IASME CYBER ASSURANCE

A Guide to the IASME Cyber Assurance Certification

Delivered by

iasme

The **IASME Cyber Assurance (ICA)** standard is a comprehensive, flexible, and affordable way to achieve cyber resilience. It demonstrates that an organisation has put into place a range of important controls related to cyber security and data protection. It also provides an organisation with the practical steps and key controls that are needed to become cyber resilient, as highlighted within the Cyber Governance Code of Practice.

Gaining certification provides a structured way for your organisation to achieve cyber resilience for a realistic cost. It indicates that you are taking good steps to protect your information and business systems. ICA certification is recognised by a wide range of industry sectors as evidence that an organisation has implemented appropriate controls to mitigate cyber risk within the supply chain.

The ICA certification is available in two levels: **Level One Verified Assessment** and **Level Two Audited**. You must pass your Level One assessment before you apply for Level Two.

This document outlines how an organisation can apply for ICA certification and aims to answer all the questions you may have about the process.

For any questions in relation to IASME Cyber Assurance, please contact info@iasme.co.uk.

IASME CYBER ASSURANCE

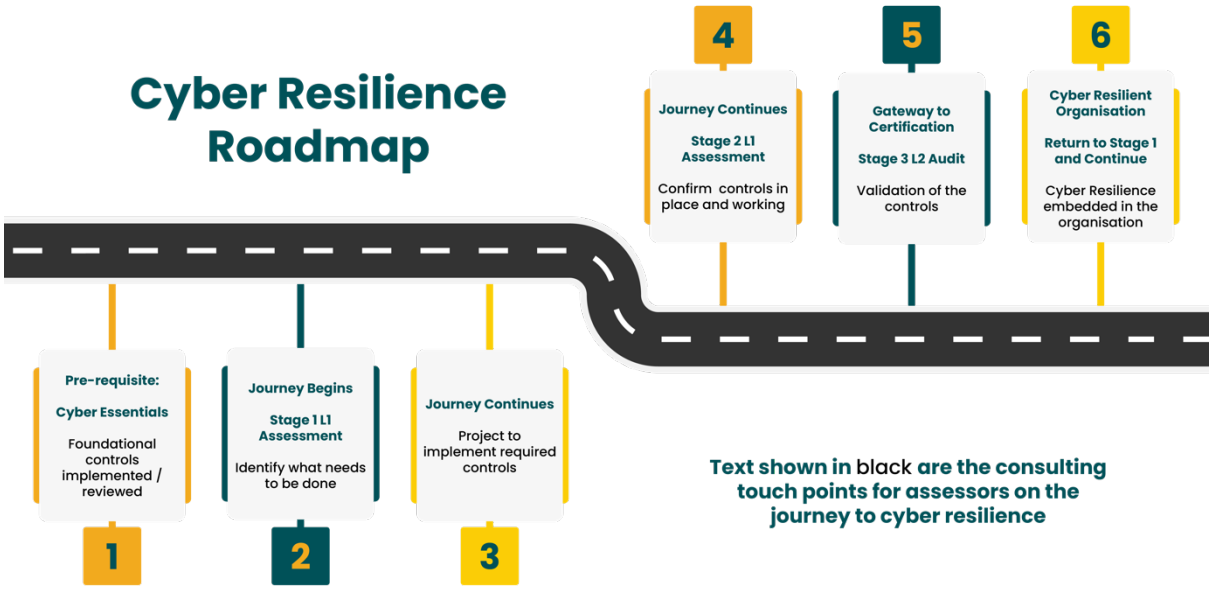
Table of Contents

IASME CYBER ASSURANCE

The Roadmap to Cyber Resilience

The government's Department for Science, Innovation and Technology (DSIT) defines cyber resilience as the ability for organisations to prepare for, respond to and recover from cyber attacks. The IASME Cyber Assurance standard provides a roadmap to cyber resilience for every organisation

ICA was developed with insights from academics, business leaders, and security professionals, drawing on lessons learned from a broad spectrum of security breaches. Designed to address the needs of smaller organisations, it offers a more streamlined and user-friendly approach. By doing so, it not only delivers significant time and cost savings but also provides clear guidance to help companies implement the necessary security measures effectively.



IASME CYBER ASSURANCE

Tailored to Your Organisation's Size

The IASME Cyber Assurance standard has been written to address the security needs of organisations of all sizes, from the sole practitioner to large enterprises. As the full standard is broad-in-scope, it contains requirements that aren't necessarily applicable for everyone.

IASME has tailored the standard to reduce the compliance burden for smaller organisations.

When you apply to complete an assessment, the size of your organisation will determine the appropriate depth of the IASME Cyber Assurance Standard and the themes and requirements that are relevant to you.

- Sole trader / two-person partnership
- Micro businesses (3 to 9 people)
- Small businesses (10 to 49 people)
- All other businesses

The Fourteen Themes of IASME Cyber Assurance

IASME Cyber Assurance is a risk-based, cyber security standard comprising of controls which are divided into fourteen themes. Your organisation needs to meet the requirements of all the applicable themes for the size of your organisation in order to achieve certification against the standard.

The themes cover four major areas; Identify & Classify, Deter & Detect, Protect, and Respond & Recover.

IASME CYBER ASSURANCE

Identify & Classify

Identifying and protecting assets

Having a good understanding of your key information assets is essential in order to know what you need to protect.

Legal and regulatory landscape

Be aware of legal obligations, contractual requirements and agreements and ensure you are fulfilling your responsibilities.

Assessing and treating risks

In order to effectively apply the correct controls to protect your business assets, it is important to understand what the risks are to your business and to manage those risks to keep them at an acceptable level to you, your customers, and supply chain.

Organisation

A clear structure within your organisation is the foundation for effective and successful security. This should include who is responsible for making information safe and who is accountable when incidents happen.

Planning information Security

It is important to include information security considerations within your planning. You must also consider security when planning projects, procurement, contracting, suppliers, and when dealing with partners, and other interested parties.

IASME CYBER ASSURANCE

Protect

Physical and environmental protection

Protect your information assets from physical threats such as theft or loss and environmental harm such as damage from temperature or humidity.

People

Thorough and consistent measures are required to screen and train all staff to enable them to understand and comply with the security responsibilities of their job.

Policy realisation

Policies specify the rules, guidelines, and regulations that you require people to follow. They also reflect the values and ethics that are at the heart of your business.

Managing access

Best practice access control utilises the law of 'least privilege' which means giving users access to all the resources and data necessary for their roles, but no more.

Technical intrusion

It is important to develop capabilities to monitor and respond to unauthorised access and usage. This includes anti-malware solutions and measures to prevent insider threats.

Change Management

Implementing a well-documented procedure for operational and technological changes ensures smooth transitions and helps maintain business continuity.

IASME CYBER ASSURANCE

Deter & Detect

Secure business operations: monitoring and review
Creating processes to track and monitor information systems is important in order to detect threats and take steps to analyse and act on this information.

Respond & Recover

Backup and restore
Regularly backing up information, and having the ability to restore the backup, may be one of the most effective methods of protecting your business from the effects of accidental or malicious tampering.

Resilience: Business continuity, incident management and disaster recovery
A resilient company is one that is able to respond to an incident, keep operating through it, and eventually recover.

Benefits of Certification

Levels of Certification

The IASME Cyber Assurance certification is available in two levels: Level One Verified Assessment and Level Two Audited. **You must pass your Level One assessment before you apply for Level Two.**

Level One consists of a verified assessment which is reviewed by an independent Assessor.

Level Two involves an audit of your processes, procedures and controls required by the IASME Cyber Assurance standard. The audit is independent and conducted by an IASME assured Assessor who will look at documentation, interview key staff and observe activities. This can be done in person or sometimes remotely (such as via a video call).

The Process of Certifying

Before certifying to IASME Cyber Assurance, you will first need to demonstrate that your organisation has got the basics in place. The prerequisite for IASME Cyber Assurance certification is an up-to-date Cyber Essentials certification. If your organisation is outside of the UK, please contact us at info@iasme.co.uk to discuss the prerequisite certification.

The **scope of organisation** that you are certifying to IASME Cyber Assurance must not be larger than the scope of your organisation that is covered in your Cyber Essentials certification.

In order to **purchase** your IASME Cyber Assurance assessment, you must have a valid Cyber Essentials certification in place that has at least 30 days left before expiry.

As soon as you have paid, we will send you login details for your online assessment portal. You will have six months to complete your assessment before your account becomes invalid and unfortunately, we cannot issue a refund if this happens.

In order to **pass** your IASME Cyber Assurance certification, you must have a Cyber Essentials certification with least 30 days left before expiry.

If you do not already hold Cyber Essentials, you can conveniently purchase it online as part of a bundle with your ICA. Once purchased, you'll have six months to complete your Cyber Essentials assessment. After successful completion, your account will be manually upgraded to IASME Cyber Assurance, giving you an additional six months to complete that assessment.

Recertification Requirements

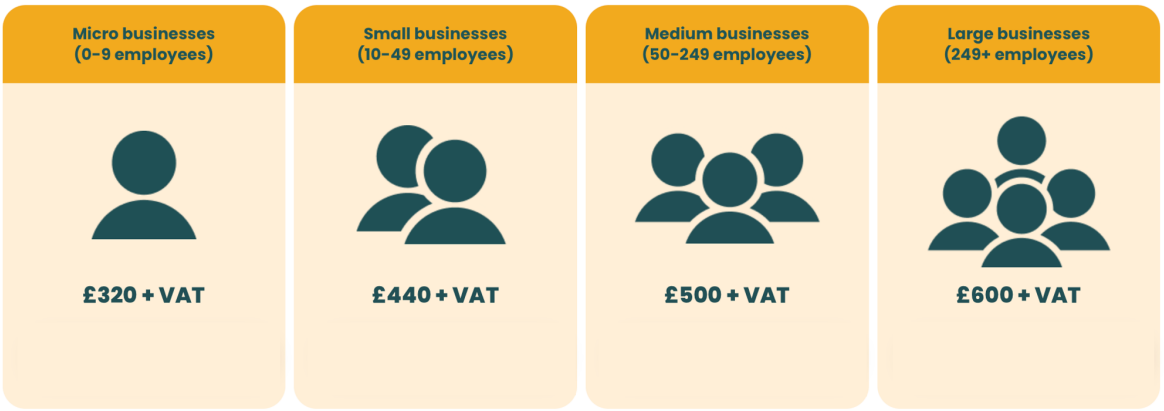
For Level One certification, the requirement is an annual resubmission of the IASME Cyber Assurance verified self-assessment using the online portal, and maintenance of the prerequisite scheme (Cyber Essentials).

The IASME Cyber Assurance Level Two audit is **valid for three years** but requires the Applicant to **achieve Cyber Essentials and IASME Cyber Assurance Level One annually**. This 'soft check' is part of what helps keep the cost of IASME Cyber Assurance more affordable than schemes that require a yearly audit.

IASME CYBER ASSURANCE

Pricing

The pricing structure for Level One certification is based on the size of your organisation:



If you are buying Cyber Essentials alongside your ICA purchase, the cost of Cyber Essentials that corresponds to the size of your business will be added to your purchase:

As the Level Two audit needs more dedicated time from a technical expert, it is more expensive than the verified assessment. The cost will depend on the size and complexity of your network and Applicants can get a quote by by using the function on the IASME website.

IASME CYBER ASSURANCE

Links to the Standard, Question Set and Helpful Templates

Our most up to date, downloadable documents are available on the IASME Cyber Assurance webpage here.

Frequently Asked Questions

Our most up to date FAQs are available on the IASME Cyber Assurance webpage here.

If you have any questions and would like to chat with one of our expert advisors, please contact us today on **03300 882 752** or email us on **info@iasme.co.uk**