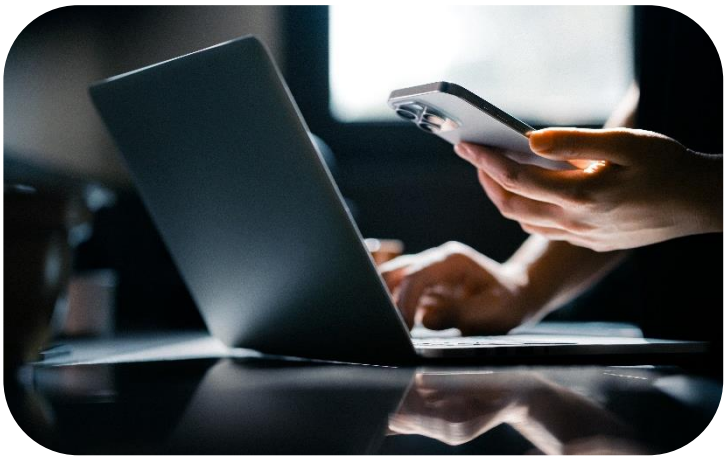
Cyber Security Certifications for Organisations

This Loss Prevention Standard discusses the benefits of cyber security certifications in helping to demonstrate effective cyber security controls, reduce exposure to common threats including those presented by suppliers and customers.

Version: 1.0
Date: 23rd July 2026

Cyber Security Certifications for Organisations

Introduction



Cyber security certifications provide an independent means for organisations to demonstrate that appropriate controls are in place to protect systems, information and services. They help reduce exposure to common cyber threats, improve customer confidence and support compliance with procurement and supply chain requirements.

Cyber Essentials, Cyber Essentials Plus and IASME Cyber Assurance are related organisational certification schemes, each serving a different purpose. Cyber Essentials establishes a baseline level of technical cyber security controls. Cyber Essentials Plus provides independent verification of those controls through technical assessment and testing. IASME Cyber Assurance extends beyond technical controls by assessing how cyber security is governed, managed and embedded across the organisation.

Certification provides assurance that an organisation has met the applicable requirements at the time of assessment. It does not guarantee that the organisation cannot experience a cyber-attack and it does not by itself establish compliance with every legal, regulatory or contractual obligation.

Because requirements and assessment processes are updated periodically, organisations should check the current NCSC and IASME guidance before beginning an application or technical audit.

Cyber Essentials

Cyber Essentials is a UK government-backed certification scheme designed to protect organisations against common internet-based attacks. It is suitable for organisations of all sizes and is widely recognised across the public and private sectors. The National Cyber Security Centre (NCSC) describes Cyber Essentials as the minimum cyber security standard it recommends for organisations of all sizes.[1]

The scheme focuses on five technical control areas:

- Firewalls,
- Secure Configuration,
- User Access Control,
- Malware Protection, and
- Security Update Management.

[1] https://www.ncsc.gov.uk/cyberessentials/overview

These controls apply to relevant computers, servers, mobile devices, network equipment, cloud services and software used by the organisation. The organisation must clearly define the scope of its assessment and ensure that all relevant systems and services within that scope meet the requirements.

The scope should normally cover the whole of the IT infrastructure used to conduct the organisation's business. Where necessary, an organisation may certify a well-defined and separately managed subset, but the scope boundary must be agreed with the Certification Body before the assessment begins. Any exclusion must be clearly identified and justified. Cloud services that store or process organisational data, or provide organisational services, cannot be excluded from scope. Personal or bring-your-own devices that access organisational data or services will also normally be in scope, subject to the specific exceptions set out in the scheme requirements.

The Cyber Essentials requirements are reviewed periodically. Organisations should therefore use the current requirements and question set applicable on the date their assessment is started. The current technical requirements, version 3.3, became effective on 27th April 2026. Assessment accounts created before that date may continue to use version 3.2, subject to the applicable completion period.

What Does the Assessment Involve?

Certification is based on a verified self-assessment. The organisation completes an online questionnaire explaining how it meets the Cyber Essentials requirements. A senior representative must confirm that the answers are accurate, after which an accredited assessor reviews the submission.

The assessment is concerned with the organisation's actual technical arrangements, not simply whether policies exist. Answers should therefore accurately describe the devices, software, cloud services, user accounts and security configurations in use.

The organisation has six months from the creation of its assessment account to complete and submit the assessment. If it does not complete the assessment within that period, it may need to reapply and pay a further assessment fee.

If the assessment is successful, the organisation receives a Cyber Essentials certificate and may use the certification badge. Certification is normally valid for 12 months and must be renewed annually.

Cyber Essentials Plus

Cyber Essentials Plus uses the same technical requirements as Cyber Essentials but provides a higher level of assurance. Instead of relying only on the organisation's answers to the self-assessment questionnaire, an accredited assessor performs independent technical testing to verify that the controls have been implemented correctly.

The organisation must complete the Cyber Essentials verified self-assessment as part of the Cyber Essentials Plus process. Where Cyber Essentials was achieved less than three months before Cyber Essentials Plus certification, the organisation will not need to repeat the self-assessment questionnaire.

The Cyber Essentials Plus audit must be completed within three months of the organisation's most recent Cyber Essentials certification.

The answers in the verified self-assessment must be complete and final before Cyber Essentials Plus testing begins and cannot subsequently be changed in response to issues identified during the technical audit.

What Does the Assessment Involve?

The assessor tests systems that are within the agreed Cyber Essentials scope. This includes a representative sample of user devices, together with relevant internet gateways and servers that provide services to unauthenticated internet users. The sample of user devices is selected by the assessor and will typically represent approximately 10% of the relevant devices, although further testing may be required.

The assessment may be performed remotely or in person, depending on the organisation and its technical environment. It normally includes internal and external vulnerability scanning, together with the aforementioned checks performed on selected systems and user devices.

Testing normally examines whether:

- Software is supported and appropriately patched,
- Automatic updates are enabled where possible,
- Security updates and vulnerability fixes are installed within 14 days of release where the vendor identifies the vulnerability as critical or high risk, where it has a CVSS version 3 base score of 7 or above, or where the vendor does not provide severity information,
- Firewalls and externally accessible services are securely configured,
- Malware protection is operating effectively,
- Separate administrative accounts are used only for administrative activities and are not used for ordinary activities such as email or web browsing,
- Standard users are prevented from performing administrative activities,
- Multi-factor authentication is used where required, including for authentication to cloud services,
- Known vulnerabilities have been removed, mitigated or otherwise addressed in accordance with the scheme requirements, and
- The technical controls described in the self-assessment are operating consistently across the assessment scope.

Any failures must be corrected before certification can be awarded. Remediation should be applied across the relevant assessment scope and not only to the individual devices selected for testing. This makes Cyber Essentials Plus more demanding than the standard Cyber Essentials assessment.

Cyber Essentials Plus certification is valid for 12 months and must be renewed annually.

IASME Cyber Assurance

IASME Cyber Assurance is a broader cyber security and information assurance standard. It builds on Cyber Essentials but also considers organisational governance, policies, people, processes and business resilience.

It is designed to be accessible to organisations of different sizes and can provide a proportionate alternative to, or a possible preparatory step towards, a more complex information security management standard such as ISO 27001.

A valid Cyber Essentials certificate is required before IASME Cyber Assurance certification can be obtained. For a UK organisation, the Cyber Essentials certificate must have at least one month remaining before its expiry when IASME Cyber Assurance is applied for. Organisations outside the UK should contact IASME to confirm the applicable prerequisite arrangements.

What Does the Assessment Involve?

IASME Cyber Assurance considers subjects such as:

- Cyber security roles and responsibilities.
- Risk management.
- Information and physical asset management.
- Staff awareness and training.
- Technical security controls.
- Incident management.
- Backup and restoration arrangements.
- Business continuity.
- Data protection and regulatory requirements.
- Physical security.
- Supplier and service-provider management.

The depth of the applicable requirements are adjusted according to the size of the organisation. This is intended to ensure that smaller organisations are not expected to implement unnecessarily complex arrangements while still meeting the objectives of the standard.

IASME Cyber Assurance operates at two levels:

- **Level One - Verified Assessment** requires the organisation to complete a detailed online assessment. A senior representative confirms the answers, and an independent assessor reviews the submission.
- **Level Two - Audited** involves a more detailed audit of the organisation's policies, processes and evidence. The auditor may review documentation, interview staff and examine how controls operate in practice.

Level One must be achieved before an organisation can proceed to Level Two. Level Two must normally be completed within six months of the Level One assessment. The security requirements are fundamentally the same at both levels; the distinction is that Level Two provides greater assurance through independent examination of how the controls have been implemented in practice.

Evidence for IASME Cyber Assurance may include:

- Information security policies.
- Risk assessments and security improvement plans.
- Information and physical asset registers.
- Staff training and awareness records.
- Supplier assessments.
- Administrative access records and access reviews.
- Backup and restoration tests.
- Security incident records.
- Business continuity plans and exercise records.
- Change-management records.
- Evidence of management review and oversight.

Documentation should reflect the organisation's actual working practices rather than consisting solely of generic policy templates. Assessors will generally expect the organisation to demonstrate that documented controls are understood, consistently followed and supported by appropriate records.

During a Level Two audit, the assessor may test a sample of records or activities to establish whether stated policies and procedures are consistently followed. Interviews may include senior management, IT personnel, information owners, operational staff and other individuals with security responsibilities. The audit may be performed in person or, where appropriate, remotely.

Certification Validity and Renewal

IASME Cyber Assurance Level One must be renewed annually, together with the prerequisite Cyber Essentials certification.

A successful Level Two audit is valid for three years. However, the organisation must continue to achieve Cyber Essentials and IASME Cyber Assurance Level One annually during that three-year period. A further Level Two audit is required at the end of the three-year cycle.

Choosing the Appropriate Certification

The appropriate certification should ultimately be determined by the organisation's risks, customer expectations, contractual obligations and supply-chain requirements. Where a customer or procurement process specifies a particular certification, the precise requirement should be confirmed before starting the assessment process.

Cyber Essentials is generally appropriate where an organisation:

- Needs a recognised baseline of technical security,
- Is beginning its formal certification journey,
- Must meet a basic customer or procurement requirement, and
- Wants to demonstrate that fundamental protections against common attacks are in place.

Cyber Essentials Plus is more appropriate where:

- Customers, regulators or contracting authorities require independent technical verification,
- The organisation wants greater confidence that its Cyber Essentials controls are operating effectively, and
- The organisation handles information or delivers services for which a higher degree of technical assurance is appropriate.

IASME Cyber Assurance is appropriate where the organisation also needs to demonstrate:

- Structured governance and management oversight,
- Formal risk management,
- Staff awareness and defined security responsibilities,
- Incident management and business continuity,
- Supplier and third-party security,
- Data protection and information management, and
- Evidence that security policies and processes are embedded in day-to-day operations.

Contact Information

United Kingdom

Please visit Aviva Risk Management Solutions or email us at riskadvice@aviva.com. To speak to one of our advisors, call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

Canada

Please visit Aviva Risk Management Solutions | Aviva Canada or email us at arms.canada@aviva.com

Ireland

Please visit Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland or Email us at armsireland@aviva.com

Specialist Partner Services

Aviva have created a network of Specialist Partners to complement our in-house capabilities and to enable our policyholders to benefit from a wide range of risk management solutions at preferential rates and terms. Together, we provide solutions to help with the significant challenges of modern-day risk management.

Note: These partner relationships are wholly for the benefit of our policyholders with no income to Aviva.

The following Specialist Partners provide products or services in relation to risk guidance provided, discussed or referenced in this Loss Prevention Standard.

United Kingdom

- Cyber Security Awareness Training **Phishing Tackle**
- Cyber Security service - **CSA Cyber**
- Online Reputational Security - **Riskeye**

For more information please visit: Aviva Risk Management Solutions – Specialist Partners

Ireland

- Online Reputational Security - **Riskeye**

For more information please visit: Insurance Risk Management | Business Risk Management Insurance - Aviva Ireland

Canada

For more information please visit: Our Specialist Partner Network | Aviva Canada

Standards, Sources and Useful Links

Canada

- Canadian Centre for Cyber Security

United Kingdom

- IASME Cyber Assurance
- IASME – Cyber Essentials
- IASME – Cyber Essentials Certificate Search
- IASME – Cyber Essentials Knowledge Hub
- IASME – Cyber Essentials Readiness Tool
- IASME - Preview the Self-Assessment questions for Cyber Essentials
- NCSC – Cyber Essentials
- National Cyber Security Centre (NCSC)

Other

- The European Union Agency for Cybersecurity (ENISA)

Additional Information

Loss Prevention Standards

These documents set out best practice recommendations to help reduce the likelihood and impact of losses.

Relevant Aviva Loss Prevention Standards include:

- **Cyber - Respond and Recover.**
- **Cyber - Supply Chain Risk Management**
- **Cyber - Ransomware**
- **Cyber - Respond and Recover**
- **Cyber - Incident Response Process**
- **Cyber - Homeworking Security**
- **Cyber - 12 Top Tips to Protect Against Cyber Attacks**

Please visit Loss Prevention Standards to view the full library.

Aviva Risks Training Solutions (United Kingdom Only)

Aviva Risk Training Solutions, delivered through our Specialist Partner, SafetyCulture, provide free, bite-sized learning modules exclusively for Aviva policyholders.

Relevant courses include:

- **Cyber Fundamentals**
- **Social Engineering**

Please visit Aviva Risk Training Solutions for further guidance.

23rd July 2026

Version 1.0

ARMSGI4442026

Aviva Insurance Limited, Registered in Scotland Number SC002116. Registered Office: Pitheavlis, Perth PH2 0NH.
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.