IoT Security Assurance Partner Scheme Assessment Report on

IASME BASIC IoT Security Scheme

Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing

Notices

Documents published by the IoT Security Foundation ("IoTSF") are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org/

Terms of Use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organisation which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF's membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high quality guidance, IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this version of the document

Scheme Inspectors:

Sarb Sembhi, Virtually Informed (lead author)

Richard Marshall, Xitex Ltd

Reviewers:

John Moor, IoT Security Foundation

Introduction

The IoT Security Foundation's (IoTSF) mission is *"to help secure the Internet of Things"* in part by:

- Composing and maintaining a comprehensive IoT Security Compliance Framework of recommended steps for creating secure IoT products and services;
- Promoting the adoption of the IoT Security Compliance Framework to IoT service and product providers, IoT system specifiers, purchasers, and policymakers;
- Composing and promoting security best practice guidance; AND
- Helping to arrange assurance processes to demonstrate that IoT products and services meet the requirements of the IoTSF Compliance Framework.

[ref: https://www.iotsecurityfoundation.org/about-us/ dated June 4th 2019].

It is the intention of IoTSF to either create, or support commercially available security assurance assessment Schemes which satisfy market needs and can be directly mapped to the IoTSF Compliance Framework, in whole or in part.

[ref: IoT Security Compliance Framework Release 2.0 downloadable from https://www.iotsecurityfoundation.org/best-practice-guidelines/].

This document is intended to provide a recommendation to the IoTSF on suitability of a proposed submitted Scheme by a duly appointed Scheme Inspector (SI). The third party will have expressed an interest to become an IoTSF Assurance Scheme and mission partner by submitting a proposed Scheme.

For successful applicants, this report will be made public to support the promotion of the Scheme in a transparent manner. The intention is to help potential customers of the Scheme make business decisions based on their specific circumstances.

The Assessment Outline

The role of the Scheme Inspector (SI) is to assess the Scheme presented, complete the report and make necessary recommendations to the IoTSF management as to the suitability of including the Scheme as part of the IoTSF Assurance Partners Program.

The assessment covers:

- How the proposed Scheme relates (maps to) the IoT Security Compliance Framework (and where relevant, related standards and frameworks).
- Target market and users
    - Description of the market and the region covered
    - Viability of market
- Scheme description: Operational Description and Governance of the Scheme
    - Corporate governance assurance
    - Product assurance
- Evaluation Methodologies
    - How will the assurance be demonstrated as fit for purpose?
- Compliance with legislation
- Does the Scheme fit within, or support any regulatory requirements?
- Assurance Scheme owner
    - Credibility and ability of owner to provide the assurance service(s)

The Assessment

This Scheme is proposed by the IASME Consortium, which has several years of experience with both the Cyber Essentials and the IASME Governance standard, and it is a member of the IoTSF. IASME intends that this proposed Scheme will have similarities with its current offering of the Cyber Essentials Scheme – in that it will offer both a low enough level of compliance which can be a verified self-certification and at the same time there are other levels of certification which are high enough to provide additional assurance.

Describe how the Scheme relates to the IoTSF Compliance Framework

The proposed Scheme references selected IoTSF Compliance Framework Requirements (CFRs) and the DCMS' Code of Practice Requirements (CoPR).

It is not the intention of the Scheme to meet all or even a majority of the IoT Compliance Framework Requirements (IoTSF CFRs), but rather to offer the industry a practical assurance Scheme that can be achieved by many suppliers. The intention is to offer a Scheme that small businesses will be able to comply with to provide security starting with the very basics.

The Scheme proposes a Basic level, which is to be considered as the equivalent of Cyber Essentials Basic in that it is aimed to be the verified self-certifying level.

The proposed Scheme will enable the IoTSF to achieve part of the following mission:

- "*Helping to arrange assurance processes to demonstrate that IoT products and services meet the requirements of the IoTSF Compliance Framework*."

This Scheme helps achieve the above mission by providing an assessment, which is achievable at a low cost to SMEs and yet still meet some key security requirements of the IoTSF CFR and the CoPR.

The IoTSF Compliance Framework compliance class '0' requirements have been mapped to a Basic level. Further details are provided with a summary in the mapping section below.

Market Description and Demand

The market for IoT devices and related supply chain components and services has had a lot of attention from market analysts with daily reports highlighting how big each sub-market will be in the coming years. There is no doubt that the market for IoT devices, systems and services will be very big, as it covers homes, offices, infrastructure, and consumer, health, surveillance, white goods, etc. Every environment and sub-market that has already seen at least a handful of devices and products in development or available and perhaps even into versions two or three.

The question to consider here for this Scheme is, "is there a market demand for the proposed Scheme, and is this of value to the IoTSF?"

In some respects, one may argue that there is no demand for such a services as: a) consumers have often opted for usability over security or privacy, and b) at this early stage, any proposed Scheme will have to create the market for all such Schemes. However, the factors that affect the demand for a low-cost Scheme include:

- The growth and pervasiveness of connected IoT devices into our lives has been astounding, and is set to grow even further.

- There has been a general and continued outrage by the press and public when toys, baby monitors and other consumable devices have lacked security and privacy. These realities are beginning to be recognised all over the world and that it is an unacceptable state for long-term consumer confidence. Therefore, if the long-term market for IoT devices and services is to grow, manufacturers and other stakeholders need to resolve security issues sooner rather than later.

- The UK Government's response, through the DCMS' Code of Practice for Consumer IoT Security requirements has provided an impetus for the market for such a Scheme. Indeed, the Code of Practice and other international standards and approaches, including the European Standards Organisation's own guidelines has been mapped closely enough to provide some levels of alignment between them. Such work has demonstrated that there is a desire by many stakeholders to have IoT products that are secure, and that the starting point to tackle among the vast range of IoT products is consumer products. There are several related projects covering health devices, manufacturing and other sectors but they are all secondary to consumer products when talking about desired outcomes by governments. The audience for the DCMS Code of Practice is Device Manufacturers, IoT Service Providers, Mobile Application developers and Retailers, and these will help drive the demand for such Schemes.

- Even though consumer products are a much smaller subset of the vast number of IoT device groups available today, it is still a very large and diverse market, which covers everything from toys to baby monitors, connected detectors and door locks, home entertainment (cameras, TVs and speakers), wearable tracking devices, home automation and alarm systems, connected appliances, and home assistants. Analysts daily market growth forecasts for different groups of products, predict ever-increasing rates of growth and market penetration by such devices. Thus, it is important every stakeholder in the supply chain will need to be prepared to meet the expected future consumer demand.

- At the time of submission there are no widely used or accepted assessment Schemes with which to independently evaluate IoT devices' and products' security. In particular, there is nothing available for SME's to have a low cost assessment which would help consumers to identify and select a product that has been certified as having achieved a known level of security. This is not to say that there are not several standards and frameworks available, but that there are currently no practical Schemes, that are able to offer a cost-effective, widely accepted solution.

- The Scheme Proposer's own research with its existing certifying bodies indicates that there is a demand by stakeholders in the Consumer IoT device distribution channels, for such a Scheme.

As the DCMS' current Cyber Essentials certification has shown, if the Scheme is kept simple, industry will find it easier to adopt as the mandatory approach by government, so that it becomes accepted as the *de facto* way forward.

Scheme Name: IASME IoT Basic Assessment.

Who is the Scheme aimed at?

The target for the proposed Scheme is manufacturers and vendors of consumer physical security products in the UK. The typical customer for the Scheme would be a manufacturer wanting certification for a specific consumer product. It is thought that a single manufacturer may pay for a number of products to be assessed under this Scheme, perhaps as a group of related products. The Scheme could enable manufacturers to differentiate their offering from other similar products or suppliers.

Market for IoT security assessment?

The market for IoT security assessments is the end stage after the uptake of devices and services, followed by increases in vulnerabilities and breaches in insecure devices experienced by consumers. The growth of insecure products and home networks is of great concern to the UK Government as it goes against its goal of being "A safe and secure cyberspace - making the UK the safest place in the world to live and work online".

Most existing security frameworks (and associated assessments) available have been focused on achieving organisational security. This Scheme is one of the first based on the IoTSF Compliance Framework, and the first aimed specifically at the IoT device and product security market.

Organisations that have achieved or sought to align with organisational standards (like ISO27001) have often argued for there to be practical assessments for IoT products, so that they can ensure that their adherence to organisational security standards are not weakened by the utilisation of IoT products and devices which don't meet any minimum security level. There is a great demand and push by enterprise security teams to use only those products meeting an agreed or acceptable level of security. Unfortunately, that same demand does not exist for consumer products since there are no organisational home security standards or assessments for secure homes leading that demand – hence the focus on the consumer device market.

Consumers in the home market generally do not understand security and are most likely to be vulnerable due to that lack of security knowledge and understanding. Without assistance, consumers are unlikely to know what they want or need when it comes to the security requirements of IoT products and devices. The DCMS Code of Practice was brought in to help device Supply Chain stakeholders to take action so that consumers do not have to do so.

Route to market

The primary route to market for this Scheme will be through the Proposer's existing wide network of Cyber Essentials Certification Bodies who already operate in a range of UK market sectors. The Scheme Proposer also has close links to some large membership organisations, such as those within the physical defence space, and would work with them to gain traction in the market.

What are the perceived benefits to the customer/market sector?

Stakeholders of this Scheme may benefit many ways, including the following:

- In the short term, the first few manufacturers requesting assessments may get a lot of publicity for making the headlines around the security of IoT devices and their commitment

to consumers. In the longer term, as more manufacturers start to push the security aspects of their assessed products, it will help raise both awareness and take-up of secure products.

- Greater publicity of both secure and insecure products may attract the attention of other manufacturers who may decide to have the certification for all their products and devices over time and benefit their entire distribution network to sell secure products.

- In the same way that the Cyber Essentials Scheme provided a single certification for working with any UK Government Agency, this Scheme may lead to becoming the *de facto* security standard for UK consumer market.

- The Scheme could be seen as a great differentiator by vendors selling consumer products in this country and especially by those reviewing them in online publications. As awareness grows by those reviewing consumer IoT products, the Scheme may become the kitemark that consumers look for in comparative reviews.

- As with Cyber Essentials, where SME's begin to understand security basics, and it provided a starting point for some to take the next steps and explore doing more. In the same way, this Scheme could provide a similar outcome in the long term, as manufacturers start to request product assessments, others may begin to undertake the assessment too so that all their distributors and retailers can sell with confidence. With a greater awareness, over time manufacturers could start to add more security and privacy features.

- When the Scheme starts to penetrate the consumer physical security devices market effectively, it will have a very noticeable impact on ordinary people who do not have any experience, knowledge or understanding of security. The effects will be to help consumers become more aware of the need and requirement of security functionality as one of the main buying criteria.

- It is anticipated that in the medium term, as manufacturers selling to the UK make changes, that these benefits will be available to consumer products sold in other markets and countries too.

- A possible outcome is that if this and similar Schemes become successful, they will reduce the likelihood of the UK being a place for foreign suppliers to dump cheap insecure products.

Any Scheme that provides greater consumer confidence on security, to help boost an already growing market, will be good for the industry, the UK and other international markets.

Scheme Description and Operation

The Scheme will has been developed in partnership with IoTSF and is owned by the IASME Consortium who is also the Accreditation Body, which will accredit Certifying Bodies to undertake assessments when requested by manufacturers to assess selected products.

The Scheme will be available through both existing and new Certifying Bodies who will offer the certification Scheme for the Basic marking level to manufacturers of connected physical security products, covering elements of the IoTSF Compliance Framework requirements and the DCMS top 3 Code of Practice requirements.

What is the process?

The proposed Scheme offers a verified self-assessment, which can be followed by manufacturers or Certifying Bodies on behalf of their customers.

A prospective Certifying Body (CB) will undertake a training course during which they will complete a test to confirm their knowledge of what is required by a Certification Body. Once the prospect has satisfactorily passed the test, it can apply to become a Certifying Body. Each Certifying Body will not only undergo a set training course but will also be expected to have the standard security background, experience and certifications as prescribed in the Proposer's "Assessor Requirements" documentary evidence.

The Certifying Body will be able to use the Accrediting Bodies' logo and other branding tools to promote its standing and participation in the Scheme. The CB will be required to attend regular update, support and training sessions throughout the year to ensure that it is informed and aware of industry changes as well as any interpretations of any requirements.

How much does it cost?

The information submitted states that cost will be low and accessible to SME's – i.e. in the same fee brackets as it is for Cyber Essentials.

Who carries out the work?

There are three key work areas to consider here, firstly the work of the assessment, secondly the work of the trainer and assessment of the Certifying Body, and thirdly the work of verifying the actual assessments on a day-to-day basis.

The self-assessment may be undertaken by anyone, including a retailer or manufacturer (as well as a certifying body), as it is aimed at a low level and that it will be 'verified' by the Accreditation Body (the Scheme Proposer).

The overall work of assessing and supporting the Certifying Bodies is undertaken by the Scheme Proposer's staff and advisory team.

What type of assurances does the Scheme cover – governance, product etc.?

The Scheme aims to provide Basic process and product assurance, as per the summary table below.

What documentation/evidence will be provided as an output of the evaluation?

When a user completes the online self-assessment questionnaire and submits it for compliance evaluation, they will be provided with the completed question / answer response details they have submitted. Later when an assessment has been completed by the Accreditation Body, the user will receive a certificate to indicate that the product assessment submitted has achieved the required level.

How can the evidence be inspected? (Certificate? Label? Request for technical file etc.)

A public list will be available on the IASME website similar to the current Cyber Essentials Certification Scheme. The two lists that will be available online are a complete list of products and related versions of certified devices, and a list of all new and expired Certification Bodies. These lists

enable anyone wanting to check either, for certified products or bodies who can undertake such work are able to do so.

How will the Scheme be maintained?

The Scheme will be reviewed annually, or when a new version of the IoT Security Compliance Framework is release using a similar process to its other current Schemes, which involve feedback from customers, certifying bodies, industry bodies and the Framework owners. There are several opportunities for certifying bodies to feedback customer views throughout the year.

The Proposer's staff maintain the Scheme on a day-to-day basis, and governance is provided through its management and advisory groups.

Scheme mapping

The following section covers the requirements of the proposed Scheme in relation to the IoTSF's Compliance Framework.

There are two key tables in this section, the first shows the IoTSF Compliance Framework (CF) requirements, which need to be met for each of the three Proposed Scheme's levels. The second shows all of the Proposed Scheme's requirements set out by the IoTSF CF Applicability Group. A summary of the above two table are also provided for guidance.

A Summary of the Proposed Scheme's IoTSF requirements for each level

Scheme level	Total IoTSF requirements
Basic	30 requirements

IoTSF CF Requirements to be met for Proposed Scheme levels

Scheme level	IoTSF Applicability Group	IoTSF Requirement number	Requirement
Basic	**Business Security Process and Responsibility**	2.4.3.1	There is a person or role, typically a board level executive, who takes ownership of and is responsible for product, service and business level security, and makes and monitors the security policy
		2.4.3.5	A policy has been established for interacting with both internal and third party security researcher(s) on the products or services.
		2.4.3.7	Processes and plans are in place based upon the IoTSF "Vulnerability Disclosure Guidelines" [ref 19], or a similar recognised process, to deal with the identification of a security vulnerability or compromise when they occur.
		2.4.3.8	A process is in place for consistent briefing of senior executives in the event of the identification of a vulnerability or a security breach, especially those executives who may deal with the media or make public announcements. In particular, that any public statements made in the event of a security breach should give as full and accurate an account of the facts as possible.
		2.4.3.9	There is a secure notification process based upon the IoTSF "Vulnerability Disclosure Guidelines" [ref 19] or a similar recognised process, for notifying partners/users of any security updates.
		2.4.3.11	As part of the Security Policy, develop specific contact web pages for Vulnerability Disclosure reporting.
		2.4.3.12	As part of the Security Policy, provide a dedicated security email address and/or secure online page for Vulnerability Disclosure

			communications.
		2.4.3.16	As part of the Security Policy, develop security advisory notification steps. For examples see US Cert programme [Ref 46]
	Device Hardware	2.4.4.1	The product's processor system has an irrevocable hardware Secure Boot process.
		2.4.4.4	The Secure Boot process is enabled by default.
	Device Software	2.4.5.1	The product has measures to prevent unauthenticated software and files being loaded onto it. In the event that the product is intended to allow un-authenticated software, such software should only be run with limited permissions and/or sandbox.
		2.4.5.2	Where remote software updates can be supported by the device, the software images are digitally signed by an approved signing authority.
		2.4.5.3	Where updates are supported the software update package has its digital signature, signing certificate and signing certificate chain verified by the device before the update process begins.
		2.4.5.4	If remote software upgrade is supported by a device, software images shall be encrypted or transferred over an encrypted channel whilst being transferred to it.
		2.4.5.22	For devices with no possibility of a software update, the conditions for and period of replacement support should be clear
		2.4.5.25	Support for partially installing updates is provided for devices whose on time is insufficient for the complete installation of a whole update.
		2.4.5.27	Where real-time expectations of performance are present, update mechanisms must not interfere with meeting these expectations (e.g. by running update processes at low priority).
		2.4.5.29	Where a device cannot verify authenticity of updates itself (e.g. due to no cryptographic capabilities), only a local update by a physically present user is permitted and is their responsibility.
		2.4.5.35	An end-of-life policy shall be published which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to users and an update should be easy to implement.
		2.4.5.36	Where possible Software updates should be pushed for a period appropriate to the device. This period shall be made clear to a user when supplying the device. The supply chain partners should inform the user that an update is required.
	Device Interfaces	2.4.7.7	If a connection requires a password, passcode, or passkey for connection authentication, the factory issued or reset password is unique to each device. Examples are Wi-Fi access passwords and Bluetooth PINS.
		2.4.7.9	Where a wireless interface has an initial pairing process, the passkeys are changed from the factory issued, or reset password prior to providing normal service.
	Authentication and Authorisation	2.4.8.3	Where a user interface password is used for login authentication, the factory issued or reset password is unique to each device in the product family. If a password-less authentication is used the same principles of uniqueness apply
		2.4.8.4	The product does not accept the use of null or blank passwords.
		2.4.8.5	The product will not allow new passwords containing the user account name with which the user account is associated.
		2.4.8.6	Password entry follows industry standard practice such recommendations of the 3GPP TS33.117 Password policy. [ref. 17] or NIST SP800-63b [ref 26] or NCSC [Ref 48] on password length, characters from the groupings and special characters.
		2.4.8.13	The product supports having any or all of the factory default user login passwords altered when installed or commissioned.
	Web User Interface	2.4.10.4	Where a web user interface password is used for login authentication, the initial password or factory reset password is

			unique to each device in the product family.
	Mobile Application	2.4.11.1	Where an application's user interface password is used for login authentication, the initial password or factory reset password is unique to each device in the product family.
		2.4.11.2	Password entry follows industry standard practice such recommendations of the 3GPP TS33.117 Password policy. [ref. 17] or NIST SP800-63b [ref 26]

Summary of Proposed Scheme requirements by IoTSF CF Applicability Group

IoT SF CF Applicability Group	Total IoTSF CF Group requirements	Comments / Notes
Business Security Process and Responsibility	8 requirements	
Device Hardware and Physical Security	2 requirements	
Device Software	10 requirements	
Device Wired and Wireless Interfaces	2 requirements	
Authentication and Authorisation	5 requirements	
Web User Interface	1 requirements	
Mobile Application	2 requirements	
Total requirements:	**30 requirements for Scheme**	

Evaluation Methodology

Is it clear how each evaluation will be carried out and the skills required by the evaluator?

Since the Basic Self-Certification level is just a verified Certification, the evaluation of the submitted data is not through a Certifying Body. The data submitted will be evaluated by the Scheme's staff with input from its advisors (which include experts providing the training and support to the Certifying Bodies). The questionnaire required for verification is simple to follow and complete both from the self-assessment level and beyond, as it consists of a set of questions set out for each level.

Legal Framework

The Scheme is not expected to support demonstration of conformance to any standard or legal requirement, although it does support a number of the requirements of the IoTSF Compliance Framework which meet the top 3 CoPR guidelines.

About the Company

The following sub-sections provide information about the company behind the proposed Scheme.

Company details

The IASME Consortium Ltd, Wyche Innovation Centre, Walwyn Road, Malvern WR13 6PL, was formed on 4 January 2012, the Company number is 07897132.

The first certification it became an accreditation body for was Cyber Essentials in 2014; it did so along with its own IASME Security Management Certification. It promotes both certifications and offers discounts for taking up both.

The Consortium was the first accreditation body to offer free Cyber Insurance for any business completing Cyber Essentials in 2015 where the premium for the cover is organised by IASME, a local insurance broker and one of the largest UK SME insurers.

Since its first assessment service, it has created and provided the following: a GDPR Readiness certificate, as well as specific Cyber Essentials assessments for the Health Sector and Defence requirements for Cyber Essentials. Given these specialisms, the Consortium has shown itself to be able to not only develop accreditation Schemes but also to identify specialist niches that can be offered for those who may not have fitted into the traditional profile of a small business. This means that it can identify additional market niches for compliance assessment products to support widespread coverage.

All assessments offered by the company are security assessments focusing on small organisations (not just businesses), and it works with others to provide services for this target size.

Facts and figures about IASME and certification

IASME worked closely with the UK's National Cyber Security Centre (NCSC) to develop Cyber Essentials since 2013 when we contributed to writing the first technical requirements document. IASME became an Accreditation Body (AB) at the start of the Cyber Essentials Scheme in 2014 and now licences to more than 170 Certification Bodies. IASME holds the largest market share, more than 40%, of all Cyber Essentials certifications issued. Since the Scheme started, IASME has issued

more than 8,000 certificates and now certifies between 400 and 500 companies a month to Cyber Essentials, Cyber Essentials PLUS and roughly 20% of those certify to the wider IASME Governance including GDPR certification.

Training and Development of assessors

The Scheme Proposer is currently working on the training plans for the assessors and Certification Bodies. The training course, which all assessors will need to attend and pass will be 1 or 2 days long and expected to be accredited to the GCHQ Certified Training Scheme. There will be some pre-requisites in terms of experience, which people must already have before attending the course but are yet to be finalised.

Once an assessor is trained, it is likely that the company they work for, the Certification Body, will need to achieve Cyber Essentials and also either ISO27001 or IASME Governance Gold.

The assessor will then have to attend a meet-up at least once a year where any changes or updates are described and some update training takes place. They will have to do refresher training once every 3 years. In between there will be monthly webinars run by IASME and all of them will be members of a Yammer group where they can discuss issues.

Certification Scheme

Initially, the IoT Security assessment will be similar to the basic level Cyber Essentials assessment. It will be an on-line assessment where the client only answers the questions and a board member signs to confirm the answers are all true. No further evidence is needed. The assessor marks each answer according to the mark Scheme developed by IASME and their experience.

Assessor skills

The Scheme Proposer has provided its policy for Assessor Requirements, the core parts of which are attached as Appendix A. In addition to the requirements in the Policy, assessors must complete a one day training course and achieve certification for their company to IASME Governance Gold standard.

For the IoT assessment proposed by this Scheme, further knowledge and skills will be provided by the IoT Assessor Training course (details below) with ongoing professional development and support provided by the IASME team (also detailed below). Due to the baseline knowledge already verified, the IoT assessors will not be expected to achieve a further level of experience or hold a particular qualification before being allowed to take the training course.

Training course for Certifying Bodies

The IoT training course for assessors is expected to be a one-day in-person course, which will be developed and run by an IASME contractor who is an IoT security expert and who lecturers on the subject. The course is expected to cover:

- Introduction the world of IoT
- How the IASME IoT standard relates to Cyber Essentials
- Differences between company and product-focussed assessment

- Key issues of IoT device/service security and how they differ to corporate security
- Examples of IoT devices
- Example scenarios
- Marking the assessment hands-on
- Assessment exam

Candidates will be required to pass the assessment exam, which will be marked by the course tutor, in order to become an IoT assessor.

IASME Team

Once a candidate has passed the training, IoT assessors' ongoing development will be provided by the IASME team through interactive webinars and regular meetings of all Certification Bodies. Ongoing support will be provided during office hours by telephone; email and Yammer (secure internal social media). The IASME admin team handle incoming calls and pass to the IASME technical team as needed. The technical team consists of the CTO and the Technical Operations Manager supported by an IASME contractor who is an IoT security expert. The CTO has 10 years' experience in information security/forensics, is an ISO27001 Lead Auditor, and holds CISSP and ethical hacking qualifications. The Technical Operations Manager has over 15 years' experience of enterprise IT systems and support as well as substantial security experience. The IASME contractor will be used to escalate complex queries. Both the CTO and Technical Operations Manager will also complete IoTSF IoT Security Training.

In accordance with the other standards operated by IASME, the moderator will have the final say on whether an assessment is a pass or a fail. The moderator will draw on knowledge from the team and can engage other external experts, if needed to come to a final conclusion. Any complaints or appeals about marking will be handled through the standard IASME complaints and appeals processes, which have been developed through IASME's operation of the Cyber Essentials and IASME Governance certification Schemes over the past five years.

Assessment process

The assessment process for the Scheme will be identical to that followed for existing assessments (Cyber Essentials and IASME Governance self-assessment). Prospective customers can take two routes to assessment:

- Contact IASME directly through the IASME website: customers sign up online and make payment for the assessment, they are then granted access to IASME's central assessment online portal where they answer the questions and then submit their answers for assessment.

- Approach a Certification Body directly: customers can approach a Certification Body for guidance on how to improve their IoT security and can then get certified directly through the Certification Body. Again, customers will be granted access to the central assessment online portal to enter their answers. In this route, customers are invoiced by the Certification Body for the assessment.

Once the answers are submitted by the customer, in both routes an IoT assessor will mark the assessment using the online portal (asking for support and guidance from the IASME team as needed). Once the assessment is marked, the customer receives an email asking them to log into the portal. Once logged in they will find out if they have passed or failed.

If they pass, they can download a PDF certificate for the assessment and review a feedback form to see any assessor comments showing any opportunities for improvement

If they fail, they can review a feedback form showing any failures and detailing the improvements needed to achieve the relevant control. On failure, customers are given a 48-hour period to resubmit their assessment for a free re-mark. Our experience has shown that most customers fail due to misunderstanding a question or two, so this is an important opportunity to address minor issues.

As mentioned above, there is an appeals process, which includes getting a second assessor to re-mark an assessment, in the event of a query where and escalation to the moderator as needed. In addition, 2% of all assessments will be reviewed by the moderator with feedback to the relevant assessor to ensure consistency of marking and identify any knowledge gaps.

Consideration

Are there any notable gaps or recommendations to improve the Scheme?

As stated above, this Scheme has been modelled on the experience of the established Cyber Essentials Scheme, which the Proposer has been running as an Accreditation Body for several years and is considered to be the current market leader. There are no notable gaps, which need to be highlighted for this report.

Other comments from inspector

Evidential documents provided includes:

- A spreadsheet of the Assessment questions for the marking Scheme.
- A document of the requirements for Assessors
- Emails providing information on the Scheme operations.

Recommendation

It is the view of the Scheme Inspector that this Scheme be recommended based on the following considerations:

- The Scheme Proposer has an existing background and several years of experience in operating similar related schemes.
- There is an existing network of Certifying Bodies who are interested in getting trained to provide the assessments offered by this Scheme.
- The Proposer has an established support network at all levels to ensure it is able to pick up and respond to any early stage issues that may arise.
- The process of on-boarding new Certifying Bodies is already well established to respond to any growth rates the Proposer may experience.
- The Scheme will compile and maintain a complete searchable list of Certification Bodies able to carry out assessments, as it does currently with other Certifications.
- The Scheme will Compile and maintain a complete, searchable list of products that have achieved the required level of certification with all necessary details (customer, product, date, etc.), as it does currently with other Certifications.
- The Scheme provides three levels of assessment and all levels as a whole support the mission of the IoTSF “Helping to arrange assurance processes to demonstrate that IoT products and services meet the requirements of the IoTSF Compliance Framework.”
- The Scheme also provides for an entry-level assessment, which will help stimulate the market in the early stages.

It is the view of the Scheme inspector that this Scheme is fit for purpose.

As the Scheme Inspector, I would recommend that the IoTSF adopt this proposed Scheme within its Assurance Program.

Appendix A: Scheme Assessor Requirements

1. IASME and CE Assessor Requirements

IASME requires that anyone who applies to become an IASME assessor to offer Cyber Essentials and/or IASME Governance assessment to clients must meet a certain level of skill and experience.

This is usually demonstrated by meeting all of the following requirements:

- Have at least 3 years' experience in information technology or cyber security
- Hold at least one of the following security qualifications or memberships:
    - ISC2 Certified Information Systems Security Professional (CISSP)
    - ISACA Certified Information Security Manager (CISM)
    - ISO27001 Lead Auditor
    - CompTIA Advanced Security Practitioner (CASP+)
    - Certified Professional (CCP) scheme – either SIRA, IA Auditor or IA Architect roles at any level
    - Full member of Institute of Information Security Professionals (IISP)
- Attend the IASME Assessor training course (currently two days) including completing the practical exercises that form part of the training

Assessors who wish to certify their company as a Certification Body must also complete a pairing-up process where they assess another trainee assessor's company to the IASME Governance Gold audited standard. This process is moderated and the assessors audit report must pass the moderation before the company can become an authorised Certification Body. Assessors who are already working for a Certification Body do not need to complete this process.

2. CE+ Assessor requirements

IASME requires that anyone who applies to become a CE+ assessor to offer Cyber Essentials Plus assessment to clients must meet a certain level of skill and experience.

This can be demonstrated by either one of two options:

Option 1: Fully qualified and experienced technical assessors

This option is for those with experience and skill in vulnerability assessment of penetration testing.

Assessors using these options must:

- Have at least 3 years' experience in information technology or cyber security
- Hold at least one of the following technical assessment qualifications or memberships:

- Certified Ethical Hacker (CEH) - GCHQ-certified
- Offensive Security Certified Professional (OSCP) - GCHQ-certified
- Tranchulas Certified Penetration Testing Professional (CPTP) - GCHQ-certified
- 7Safe Certified Security Testing Associate (CSTA) - GCHQ-certified
- Learning Tree Penetration Testing Training - GCHQ-certified
- QA Advanced Infrastructure Hacking training - GCHQ-certified
- CompTIA PenTest+
- CREST Registered Penetration Tester
- CREST Certified Infrastructure Tester
- TigerScheme CHECK Team Member (CTM/QSTM)
- TigerScheme CHECK Team Leader (CTL/SST)
- Cyber Scheme Team Member (CSTM)
- Cyber Scheme Team Leader (CSTL)

• Attend the one-day Cyber Essentials Plus Procedures training course and complete the course exam successfully

Option 2: Assessors requiring technical assessment training

This option is for technically competent people who will need additional training to understand how to carry out vulnerability testing for CE+.

Assessors using these options must:

• Have at least 3 years' experience in information technology or cyber security

• Hold at least one of the following security qualifications or memberships:

- ISC2 Certified Information Systems Security Professional (CISSP)
- ISACA Certified Information Security Manager (CISM)
- ISO27001 Lead Auditor
- CompTIA Advanced Security Practitioner (CASP+)
- Certified Professional (CCP) scheme – either SIRA, IA Auditor or IA Architect roles at any level
- Full member of Institute of Information Security Professionals (IISP)

• Attend the two-day Technical Cyber Auditing training course and complete the course exam successfully

• Attend the one-day Cyber Essentials Plus Procedures training course and complete the course exam successfully

3. Equivalent Qualifications and Skills

IASME wants to ensure that the assessor role is accessible to all competent and appropriately skilled people. We recognise that some candidates will hold qualifications or have relevant experience that can be used to demonstrate equivalency to our requirements. In this situation, IASME will consider each candidate on an individual basis, and will be guided by the principles below:

• There should be a competent third party, who can verify the candidate's claim of holding the appropriate skills. A competent third-parties would include: membership organisations that specialises in IT or information security, vendor owned or sponsored certification schemes, national-government certification schemes, any Cyber Essentials Accreditation Body, IASME Certification bodies (excluding the candidate's own organisation)

• The third party (or multiple third parties) should be able to verify that the candidate is able to meet the majority of the skills listed below, based on the IISP Skills Framework:

Skill Set	Description	Level
A	Information Security Management	2
B	Information Risk Management	2
C	Implementing Secure Systems	1
D	Information Assurance Methodologies and Testing	2
E	Operational Security Management	2
F	Incident Management	2
G	Audit, Assurance & Review	2
H	Business Continuity Management	2
I	Information Systems Research	1
J	Soft Skills	2

• Where a third party cannot verify certain skills, the candidate may provide evidence of such skills being obtained through experience either in a current or previous role (including volunteering or unpaid work). It is up to the candidate to provide sufficient evident to IASME to demonstrate this experience beyond reasonable doubt.

• Where a candidate falls short of the required skills in a small number of areas, IASME may ask a candidate to commit to an undertaking to learn certain skills before allowing the candidate to attend the Assessor Training.

• IASME will make the final decision on the suitability of candidates who are attempting to demonstrate equivalent skills.

3.1. Examples

• Abby has 7 years' experience of working hands-on providing advice to companies as a consultant with a cyber security company. She has attained the EC Council's Certified Ethical Hacker (CEH) certification, which allows her to demonstrate her understanding of risks, threats, incident response and how to improve security. Abby's current role requires her to review companies against security standards and to manage the internal risk management process. Abby is able to demonstrate this experience to IASME's satisfaction. Abby is accepted onto the Assessor Training course

• Mohammed has worked for 8 years in an IT role within a managed services company where he implements new systems and manages technical incidents, which often lead to making improvements to business systems and processes. He has a Cisco CCNA certification, which shows his understanding of network technologies. Mohammed is not able to demonstrate experience of implementing security policy or processes, or of managing security risks. Mohammed is not accepted onto the Assessor Training course until he can demonstrate experience or qualifications relating to these skills.