
Key Benefits.....	2
Scope	3
What is in Scope?	3
What is Out of Scope?	4
Data Protection & GDPR.....	4
Why Partner with Atech?	5
Credentials and Capability	5
Microsoft Endorsements and Specialisations	5
Security and Compliance	6

Solution Overview

What is Assisted Cyber Essentials Certification?

A guided, end-to-end service helping organisations prepare for, complete and achieve **Cyber Essentials** certification, the UK Government-backed baseline cyber security standard. We provide readiness assessment, practical remediation support, assisted completion of the IASME self-assessment, and submission support through to certificate issuance.

Key Features

- Gap analysis against Cyber Essentials and CE+ requirements
- Vulnerability scanning and detailed compliance reporting
- Review of firewalls, servers, and workstation configurations
- Secure configuration and patch management assessment
- Malware protection and user access control verification
- Coordination with accredited Cyber Essentials assessor
- Assistance with evidence submission for certification
- Pre-assessment for Cyber Essentials Plus readiness
- End-user environment testing for CE+ certification
- Electronic certification and official Cyber Essentials logos

Key Benefits

- Achieve Cyber Essentials or Cyber Essentials Plus certification
- Compliance with UK government and NCSC cybersecurity standards
- Reduced risk from common cyber threats and vulnerabilities
- Eligibility for government contracts and regulated industry work
- Improved organisational security posture and resilience
- Increased trust with clients, partners, and stakeholders
- Clear remediation roadmap for non-compliant systems
- Verified protection against phishing, ransomware, and malware attacks
- Simplified certification process through expert guidance and coordination
- Strong foundation for future cybersecurity improvements

Scope

What is in Scope?

Cyber Essentials Gap Analysis

- Review of the workstations, servers and firewalls to identify their current configuration.
- Review of the primary Identity Provider (eg. Active Directory/Entra ID) to identify their current configuration for standard users and administrators.
- Review of Cloud services and environments to identify their current configuration.
- Deployment of a Nessus Vulnerability scanner on the client network
- Running vulnerability scan, targeted at workstations and scanners
- Export of detailed vulnerability reports from these scans.
- Collation data from information gathering and vulnerability scans.
- Comparison of the current state to the current Cyber Essentials & Cyber Essentials Plus specifications.
- Creation of detailed report detailing alignment of the current state of the environment with the certification specification.
- Detail improvement actions for non-compliant areas of the environment, to improve these to the required target state.

Cyber Essentials Certification

- Cyber Essentials (CE) pre-assessment to review customer's current situation. Assets for assessment will be identified.
- Working with CE partner to apply for the certification.
- Working through CE questions and assisting evidence for each.
- 1x resubmit, if necessary.
- Electronic certificate provided by CE assessor with CE logos.

Cyber Essentials Plus Certification

- Cyber Essentials Plus (CE+) pre-assessment to review customer's current situation.
- Assets for assessment will be identified.
- Deployment of vulnerability scanner for pre-assessment scan to identify issues in the network.
- Provide advise on how to remediate devices or processes that do not comply with CE+ (remediation to be scoped and priced separately).
- Working with CE+ partner to apply for the certification.
- Deployment of assessor's vulnerability scanner to endpoints for CE+ assessment.
- Coordination of end user environment testing on assessment day.
- Electronic certificate provided by CE assessor with CE+ logos.

What is Out of Scope?

Cyber Essentials Gap Analysis

- Actions to remediate non-compliant areas of the customer environment.
 - Reassessment of the customer environment after remediation actions take place.
 - Completion of or assistance with completion of the CyberEssentials questionnaire for submission to IASME.
 - Assistance with completion of Cyber Essentials Plus certification.
- Gap Analysis or recommendation of remediation actions for other certifications or standards that are not Cyber Essentials & Cyber Essentials Plus.

Data Protection & GDPR

Atech, part of the Iomart Group, is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. Our Data Protection policy sets forth the expected behaviours of Iomart Employees and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to an Iomart Contact (i.e. the Data Subject). Iomart, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in our Data Protection policy (available on request).

Iomart's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all Iomart Employees and Third Parties to share in this commitment.

Iomart uses the Personal Data of its Contacts for the following broad purposes:

- The general running and business administration of Iomart Entities.
- To provide services to Iomart customers.
- The ongoing administration and management of customer services.
- The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object.

Each Iomart Entity will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Iomart will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or to take steps at the request of the Data Subject prior to entering a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party.

Why Partner with Atech?

Credentials and Capability

Atech is the one of the UK's most accredited providers of secure hybrid cloud managed services, delivering deep expertise across Microsoft technologies, data protection, and cybersecurity. We hold Microsoft designations for **Modern Work, Security, Infrastructure (Azure)** and are recognised as an **Azure Expert MSP** – a status achieved by only 60 partners globally and 15 in the UK.

As part of the Microsoft AI Cloud Partner Program, we have validated technical capabilities across the full cloud lifecycle. Our inclusion in the **Azure Expert MSP Program** reflects proven excellence in people, processes, and tools, ensuring sustainable, repeatable, and scalable managed services. This means you can rely on a partner that consistently delivers best practice and operational efficiency.

Partnering with us gives you access to over **200 Microsoft cloud specialists**, including **two Microsoft MVPs**, ensuring unparalleled technical depth and experience.

Microsoft Endorsements and Specialisations

We hold multiple Microsoft Solutions Partner designations, including:

- Digital & App Innovation (Azure)
- Data & AI (Azure)
- Business Applications



Figure 1: Microsoft Accreditations

In addition, we have achieved advanced specialisations in areas such as:

- Cloud Security
- Identity and Access Management
- Threat Protection
- Infra & Database Migration
- Azure Virtual Desktop
- Enterprise Application Migration to Azure



Figure 2: Microsoft Designations

These credentials validate our ability to deliver complex, secure, and innovative solutions aligned to Microsoft best practices.

Security and Compliance

Security is at the heart of our services. Atech is **ISO 27001 certified**, **Cyber Essentials Plus accredited**, and a member of the **Microsoft Intelligent Security Association (MISA)** – an invitation-only program granting access to Microsoft's top security experts. We also hold **CREST accreditation** and participate in the **Microsoft MSSP Program**, one of only 12 partners in the UK, giving our customers direct benefits such as access to product teams and funded workshops.

Further reinforcing our security leadership:

- **Microsoft Gold Partner Status** alongside **Azure Expert MSP**
- **Microsoft MSSP Program** (1 of only 12 UK partners)
- **Microsoft Fastrack Ready Partner** (1 of only 300 globally)
- **Microsoft XDR status**

These credentials provide you with assurance that security is embedded throughout design, migration, and ongoing management. Combined with our advanced specialisations and industry recognition, they demonstrate our ability to deliver secure, compliant, and future-ready solutions.

ATECH IOMART

6 Atlantic Quay, 55 Robertson Street, Glasgow, G2 8JD