IASME Consortium Ltd - Information Assurance for Small and Medium Enterprises

Introduction

The IASME Consortium Ltd took forward a project which was initially supported by the Technology Strategy Board and has now developed the emerging Information Assurance management standard for SMEs.

What does it do?

Certification to the standard demonstrates that the business is implementing the requirements for effective cyber-security. IASME accreditation demonstrates compliance with international information security management standards.

What does the standard cover?

The standard is openly published on the Consortium website. It is derived from HMG guidance, international standards such as ISO/IEC 27001 and best practice from the EU, USA and other sources. It is correctly sized and priced for smaller businesses in the supply chain and may be achieved through self-assessment or an independently audited approach.

The following table illustrates the requirements of the IASME Standard compared with the requirements of ISO/IEC BS27001:2005.

IASME Category	IASME Requirements	ISO/IEC BS 27001:2005 Annex A: Domains	ISO/IEC BS27001:2005 Requirements
Organisation	Manage information resources within the organisation and in the organisation's relations with partners.	Organization of information security	To manage information security within the organization and to maintain the security of the organization's information and processing facilities that are accessed, processed, communicated to, or managed by external parties.
Risk	Understand and manage the risk to your business information.	[Risk Management is included in the body of the standard]	
Policy	Establish management direction and communications.	Security policy	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
Assets	Know your information assets, and acquire and dispose of them securely.	Asset management	To achieve and maintain appropriate protection of organizational assets.

IASME Category	IASME Requirements	ISO/IEC BS 27001:2005 Annex A: Domains	ISO/IEC BS27001:2005 Requirements
People	Know your people and educate them in business security.	Human resources security	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, are aware of information security threats, and exit an organization or change employment in an orderly manner.
Things	Protect your information assets from physical harm.	Physical and environmental security	To prevent unauthorized physical access, damage and interference to the organization's premises and information. To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.
Technical Security	Defend your information from hostile attack and be ready to recover from infection.	Communications and operations management	To help ensure that information is processed correctly, backed up securely and handled appropriately.
Access	Control who and what can access your information.	Access control	To assist with controlling access to information, networks and applications, preventing unauthorised access, interference, damage and theft.
Planning	Build security and privacy in at the start; make sure you have the right-sized information systems.	Information systems acquisition, development and maintenance	To ensure that security is an integral part of the information system, helping with securing applications, files and reducing vulnerabilities.
Operations	Manage and monitor your information systems effectively.	[Communications and operations management] See above	
Incident management	Ensure breaches of confidentiality, integrity or availability of your systems are detected and dealt with; learn the lessons.	Information security incident management	To ensure information security breaches and issues are communicated consistently, in a manner allowing timely corrective action to be taken.

IASME Category	IASME Requirements	ISO/IEC BS 27001:2005 Annex A: Domains	ISO/IEC BS27001:2005 Requirements
Continuity	Make sure you can recover quickly from partial or total loss of key information assets.	Business continuity management	Business continuity management - To ensure you counteract interruptions to business activities and protect critical business processes from the effects of major information systems failures or disasters
Legal compliance	Know what is required and make sure you comply.	Regulatory compliance	To avoid breaches of any law, statutory, regulatory or contractual obligation, and of any security requirements. To ensure compliance of systems with organizational security policies and standards.

Working with the community

The Consortium is a member of the Malvern Cyber Security Cluster. It gives lectures and seminars, publishes articles and works with universities, the National Fraud Authority, solution providers and others to advise and develop assurance models to meet particular business needs. The Consortium also contributes input to the new PAS 555 security specification being developed by business and the British Standards Institute. The IASME standard will continue to be compliant with these and the CESG emerging requirements. A small number of businesses have already been independently certified and are re-assessed annually.

Continued development

The Consortium will continue to develop the standard in the light of evolving threats and vulnerabilities as they emerge and will continue to develop new ways of supporting business security.

The IASME Consortium Ltd

Registered in England and Wales

Company no. 07897132.

IASME Consortium

www.iasme.co.uk