



# IASME CYBER ASSURANCE STANDARD V7.0 EXECUTIVE SUMMARY

© IASME Consortium Limited 2025

All rights reserved.

The copyright in this document is vested in IASME Consortium Limited. The document must not be reproduced, by any means, in whole or in part or used for manufacturing purposes, except with the prior written permission of IASME Consortium Limited and then only on condition that this notice is included in any such reproduction.

Information contained in this document is believed to be accurate at the time of publication, but no liability whatsoever can be accepted by IASME Consortium Limited arising out of any use made of this information.

# MODIFICATION HISTORY

Revision	Date	Revision Description
6.0	April 2022	Detailed revision, restructure, and full update of the standard. Rename of standard from IASME Governance.
6.0a	May 2022	Re-name Assured to Assurance
7.0	May 2025	Detailed revision, restructure, update of the standard and the introduction of Themes and Requirements by organisational size in separate documents. This document contains the Executive Summary of the Standard.

# CONTENTS

Modification History.....	2
Contents .....	3
Chapter 1 – Introduction .....	4
The need for cyber resilience.....	4
The aims of the IASME Cyber Assurance standard .....	5
What are the business drivers for applying the IASME Cyber Assurance standard? .....	5
Compatibility with regulation and other standards .....	6
How to use this document .....	6
Chapter 2 – How the IASME Cyber Assurance standard works .....	7
Understanding your organisation – and defending it .....	7
Learning from your risk assessment and making changes to become more secure .....	8
Showing customers, suppliers...and yourself.....	9
The assessment and certification process.....	10
Who governs the Standard? .....	12
Chapter 3 – Scope .....	14
How to scope your organisation for certification .....	14
Chapter 4 – The fourteen themes: requirements and guidance.....	17

# CHAPTER 1 – INTRODUCTION

## The need for cyber resilience

Organisations of all sizes need to keep their data safe and prevent breaches of information that would expose their customers, clients and investors to negative impacts. They also need to be resilient to cyber-attack, minimising disruption to the organisation and allowing them to continue to operate without undue disruption in the event of an attack.

Increasing reliance on information has made good information security a fundamental requirement. The types of data that need protecting include information about customers, clients, finances, details of how products are manufactured, communications via instant message/email and so on.

It has also led to the increasing use of information systems, meaning that organisations are now reliant on their information systems in order to operate efficiently and effectively. Information systems are used to collect, store, process and transmit digital data and information. The loss of one or more systems to a cyber-attack reduces the ability of the organisation to achieve its aims and in the worst case totally prevents it.

Organisations often overlook the need to protect their information systems and data in their spending priorities because they are often difficult to value. The true worth may only be realised after their systems are no longer useable or information has been lost or damaged.

While there can be no guarantees for cyber resilience, security frameworks and standards can guide organisations on how to reduce the risks to systems and data – and their impact – to an acceptable level to prevent disruption to the organisation.

Unfortunately, many security frameworks have historically been created with large corporations in mind, where size and resources give them the ability to implement complex protective measures.

By contrast, smaller or more flexible businesses and organisations need to deal with cyber resilience with greater flexibility and with much smaller budgets. The structure of rigid procedures that support the internal communications in large organisations must give way to the informal cultures of small to medium-sized enterprises (SMEs), including where people are working alone or in a partnership.

The IASME Cyber Assurance standard was created specifically to address these needs and thereby help organisations achieve cyber resilience. Given different size organisations

have different risks, the standard has been tailored by size to reflect the key security issues faced by various sizes of smaller organisations.

## The aims of the IASME Cyber Assurance standard

The Cyber Assurance standard is a formal information security methodology that is particularly accessible to SMEs but can be applied successfully to any organisation. It is sector agnostic and provides a working framework to assure information security against the background of contemporary threats.

The standard is designed to provide clear, simple to understand guidance to applicants on cyber resilience and then to provide a high-quality, independent assessment of the level of maturity of an SME's cyber resilience.

Once assessed to the standard, applicants can demonstrate good security practices to assure customers/clients, supply chains and others that the systems used, and the data stored and handled by the certified company are protected to a reasonable level for most practical purposes.

The IASME Cyber Assurance standard is an organised way for a business to implement new ways of securing its systems and information, improve existing ones, and be recognised in its sector for having done so. It is also a great opportunity for those operating the business to improve their knowledge of security.

## What are the business drivers for applying the IASME Cyber Assurance standard?

The IASME Cyber Assurance standard enables organisations to:

- Identify risks to their information and information systems
- Apply adequate barriers and controls to reduce the likelihood and impact of cyber incidents to an acceptable level
- Proactively verify that the security controls that they implement provide the intended level of security
- Be independently reviewed by an assessor who understands their size and level of business risk to verify the effectiveness of their security activities
- Work to a standard of information security within a supply chain regardless of size
- Give themselves, customers – including government procurement departments, and their supply chain – a level of assurance that appropriate controls are in place
- Demonstrate to legal authorities the actions taken towards complying with applicable legislation and regulation such as GDPR

## Compatibility with regulation and other standards

The standard has been compiled by SMEs for SMEs, originally with the support of the Technology Strategy Board (now Innovate UK). It provides common ground for SMEs alongside other information security standards – which are either not comprehensive or are too prescriptive in their level of complexity for an SME.

The IASME Cyber Assurance standard requires attention to the respective laws and regulations that are applicable to the target of evaluation in general and those applicable to information security arising from information collection, storage, processing, and disposal in particular.

The standard predicates itself on good practice and so avoids having to be reissued as legal systems change to deal with new technology or changes in its use.



### GDPR:

*The General Data Protection Regulation (GDPR) enshrines the basic principle of the IASME Cyber Assurance standard in law. It requires you to know what you are protecting and understand its relative value to its subjects and the impact of a security breach. Through this, protective measures can be put in place and routes to recovery planned in case of an incident. Additional supporting guidance for those seeking to implement the IASME Cyber Assurance standard in tune with the nuances of EU and/or UK GDPR is available at <https://iasme.co.uk/gdpr/>*

## How to use this document

The remainder of this document is organised into the following sections:

- **Chapter 2** – explains how the IASME Cyber Assurance standard works to help you achieve a state of information security. In this section:
  - The fourteen IASME Cyber Assurance themes for information security are introduced.
  - The process of implementing the controls and improving your security is outlined, alongside an overview of how the assessment process works to measure and demonstrate your compliance.
- **Chapter 3** – covers how to define an appropriate scope, to realise the IASME Cyber Assurance standard's fourteen themes, and to create and manage your information security management system.
- **Chapter 4** – sets out the fourteen themes: requirements and guidance.

## CHAPTER 2 – HOW THE IASME CYBER ASSURANCE STANDARD WORKS

### Understanding your organisation – and defending it

The IASME Cyber Assurance standard is a route to maintaining a balanced state of information security so that you can focus on your core business objectives, without either limiting your activities by restrictive practices, or leaving yourself vulnerable to avoidable losses.

The standard is risk-led, and your risk assessment will provide guidance on how you prioritise your activities. The controls within the standard form the baseline for protection of your organisation, with your risk assessment always guiding the depth of protection and any additional controls that may be needed.



#### *Template available:*

*IASME can provide a risk assessment template that is suitable for smaller organisations*

The depth of protection you need is not always linked to the size of your organisation – a small organisation with highly sensitive information assets may need to put more effort into protecting them than would a large company that deals with less sensitive information.

You will need to consider any number of threats ‘actors’ and potential events that might vary from invisible technical hacking to social engineering. Do they have the capability, the intent, and the opportunity to cause harm? And if they did, would the impact matter? Might you be the conduit to your customers who are the ‘high value’ targets for the attackers?

When reviewing risk, consider:

- How information systems support your organisation
- How outsourced (including ‘cloud’) facilities are used
- Whether you and the people you work with use their own equipment for business (BYOD)
- How remote and mobile systems are used
- Awareness and attitude to the threat environment
- Estimated value of the business’ information assets, including physical equipment used and the data itself

## Learning from your risk assessment and making changes to become more secure

Your risk assessment will guide the decisions made about the information security controls you need to put in place to keep your data safe and your organisation resilient. These controls are the practical measures that you put in place to protect your information and technology.

It is best for these controls to be built into business processes so that security operates in harmony with the business and is indistinguishable from it as much as possible. You choose the controls based on your risk assessment and you can make adjustments at any time as the risks change.

The controls are divided into four categories which should be a logical progression:

### Identify and Classify:

This category helps you to identify your assets, classify the importance of each one, look at the legal landscape, your risks, and understand what you need to protect.

### Protect:

This category focuses on putting in place good policies, controlling access to information, preventing technical attacks, physical security and people.

### Detect and Deter

This category looks at business processes, including monitoring to detect attacks, reviewing and managing changes to systems.

### Respond and Recover

This category looks at how you can respond to incidents and recover from them through backing up your information along with good business continuity and disaster recovery processes.

The IASME Cyber Assurance standard breaks these four categories down into fourteen manageable, bite-sized themes, allowing you to easily control the pace at which you implement, improve, and measure the effectiveness of your information security (see Figure 1 below).

These controls are built upon the foundation of the organisation having achieved a basic level of technical cyber security. This comes from the mandatory requirement to achieve one of the pre-requisite schemes (Cyber Essentials or IASME Cyber Baseline), before applying for certification to IASME Cyber Assurance.





*Figure 1 - The fourteen Themes of the IASME Cyber Assurance standard*

## Showing customers, suppliers...and yourself

The standard is a simple to understand process that produces a documented and objective measure of the level of security in your organisation. This is important and useful because it can be used to reassure your customers and supply chain that you will keep their information secure and that the products and services that you supply will not be interrupted by avoidable information security incidents. You can also reassure yourself that your company systems and information are safe, and you have achieved a level of cyber resilience.

The standard and the question set are freely available to anyone who wants to download them from the IASME website (<https://iasme.co.uk/iasme-cyber-assurance/>). This means that your customers and suppliers can see exactly what is involved in the certification process and use it to verify your security.

## The assessment and certification process

### *Certification Bodies and Assessors*



IASME owns and operates the IASME Cyber Assurance standard, but the assessment of organisations is operated by IASME's Certification Bodies.

The Certification Bodies are companies with in-depth knowledge of information security who have met the high security, quality and skills requirements set by IASME. Each Certification Body has a number of Assessors, who are skilled and experienced information security experts who carry out the assessments.

### *The process*

Although accessible to organisations of all sizes, the Standard is designed specifically to accommodate the needs of SMEs and ensure the certification and compliance process does not place an onerous burden on smaller organisations.

Table 1: Certifications available

Following online self-assessment by an IASME Certification Body (Level 1)	
	An award demonstrating an organisation's proactivity towards maintaining a reasoned state of cyber and information security.
Following an audit by an IASME Certification Body (Level 2)	
	An award independently confirming that an organisation's achievement in cyber and information security is in line with industry expectations.

An organisation can certify to IASME Cyber Assurance at two levels (see table 1):

- Level 1 (Verified self-assessment)
  - The organisation achieves one of the pre-requisite schemes (Cyber Essentials or IASME Cyber Baseline).
  - The organisation completes the online IASME Cyber Assurance assessment by answering a set of questions through IASME's online portal. The questions are marked by an Assessor who provides useful feedback and determines pass/fail for the assessment.
- Level 2 (In-person or remote audit)
  - After completing and achieving a pass in the Level 1 assessment, an Assessor carries out an audit of the organisation looking at documentation, interviewing key staff and

observing activities. This can be done in person or remotely (such as via a video call).

- The draft report can be shared with the client to allow any issues identified to be addressed before ratification by IASME's moderators.
- After the audit has been ratified by IASME's moderators, the organisation will achieve pass/fail depending on how well the organisation meets the standard.

The standard relies on a process of continuous assessment, with an initial cycle leading to your first certification, and continuing with assessments annually.

For Level 1 certification, the requirement is an annual resubmission of the IASME Cyber Assurance self-assessment using the online portal and maintenance of the pre-requisite scheme (Cyber Essentials or IASME Cyber Baseline).

For Level 2 certification, the requirement is based on a three-year cycle. Organisations are required to complete the IASME Cyber Assurance self-assessment using the online portal in years two and three after achieving their audited certification. At year four, the organisation needs to recertify to Level 2, starting the process afresh (see Figure 2).

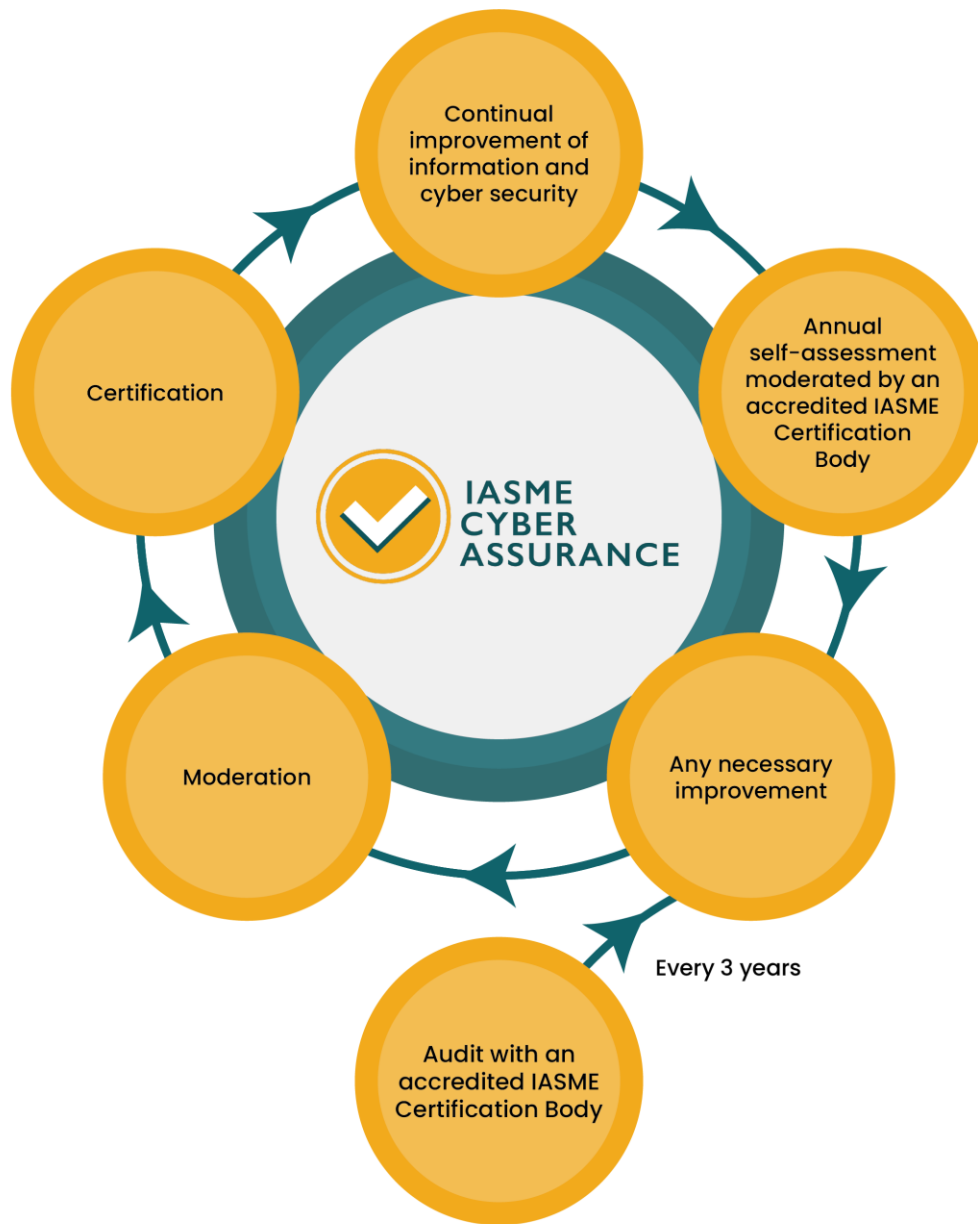


Figure 2: Round-tripping with the IASME Cyber Assurance implementation cycle

## Who governs the Standard?

The development of the IASME Cyber Assurance standard is reviewed by an independent advisory panel and updated as a result of changes to the threat landscape, drawing on the latest expertise from across industry sectors.

IASME is an ISO 9001 certified organisation and follows a strict set of quality policies and processes to ensure consistency within the certification process.

The Certification Bodies meet strict security and quality requirements, and the Assessors meet specific skills and experience requirements, as well as receiving ongoing training and support from IASME's dedicated support and customer services team. All Assessors are required to comply with a code of conduct which is accessible from IASME's website (<https://iasme.co.uk/wp-content/uploads/2020/03/Schedule-18-Assessor-Code-of-Conduct.pdf>).

The certification process itself includes ongoing quality control with sampling of assessments and feedback to Assessors and clients as needed.

A key part of the IASME Cyber Assurance standard is the role of the IASME moderators. These are experienced security auditing professionals who act as custodians of consistency and quality for the assessment process. Assessors act as a proxy for the moderators. It is the moderators who make the ultimate decision on certification for a particular organisation, which allows more flexibility for the Assessors to provide guidance and support to the client on how to comply with the standard.

This is a deliberate and important part of the standard – we believe that an end result of better information security is achieved if the Assessors are able to provide detailed guidance to clients on how to improve their security. The role of the IASME moderator allows this to happen whilst retaining the integrity and simplicity of the assessment process.

## CHAPTER 3 – SCOPE

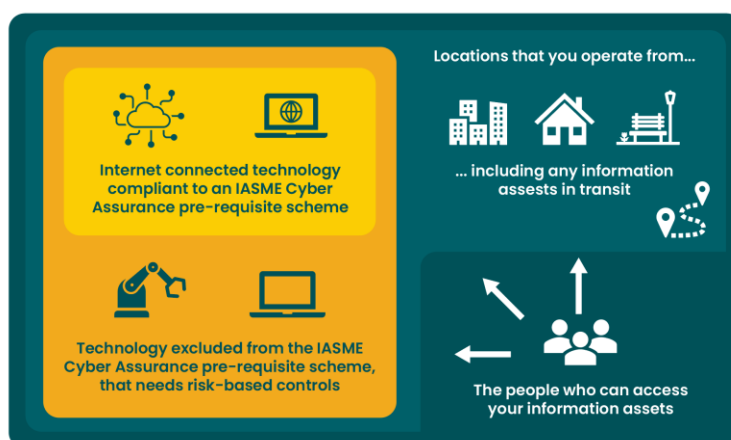
### How to scope your organisation for certification

Perhaps surprisingly, scoping can be the most difficult part of certification! The ultimate aim of the standard is to certify your 'whole organisation' because this gives you the most protection and ensures you have embedded the controls appropriately.

But, the details of scope can be confusing, particularly for more complex organisations. The information below will guide you on what needs to be in scope for assessment.

There are four elements to consider for the scoping boundaries:

1. the size of the organisation
2. the technology used (both internet and non-internet connected technology)
3. the locations from which you operate
4. the people who can access your information assets



*Figure 3 – The three components for defining the IASME Cyber Assurance scope*

#### 1 – The size of your organisation

Whilst it is true that the depth of protection you need is not always linked to the size of your organisation, there are some elements of the standard that are not applicable to all organisations. For example, having a formal process for hiring staff does not apply to a sole trader and forming a security group to coordinate and implement security activities isn't necessarily appropriate for a micro company.

To accommodate organisations of various sizes the Themes and the Requirements of the IASME Cyber Assurance Standard has been tailored to size, based on a set of mandatory requirements, to provide a cost effective and efficient set of security controls.

The Themes and Requirements are available separately to this document and are sized as follows:

Theme and Mandatory Requirements Tailored to Organisation Size	
Organisation Size	Theme and Requirements to Use
0-2 people	Sole Trader / Two Person Partnership
3-9 people	Micro organisation
10-49 people	Small organisation
50+ people	All other organisations

## 2 – Your technology

The base level security of your technology is mostly covered by your achievement of one of the pre-requisite security schemes in table 2 below. For UK organisations, the pre-requisite scheme will be Cyber Essentials at the self-assessed level. We use these schemes to ensure that your organisation has basic technical cyber security in place. The IASME Cyber Assurance standard then builds on these foundations.

In all instances, any IT equipment within the scope of your certification must meet the scoping requirements from your chosen prerequisite scheme.

Table 2: Prerequisite schemes

Scheme name	Requirements and availability
Cyber Essentials self-assessment	Mandatory if the organisation is in the United Kingdom
IASME Cyber Baseline self-assessment	Optional alternative to Cyber Essentials for organisations not in the United Kingdom

In addition to the requirements of your chosen pre-requisite scheme, all systems that contain information are in scope for IASME Cyber Assurance, including those that don't

have an internet connection such as offline servers, air-gapped systems, and production networks. Paper-based systems are covered too.

### 3 – Locations from which you operate

If your organisation has multiple locations, then all locations must be in scope for assessment. You should apply tools, techniques and policies to all areas of the business and consider all locations as part of your risk assessment.

If you share a location with other businesses (such as at a co-working space or share office building), ensure that you have sufficient security controls to cover the risk of other businesses activities affecting the security of your own. For example, you might need your own segregated network or separate physical security system.

### 4 – People that can access your information assets

Franchises, agents, and resellers need their own certification if they are accessing your data, and this should be managed through your contractual agreements with them. However, you must include them in your risk assessment alongside all your staff and any other people who have access to your business information on a regular basis, such as contractors. This allows you to consider how best to apply your security controls consistently throughout.

For example, although contractors will likely still need their own certification to an information security standard, your close relationship with them means you are likely to undertake relevant activities to ensure they meet security requirements, such as providing training regarding keeping your data safe and managing their access to your data.



## CHAPTER 4 – THE FOURTEEN THEMES: REQUIREMENTS AND GUIDANCE

The IASME Cyber Assurance standard comprises of activities which are divided into fourteen themes. Your organisation needs to meet the requirements of all of the requirements within the themes that are applicable to your size of organisation in order to achieve compliance with the standard.

The Standard tailored to size is shown in Chapter 3 above and the relevant download is available from the IASME website (<https://iasme.co.uk/iasme-cyber-assurance/>). You may wish to start with a couple of themes and build up your activities from there. The themes are in a logical order, so we would suggest starting with the first theme and progressing forward with your activities as time and resources permit.

Once you have implemented each theme, it is important to maintain it on an ongoing basis and the three-year cycle is designed to help you keep up to date.