Comparing the Cyber Essentials and IASME Governance Standards

What are the Benefits of Security Certification

- Gaining certification reassures customers that organisation is following a defined level of cyber security which protects their data.
- Badge that can be used on websites and marketing material demonstrating certification
- With IASME Governance certification comes Automatic Cyber Essentials Certification
- Cyber liability insurance for UK domiciled organisations with less than £20m turnover who pass the assessment (terms apply)

Comparing the Cyber Essentials and IASME Governance Standards

Cyber Essentials	IASME Governance
The Cyber Essentials scheme has been developed by UK Government and industry to fulfil two functions • providing a clear statement of the basic controls organisations should implement to mitigate the risk from common internet based threats • provide certification to enable organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions. Cyber Essentials defines a set of controls which, when properly implemented, will provide organisations with basic protection from the most prevalent forms of threats coming from the Internet. It focuses on threats which require low levels of attacker skill, and which are widely available online. The scheme considers these threats to be: • phishing — and other ways of tricking users into installing or executing a malicious application • hacking — exploiting known vulnerabilities in Internet-connected devices, using widely available tools and techniques • password guessing — manual or automated attempts to log on from the Internet, by guessing passwords Risk management is the fundamental starting point for organisations when acting to protect their information. However, given the nature of the threat, Government believes that action should begin with a core set of security controls which all organisations – large and small – should implement. Cyber Essentials defines what these controls are. Government believes that implementing these measures can significantly reduce an organisation's vulnerability. However, it does not offer a silver bullet to remove all cyber security risk; for example, it is not designed to address more advanced, targeted attacks and hence organisations facing these threats will need to implement additional measures as part of their security strategy. What Cyber Essentials does do is define a focused set of controls which will provide cost effective, basic cyber security for organisations of all sizes.	The Information Assurance for Small to Medium-sized Enterprises (IASME) Governance standard is designed as a security benchmark for SMEs. The IASME Governance standard was developed over several years during a Technology Strategy Board funded project to create a cyber security standard which would be an affordable and achievable alternative to the international standard, ISO27001. IASME is designed to guide SMEs, where needed, and then assess the level of maturity of the SME's information security. IASME is a formal information and cyber security methodology that is suitable for any organisation and SMEs in particular. It is sector agnostic and provides a working framework to assure information security against the background of contemporary threats. IASME comprises clear guidance on good information security practices so a business knows where to start taking security measures. IASME has been established so that businesses can: • Identify risks to their information. • Apply adequate controls to keep that risk at an acceptable level. • Use a self-assessment for the completeness of what they are doing to protect information. • Be independently reviewed by an assessor who will be sympathetic to their size and business risk and verify the effectiveness of what they are doing. • Raise the awareness of information risks in businesses and the wider supply chain of which they may be part. • Give customers, and their supply chain, a level of assurance akin to ISO/IEC 27001 and similar standards. The IASME certification has been updated to include an readiness for the new data protection regulations - EU regulation General Data Protection Regulation(GDPR) or equivalent data protection regulation going through parliament)

Comparing the Cyber Essentials and IASME Governance Standards

<table>
<tr><th>Cyber Essentials</th><th>IASME Governance</th></tr>
<tr><td colspan="2">The security measure covered by the standard</td></tr>
<tr><td>The Cyber Essentials scheme covers only the essential steps to mitigate the threats in scope. It is deliberately prescriptive and is aimed to provide a base level of controls before the business even begins to work with computers and other information technology. The scheme:
• only recognises preventative technical controls
• does not include detective or recovery controls
The scheme requirements do not consider whether a management regime is in place to maintain these protections.</td><td>The IASME standard requires that an organisation has a management regime in place with appropriate controls in the following areas
• Identification of what needs to be secure
• Protection to make it as secure as possible within the risk profile.
• Detection of defects in business processes, accidental or deliberate security incidents and deterrence (of attacks).
• Response and recovery from incidents (in tune with the level of resilience needed by the business).</td></tr>
<tr><th colspan="2">Levels of Certification</th></tr>
<tr><td colspan="2">Self -Assessment</td></tr>
<tr><td colspan="2">The organisation answers questions about how security is managed within their organisation. A board member asserts that the questions have been answered honestly. The questions are marked by an accredited assessor who is a security professional and has been through training and licensed with IASME. To pass certification most questions need to be answered positively.</td></tr>
<tr><td>Cyber Essentials basic
CYBER ESSENTIALS only requires a self-assessment. A vulnerability scan is not required for a basic assessment although other ‘Accreditation Bodies’ may require and charge for such a scan. However, this is not required by the Government and certification through IASME, without a vulnerability scan, is just as valid a Cyber Essentials assessment as any other.</td><td>IASME Self-certified
only requires a self-assessment. Organisationals can optionally choose to answer questions about data protection, their readiness for GDPR. As the Cyber Essentials questions are a subset of the ISAME requirements, organisatons who gain IASME self-certificed also gain an automatic Cyber Essentials Certification.</td></tr>
<tr><td colspan="2">Audited</td></tr>
<tr><td colspan="2">Having passed the basic self-assessment level of chosen certification, organisations can opt to have their responses verified by an independent auditor, providing further proof they are following the requirements of their chosen standard. Organisations are expected to complete audited certification with 3 months of having passed the self-assessment level.
For both certification the assessor will need to visit your head office and a representative sample of your other offices. The number of other offices visited depends on the complexity of your organisation.</td></tr>
<tr><td>Cyber Essentials PLUS
involves a technical audit of the systems that are in-scope for Cyber Essentials. This includes: a representative set of user devices, all internet gateways and all servers with services accessible to unauthenticated internet users. The assessor will test a suitable random sample of these systems (typically around 10 %) and then decide whether further testing is required.
Some tests may be carried out remotely provided that the agreed on-site visits have been carried out.</td><td>IASME Audited.
The documentation and maturity of the organisations security controls will be reviewed by the auditor. The IASME audit does not include a technical audit of systems as required by Cyber Essentials Plus.</td></tr>
<tr><th colspan="2">Validity of Certificates</th></tr>
<tr><td>Cyber Essentials
There is no formal expiry date for Cyber Essentials certificates. Certification demonstrates that the organisation has “in place industry recognised minimum standards” on day of assessment. Cyber Essentials certification does not give any assurance that this security stance will be maintained, or that it will be</td><td>IASME
As the IASME standard requires a Management System in place, the certificates provides more assurance can that the security stance is maintained. Given the evolution of the business which potentially changes risk profile and changing IT ecosystem IASME certifications have expiry dates.</td></tr>
</table>

Comparing the Cyber Essentials and IASME Governance Standards

Cyber Essentials	IASME Governance
robust enough for anything beyond the most basic external internet based risks. Over time the IT ecosystem changes, the technology evolves, the support teams change and the way technology is used changes. For all these reasons, organisations are recommended to recertify at least once a year, and potentially more frequently if customers demand it.	IASME Self-certified is valid for 1 calendar year. IASME Audited certificates are valid for up to 3 years, subject to annual successful self-certified assessments.

Security Controls Explicitly Required

Cycle	Security aspect		Cyber Essentials	IASME
Identify	Planning		NO	YES
	Organisation		NO	YES
	Asset Management		NO	YES
	Assessing risks		NO	YES
	Legal and regulatory Landscape		NO	YES
	People		NO	YES
Protect	Policy realisation		NO	YES
	Physical and environmental protection		NO	YES
	Secure business operations	Firewalls	YES	YES
		Secure Configuration	YES	YES
		Patching	YES	YES
		Operations Management	NO	YES
	Access control		YES	YES
Detect and Defer	Malware and technical intrusion		YES	YES
	Monitoring		NO	YES
Respond and Recover	Backup and restore		NO	YES
	Incident management		NO	YES
	Business continuity, disaster recovery, and resilience		NO	YES

Comparing the Cyber Essentials and IASME Governance Standards

Explicit and implied information and cyber security policies and processes required

Policy Type	Policy	Areas covered	Cyber Essentials	IASME
Asset Management	Intellectual property	How intellectual property should be managed and how to comply with relevant legislation	NO	YES
	Classification of information	How information should be prioritised and marked in terms of risk to the business	NO	YES
	Ownership and responsibilities	Who owns different information and physical assets	NO	YES
	Physical security	Keeping assets safe from physical loss or damage	NO	YES
	Clear desk policy	Ensuring that office environment is regulated and controlled	NO	YES
	Acquisition of hardware, software and services	How such items are evaluated, directed, monitored, accepted and licensed/registered	NO	YES
	Handling and disposal of computer equipment and information assets	Details how to transport and securely dispose of computer equipment, how to handle information assets, and how to securely destroy information	NO	YES
	Media handling	How to store and handle media containing information	NO	YES
	Data sharing and exchange	Regulate which information can be shared and how	NO	YES
People	Governance	Detailing management commitment to policies, governance and organisation of policy, authority for enforcing policies and management review	NO	YES
	Acceptable use of computers	Covering topics such as personal use, BYOD and social media	YES if BYOD	YES
	Data and account access	For permanent staff, temporary staff and contractors detailing new starter data access, data access for leavers, modifications and access privilege review and management	YES	YES
	Data protection	How the business will comply with Data Protection Act	NO	YES
	Remote working	Covering how staff should act when working remotely/teleworking	YES if home workers	YES
	Third-party services	Detailing how agreements are to be set with third parties	NO	YES
	Training and awareness	How training commensurate with roles and responsibilities is provided and end-user guidance to security issues	NO	YES
	Risk management	How risk is assessed, acceptable levels, treatment6, business continuity and resilience including disaster recovery	NO	YES
	Passwords and key management	Management of cryptographic keys and passwords that provide access to information	YES	YES
	Remote access (such as VPN)	Criteria for allowing remote access	YES	YES
	Change Management	New Installations and Change Management Procedures including data quality and integrity, backup and storage	NO	YES
	Incident and event management	How incidents are to be managed including points of escalation and incident logging	NO	YES
	E-commerce and credit card handling	Compliance with e-commerce legislation and credit card standards such as PCI	NO	YES
	Assessment	Auditing of the company including internal and external	NO	YES
	Legal and regulatory compliance	How the company will comply with relevant legislation and regulations	NO	YES
	Architecture	How systems are managed and deployed including data centres, cloud both private and public	NO	YES
Technology	Configuration management	How to keep configuration of systems secure including vulnerability management/ patching	YES	YES
	Internet Connection	Topics relating to internet access, permitted protocols, content filtering, firewall, internet facing services, DMZ, routers and switches	YES	YES
	Communications	How telecoms are managed such as VOIP, wireless communication, mobile phones	NO	YES
	Internal Server Security	What is the appropriate set up for internal servers so that they support the work done with adequate flexibility?	NO	YES
	Mobile devices	Specific requirements for portable devices such as laptop computers, tablets, and portable storage7.	YES	YES
	Protection against malicious software	How the company protects against virus, Trojan, worm, adware and spyware	YES	YES
	Testing	How the Demonstration/Testing/ Sandbox Facility is to be setup and configured	NO	YES
	Monitoring	Topics such as Intrusion detection/prevention, non- repudiation and log management	NO	YES
	Encryption	Management of cryptographic communications	NO	YES