The IASME Consortium
e-mail: info@iasme.co.uk
web: http://iasme.co.uk/

THE STANDARD FOR INFORMATION ASSURANCE FOR SMALL AND MEDIUM SIZED ENTERPRISES (IASME)

Issue 2.3-2013

Document	IASME Standard
Issue:	2.2
Date:	March 2013
Author:	David A. Booth

Modification History

Revision	Date	Revision Description
1.0	1 April 2011	For issue
1.0e	March 2012	Review
1.1	April 2012	Reissue
1.2	August 2012	Minor additions
2.1	December 2012	Alignment with other standards
2.2	March 2013	Inclusion of social media
2.3	March 2013	Conformance statements

Information contained in this document is believed to be accurate at the time of publication. This document is provided 'as is', without any representation or endorsement made and without warranty of any kind whether express or implied, including but not limited to the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security and accuracy.

We do not warrant that the functions contained in the material will be error free, that defects will be corrected, or that this document represents the full functionality, accuracy, reliability of the materials. In no event will we be liable for any loss or damage including, without limitation, indirect or consequential loss or damage, or any loss or damages whatsoever arising from use or loss of use of, data or profits arising out of or in connection with the use of this document.

Adherence to the Standard does not guarantee security – nothing can.

These Terms and Conditions shall be governed by and construed in accordance with the laws of England and Wales. Any dispute arising under these Terms and Conditions shall be subject to the exclusive jurisdiction of the courts of England and Wales.

Contents

Figures

Tables

Conformance with other standards and guidance

1.1. Conformance with ISO/IEC BS27001:2005 Information Security Management Standard

The principles of the IASME Standard reflect the international standard best practice. The key elements of the international standard can be found in the IASME Standard, e.g. risk assessment, security policy, security organisation, business continuity and so on. Full compliance with the IASME Standard also demonstrates compliance with the international standard.

1.2. Conformance with PAS 555

PAS 555 (in development in early 2013) intends to define all-encompassing good cyber security by providing a framework that enables understanding of the full scope of the capabilities required. Importantly it emphasizes that technical measures alone are not enough – good practice encompasses people and behaviours, physical and equipment security, as well as effective governance, leadership and culture.

The key outcomes of implementing PAS 555 are:

a) investment in cyber security is focused in the most appropriate way;

b) an organization knows what its adversaries are doing;

c) cyber security is managed holistically;

d) the organization is responsive and adaptable.

These outcomes can, in turn, result in:

- improved stakeholder **confidence and trust**;
- increased likelihood of **achieving objectives**;
- **enhanced business reputation** and competitive advantage

1.3. Conformance with the CESG 10 Steps to Cyber Security

The IASME Standard reflects the measures contained in the 10 Steps to Cyber Security. Guidance for SMEs for implementing these controls can be found on the IASME website.

1.4. Conformance with the CPNI/SANS 20 Critical Controls for Cyber Defence

The IASME Standard reflects the measures contained in the 20 Critical Controls for Cyber Defence. Guidance for SMEs can be found on the IASME website.

1. Introduction

Information is an organisation's most valuable asset. However, it is often neglected in favour of protecting material assets, maintaining cash flow and the like, when considering the organisation's long-term future. This is often because assigning a value to information is seen as much more difficult than valuing buildings, stock, people, and the other more tangible assets in an organisation.

There are methods of providing assurance of the protection of information. The most prominent and internationally recognised method or framework is certification to the international information security standard BS ISO/IEC 27001. Many organisations throughout the world use this to provide assurance to themselves, their supply chain partners, and customers that information is well protected. Unfortunately, the process to establish and certify an information security management system to the ISO/IEC 27001 standard is often perceived to be too complex, time-consuming, and expensive for smaller organisations.

Smaller, dynamic businesses and organisations differ from their larger, more structured counterparts in a number of ways when considering information security. Research and investigation during the development of this standard found that SMEs are extremely sensitive to cost, need simple processes over heavily structured ones, and prefer an informal culture over a more structured organisation.

Information Assurance for Small to Medium-sized Enterprises (IASME) is intended to provide the SME with an assessment and recognition of the level of maturity of the protection of the business information that can be used to assure themselves and others in accordance with their business needs. The process is based on international standards and EU guidance and is simple, quick and cost effective. IASME certification stands a business in good stead if it wishes to progress to certification to other standards. This standard maintains a close relationship with other international standards and guidance.

1.5. End to End Assurance

The IASME process differs from most standards in that it is outcome centric and aims to manage the quality of implementation from start to finish. To achieve this it:

- carries out cyber security research and development,
- updates the standard in the light of evolving threats
- sets the criteria for training and certification of the IASME Assessor
- has well defined and transparent implementation and business processes and
- publishes an open set of requirements needed to achieve IASME assurance.

The standard is couched in business language rather than cyber-speak so that business, suppliers and partners can understand and recognise the business benefits of achieving the standard. This encourages confidence in the standard within business and government.

1.6. Continuous Development

Although developed for the smaller business, the process is now scalable to any size business. The IASME organisation continually monitors developments in the rapidly changing cyber security ecosystem and adjusts the assurance criteria accordingly. In this it is assisted by a group of businesses interested in the development of the standard. The Consortium also works with other service providers to develop the IASME concepts for use in specific business contexts.

2. How IASME works

IASME applies a balanced set of controls to all types of business and adjusts their implementation in relation to a *business risk profile*.

2.1. Continuous Assessment

The process involves continuous assessment, starting with the initial cycle leading to the first certification, and continuing with intermediate assessments annually and re-assessment after three years.

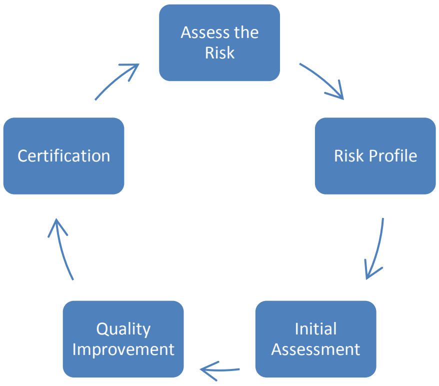


Figure 1: Continuous assessment

IASME expects a set of documentation that is right-sized for the organisation. This includes a security policy statement, a business continuity plan and a simple senior-level endorsement and management plan. These will be individual and customised to what you do. However, if you need a starting point, IASME will give you templates to work on. The documentation shows commitment at the top level, clear accountability and responsibility, and a benchmark for your certification.

Risk is assessed and your security controls are weighted in a balanced scorecard. How well you apply the security controls is measured in terms of maturity. The IASME process is documented, objective, and repeatable while retaining flexibility and scalability.

2.2. Continuous Adjustment

Controls are the practical measures that you put in place to protect your information. Each control addresses one or more aspects of information security detection, prevention, or recovery. Controls are selected based on the risk to your business and **not** the size of the business. Adjustments can be made at any time as the risk changes.

Businesses who have successfully completed their first assessment are re-assessed at least annually, or at any time the risk to their business has changed.

3. Business Process Effectiveness

There is a common set of factors to be considered when assessing the effectiveness of an organisation's business, which are summarised below. These are much the same as those for cyber security, which is most cost effective when considered to be part of the business.

Organisation

Manage information resources within the organisation and in the organisation’s relations with partners.

Risk

Understand and manage the risk to your business information.

Policy and Compliance

Establish legal and regulatory requirements, management direction and communications. Know what is required and monitor compliance

Assets

Know the value of your information assets, and acquire and dispose of them securely.

Planning

Build security and privacy in at the start; make sure you have the right-sized information systems.

Access

Control who and what can access your information.

People

Know your people and educate them in business security.

Physical and Environmental

Protect your information assets from physical and environmental harm.

Disruption

Defend your information from hostile attack and be ready to recover from the effects.

Operations

Manage and monitor your information systems effectively.

Incident management

Ensure breaches of confidentiality, integrity or availability of your systems are detected and dealt with; learn the lessons.

Continuity

Make sure you can recover quickly from partial or total loss of key information assets.

Table 1: Business Security Factors

4. Cyber Security Investment

Investment in cyber security falls into three main categories: Protection, Detection and Recovery. Typically, most investment is made in the Protection category (organisation, training, asset management, firewall etc.), but it may be possible to reduce investment in Protection by increasing investment in Detection (intruder detection, anti-malware, asset monitoring, activity monitoring etc.) or Recovery (backup/restore, disaster recovery etc.). A full impact analysis would be required before taking such investment decisions; but generally investment is required in all three.

There is no complete distinction between protection, detection and recovery measures. Many protection measures have elements of detection and may assist recovery; some recovery measures may lead to better protection and so on. Here they are organised by their main impact on cyber security.

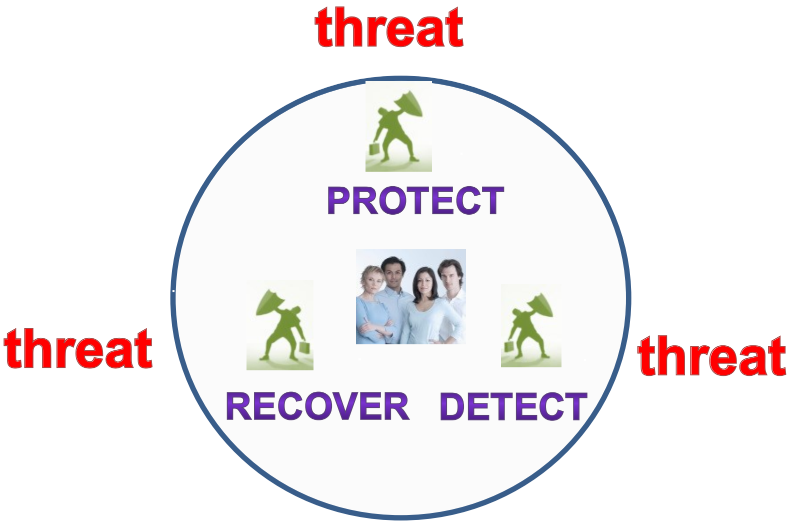


Figure 2: cyber security investment

PROTECTION

Investment in Protection overlaps with Detection and Recovery and includes

- the part of your organisation (one or more people) responsible for ensuring that your cyber security happens, both within your organisation and in relationship with your partners,
- planning security in when developing your business
- the assessment of risk to your information assets and how much of it you want to manage,
- recording your policy on how you want to manage cyber security so everyone knows
- identifying and recording at least your most important information assets (hardware, software, communications, data etc.)
- ensuring people have access to what they need but not to what they don't need (this reduces the impact of any potential data breach)
- educating your people in good security behaviour (things to do and things not to do)
- investing in good physical and environmental protection for your assets (e.g. door locks and air conditioning if needed)
- investing in good technical protection (anti-malware, firewalls, software patching etc.)

4.1. Organisation

Objectives

Security organisation	To manage information assurance within the organisation and in the organisation's relations with partners To keep abreast of emerging threats and countermeasures

Essential steps in protecting the business involve:

a. Ensuring commitment and funding agreement from the top of the organisation
b. Appointing a senior, well informed person – often referred to as Chief Information Officer and/or Risk Owner – who will lead. [1]
c. Forming a group from across the organisation to coordinate and implement activities. [2]
d. Maintain knowledge of emerging threats and countermeasures using expert advice.

Whenever possible existing posts and organisational groups should be given these responsibilities to keep impact and costs to a minimum.

4.2. Assessing the risk

Objectives

Risk assessment and management	To understand the information risk to the organisation and provide information assurance to the business To consider information risk in the business context To determine the business risk appetite To manage the risk in accordance with the risk appetite To demonstrate appropriate risk management to partners and suppliers

The next step is to identify the threats to the organisation and assess the resulting risk. Current threat assessments are listed at Annex A.

The applicability of the controls to your business is determined partly by a risk assessment and partly by your risk appetite. IASME knows that too few SMEs have a formal information risk assessment, nor a business risk assessment of any kind. However, they do have a keen sense of the risks and frailty of their business at board

[1] If the IT Manager is appointed to this post they will need training and qualification in the non-IT aspects and sufficient authority across the organisation. In a micro organisation a director is usually appropriate.

[2] In a micro organisation this can be extremely informal; larger organisations may require a more formal structure.

level. IASME assesses this knowledge using a simple questionnaire based on best practice like those from the European Network and Information Security Agency (ENISA).

Risk assessment is often one of the most complex, time consuming (and therefore expensive) parts of other methodologies and is the starting point for most information assurance processes. However, most organisations are exposed to a common set of business information risks. The IASME risk profiling process recognises this and asks questions in several categories which put information security in a business context, and in a form which the business will be able to answer fully. Some of the questions also give an insight into the people, physical, and technical business management factors that might be already in place and how much risk you want to take.

The questions are followed up by the assessor in an interview with the person who has formal responsibility for information assets in the business and the person(s) responsible for implementation.

The assessor is typically qualified and experienced in information security and trained in the application of the IASME processes. The decisions of the assessor are checked by a moderator who will have considerable experience in this field.

Further information can be found at Annex C.

4.3. Policy and Compliance

Objectives

Security policy and Compliance with legal, statutory, regulatory and contractual obligations and security requirements	To provide management direction and support for information security in accordance with business requirements To identify the organisation’s legal, statutory, regulatory and contractual obligations and security requirements for the use of information, intellectual property rights and legal use of software and other products To ensure that organisational records are protected from loss, destruction or falsification in accordance with the organisation’s legal and other obligations To prevent or deter the use of an organisation's information systems from misuse. To ensure compliance of information systems with organisational policies and standards. To ensure that system audits are effective and minimise impact on the business To limit access to audit tools and audit information

In order to support the management and development of the organisation’s security profile, the organisation requires a Security Policy. This is the ultimate responsibility of the CIO/Director.

IASME provides a model template policy which is appropriate for most organisations. This contains not only the essential investments necessary to keep the organisation as safe as possible, but also identifies responsibilities and embeds a light-weight management cycle.

Dates for achieving objectives can be set within the policy, which should be reviewed by the Board at regular intervals.

4.4. Assets

Objectives

Asset management and planning	To consider security in the acquisition and through-life management of assets To achieve and maintain appropriate protection of information assets To maintain a record of key organisational assets To ensure information security when using Public or Private Cloud assets To ensure information security when using personal mobile computing To ensure information security when remote working To dispose of assets securely

One of the key factors in both risk assessment and recovery from a cyber security incident is a good understanding of your key information assets. Clearly, the impact of any security incident will be most severe if it happens to the assets which keep the organisation going. Further, if the worst happens, the organisation will know which assets to recover first.

Often overlooked is the disposal of assets, particularly hard disks. It could be expensive or embarrassing (or both) if your organisation’s information was accidently given away with your old computers. This also applies to USB sticks or indeed any recordable media.

Particular issues arise when using cloud or personally owned assets for the business and these are particularly important when assessing compliance to the IASME Standard.

4.4.1. Cloud Assets

Cloud computing comes in many shapes and sizes, offering a variety of services, typically data storage, applications provision and many others. They may be privately owned by the business or publicly provided by re-sellers. From the cyber security viewpoint the main differences are the degree of risk to the organisation versus business benefit.

4.4.1.1. Public/Commercial Cloud

Public Cloud assets should be regarded as any other out-sourced asset particularly if the organisation relies entirely on data storage and/or application services from a public cloud provider. The organisation should ensure that the provider offers good evidence of confidentiality, integrity and availability, and should not rely on insurance or other indemnity unless it would fully compensate for any loss of business or reputation in the event of failure. There are also potential legal threats relating to the geographical location of the Public cloud servers storing organisational data.

4.4.1.2. Social Media

Social media (Facebook, Twitter, LinkedIn etc.) are varieties of public cloud and should be treated in the same way. Social media may be used for business purposes on condition that no sensitive or potentially sensitive material, IP or similar material is disclosed. Users must behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company

4.4.1.3. Private/In-House Cloud

Private cloud can offer many of the advantages of Public cloud, but have a management overhead. However, the organisation should obtain direct evidence of confidentiality, integrity and availability and avoid the potential legal aspects of Public cloud storage.

4.4.2. BYOD Assets

BYOD (Bring your own device) has become popular in the last few years, largely because the technological advances of portable devices has out-stripped the IT resources provided by the average organisation.

Threats presented by the use of personal, portable devices for business purposes include loss/compromise of business documents (including email) which become resident on the device and introduction of malware to business systems.

Organisations should ensure that the devices have corporate-level protection, detection and recovery processes in place and that users follow the business security procedures at all times. Other threats are likely to emerge as devices become more sophisticated, and organisations should ensure that their defences remain adequate by taking expert advice regularly.

The template IASME Policy includes asset management and disposal procedures and the Assessor will help to identify the important assets if required.

4.5. People

Objectives

Personnel security	To establish user responsibilities to prevent compromise or theft of information and information assets and that user security privileges reflect business need. To ensure that all employees • Are suitable from a security viewpoint before and during employment. • Are aware of, and adequately trained in, their security responsibilities • Are aware of current threats, including those arising from manipulation of social media, infected websites, use of personal devices and others • Are suitably debriefed and privileges removed on termination of employment.

In most organisations, people are the cyber security front line protection. It is important therefore to ensure that you know as much about them as possible before you employ them. This is usually done by taking up references, and in certain cases through formal vetting procedures.

It is essential that new employees are given a briefing on their corporate and security responsibilities before, or immediately after employment, preferably reinforced by reference literature.

Employee contracts should also include security obligations and reminders should take place at regular intervals. Employees with special responsibility for security, or with privileged access to business systems should be adequately trained/qualified as appropriate.

On termination of employment, user access privileges should be immediately withdrawn and the employee de-briefed on their post-employment confidentiality responsibilities.

4.6. Physical and Environmental Protection

Objectives

Physical and environmental security	To prevent: • Unauthorised physical access, damage and interference to the organisation's assets and information. • Loss, damage, theft or compromise of assets which might interrupt the organisation's activities. • Loss of environmental control which might affect availability.

Protection of an organisation's cyber security extends to the physical protection of information assets, to prevent theft, loss or damage. Usually this is no more than the common sense approach to door locks, window bars, video surveillance and so on, as dictated by the organisation's physical environment. However, in some cases, physical protection may be dictated by HMG or legal requirements.

Most modern computer and communications equipment does not require particular environmental protection such as air conditioning or water chilling, however it is important that any such devices are properly maintained including any necessary fire suppressant systems.

4.7. Operations and Management

Objectives

Operations and Management	To ensure optimum and secure operation of information systems by e.g. patching To implement and maintain appropriate and agreed levels of security and service delivery with third parties To maintain the security of electronic commerce services

One of the most effective technical security protection measures is to ensure that software and operating systems are updated with the latest patches from the suppliers.

Service level agreements with third parties who provide all or part of the organisations operating capability (particularly Cloud providers, see above) are likely to be essential to the business. These agreements should be examined carefully to ensure that they offer sufficient protection from risk to the business.

Electronic credit card transactions are regulated by PCI-DSS. Compliance with these regulations is likely to be essential to the business which have this in their business model.

4.8. Access Control

Objectives

Access to information	To control access to system files and source code To ensure access by authorised users and prevent access by unauthorised users To prevent unauthorised access to internal and external networked services To prevent unauthorised access to operating systems' facilities To prevent unauthorised access to information held in applications systems

Users should be given access to all the data necessary for their duties, but no more (sometimes referred to as 'least privilege'). Although most access would be user initiated, in some cases autonomous applications with user privileges may be employed.

There are certain types of data which are likely to be critical to the smooth functioning of information systems such as system files, software source code, parts of the operating system or database systems where deliberate of accidental damage could cause significant disruption.

Detection

Investment in Detection overlaps with Protection and Recovery and includes

- detection of malware and intrusion
- monitoring information systems for unauthorised activity

4.9. Malware and technical intrusion

Objectives

Prevention and detection of malware and intrusion/extrusion	To detect and protect systems and information from malicious software To recover from the effects of malware To detect unauthorised intrusion and extrusion.

Malware is intended by its perpetrators to affect the targets data confidentiality, integrity or availability, generally with the aim of obtaining intelligence or saleable information, blackmail, disrupting facilities, political attack and a variety of other vectors. The size of the target organisation is often not relevant to the attacker, except insofar as a smaller organisation may be less well protected and so, for example, would provide a route into a more valuable target in the supply chain.

Malware is often used in conjunction with other attack vectors such as 'phishing' and social network sites to provide a focussed attack vector, but techniques are constantly evolving and becoming unpredictable.

Anti-malware solutions are available from commercial suppliers, some free, but usually as complete software and support packages. Malware formats are continually evolving, so it is important that the supplier includes both malware signatures and heuristic detection facilities which are supported by research and updated as frequently as possible.

Some packages include automatic validation of websites so that some assurance can be provided that the site is genuine and uninfected with malware, but care should be taken nonetheless.

There are a number of commonly deployed intrusion and extrusion solutions, including firewalls and to a lesser extent ‘honey traps’. It is important that firewalls are deployed at the technical boundaries of the organisation and are correctly configured to detect and prevent unauthorised intrusion and extrusion of data. Honey traps can be set within the network boundaries to provide additional detection facilities; typically these have no protection capability.

4.10. Monitoring

Objectives

Network Monitoring	To detect unauthorised information processing by accounting and audit of activities

Most operating systems include logging of various forms of activity on the networks. Where necessary and appropriate, these logs should be monitored for evidence of unauthorised activity. Employees should consent to regular monitoring of their business-related activities.

Recovery

No security measures can be fully effective all the time, so investment in Recovery is essential.

4.11. Backup and Restore

Objectives

Backup and Restore	To maintain the integrity and availability of information and information processing facilities by backup and restore capability

Key information should be backed up regularly and the backups preferably kept in a secure location away from the business premises. Restores should be tested regularly in order to test the performance of the backup regime.

4.12. Incident management

Objectives

Security Incident Management	To ensure that information security events and weaknesses associated with information systems are identified and reported within agreed timeframes To ensure that responsibilities are identified and communicated To ensure that procedures to manage the different forms of incident are in place, effective and communicated To ensure that contingency measures are in place to manage any loss of business effectiveness as a result of an incident and to ensure effective recovery processes are in place (c.f. Business Continuity Management) To ensure that audit trails and similar records are in place to assist with containment and analysis of the incident and that forensic procedures are used where appropriate To analyse, report and learn from incidents

Ensure breaches of confidentiality, integrity or availability of your systems are detected and dealt with; learn the lessons.

4.13. Disaster Recovery/Business Continuity

Objectives

Recover and Continuity Management	To identify critical vulnerabilities of information systems which may impact integrity or availability to the detriment of the business To protect critical business processes from the effects of major failures of information systems To ensure there are joined up organisational and business unit level plans to counteract and recover from loss of integrity or availability of information systems within agreed time-frames To ensure that responsibilities are identified and plans are updated and exercised regularly To ensure that confidentiality of information is retained during a failure of an information system and subsequent recovery

Disaster recovery and business continuity are terms which have similar outcomes, that is to maintain business as usual in the event of physical or technical events which would materially affect organisational objectives.

Plans for the management of such events should be drawn up and reviewed regularly, and tested in whole or in part so that participants in the plan understand their responsibilities.

Annex A: CyberSpace Security Threats

The organisation should keep abreast of current and evolving threats to their information. Some sources are listed below.

A. ISO/IEC 27032:2012(E) First edition 2012-07-15 (Section 9)

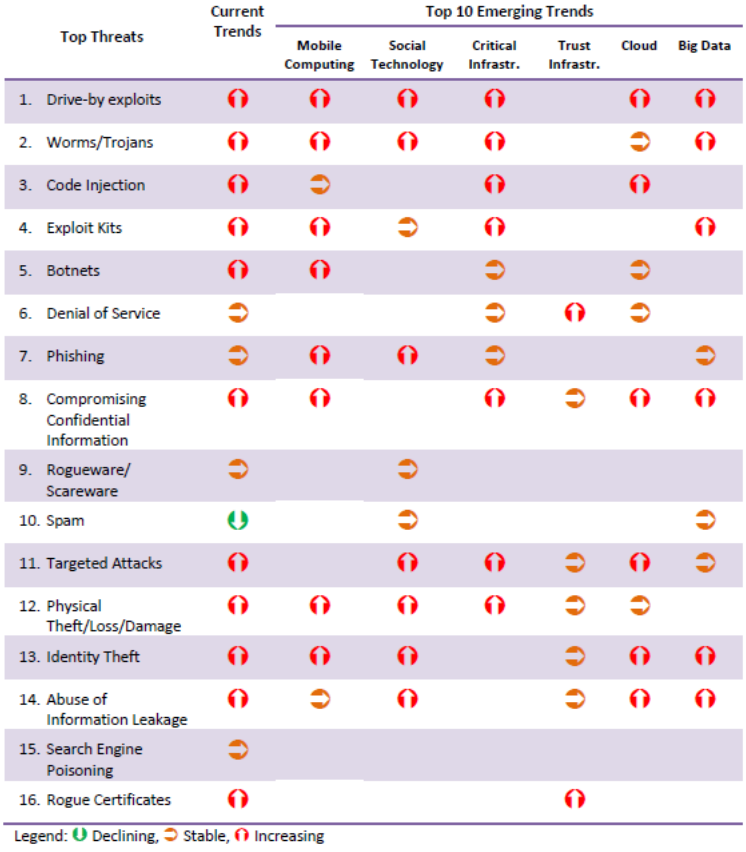
Threats to personal assets

- Credit information
- Online identity
- Financial information
- Compromised computing devices
- Virtual assets

Threats to organizational assets

- Blackmail threats
- Identity theft
- Employee, client and supplier information
- Financial information
- Government held information
- Internet infrastructure

B. ENISA Threat Landscape: Responding to the Evolving Threat Landscape 2012-09-28

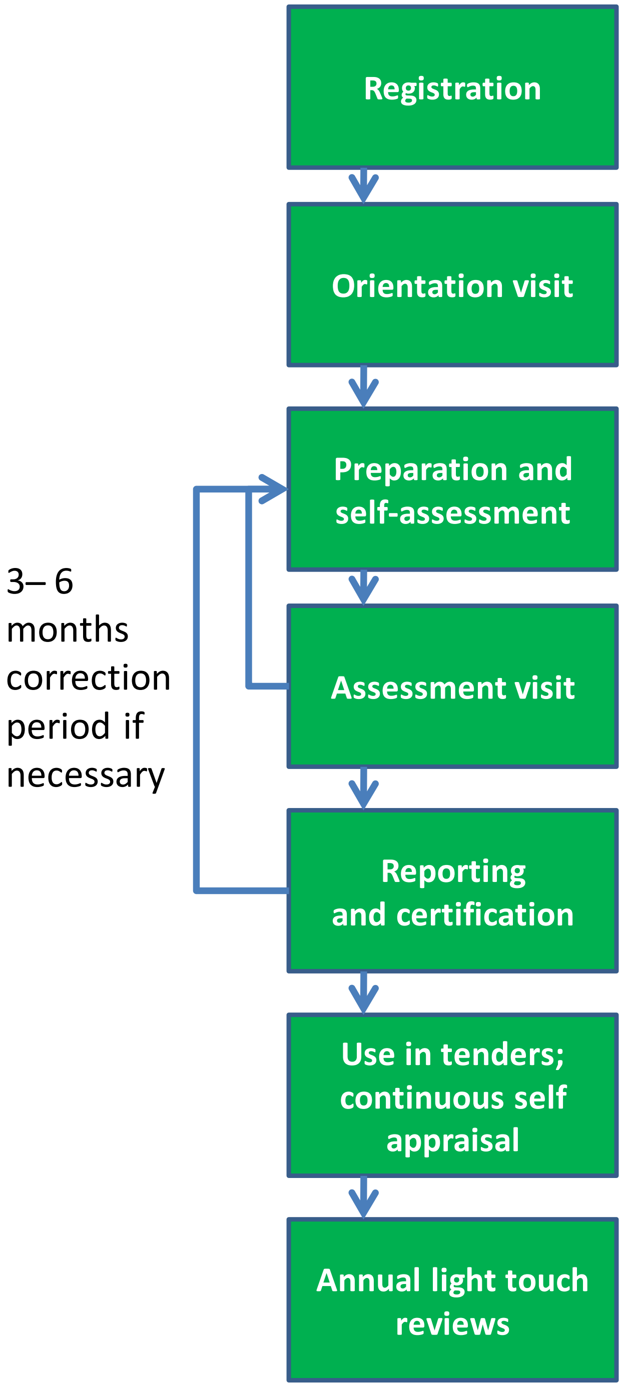


Top Threats	Current Trends	Top 10 Emerging Trends					
		Mobile Computing	Social Technology	Critical Infrastr.	Trust Infrastr.	Cloud	Big Data
1. Drive-by exploits	↑	↑	↑	↑		↑	↑
2. Worms/Trojans	↑	↑	↑	↑		→	↑
3. Code Injection	↑	→		↑		↑	
4. Exploit Kits	↑	↑	→	↑			↑
5. Botnets	↑	↑		→		→	
6. Denial of Service	→			→	↑	→	
7. Phishing	→	↑	↑	→			→
8. Compromising Confidential Information	↑	↑		↑	→	↑	↑
9. Rogueware/ Scareware	→		→				
10. Spam	↓		→				→
11. Targeted Attacks	↑		↑	↑	→	↑	→
12. Physical Theft/Loss/Damage	↑	↑	↑	↑	→	→	
13. Identity Theft	↑	↑	↑		→	↑	↑
14. Abuse of Information Leakage	↑	→	↑		→	↑	↑
15. Search Engine Poisoning	→						
16. Rogue Certificates	↑				↑		

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 1: Overview of Threats and Trends of the ENISA Landscape[2]

Annex B: The IASME Accreditation Flow Diagram


Registration
Orientation visit
Preparation and self-assessment
Assessment visit
Reporting and certification
Use in tenders; continuous self appraisal
Annual light touch reviews
3– 6 months correction period if necessary

Tell us who you are.

We visit you and manage everyone's expectations – what is your risk profile?

Where you collate evidence Preparing any new activities to manage risk

An intensive day with your assessor to review information security in your business

Assessor makes a case for your certification to the independent programme moderator.

Successful businesses are awarded a bronze, silver, or gold marque

Is information security maintained and in line with your risk profile?

Annex C: Assessment and Certification Process

The assessor scores the maturity of each control, and the total scores determine the level of achievement and certificate to be awarded. The scoring is carried out on a scoring matrix tailored to the business risk profile and is carried out by assessing the capability maturity of each control as follows:

Level 0	Initial	Little or no evidence available of the security control.
Level 1	Minimal.	Some evidence of the control, but little or no documentation available.
Level 2	In Use.	The control is in use, partially documented and some evidence of use is available.
Level 3	Managed.	The control is in use, is fully documented, and some metrics are collected but not fully exploited.
Level 4	Controlled.	The control is managed, fully monitored and the metrics are used to improve security.
Level 5	Optimised.	The control is managed and leads to optimised security management and forecasting for the business.

Table 2: Maturity levels

Assessment options

Depending on the complexity of the risk profile, the audited assessment may follow either the Fast Track or the Full Matrix assessment process.

Self-Assessment

A self-assessment form is available which required the client to fill in a questionnaire relating to their organisation cyber security and return it for moderation to IASME. So long as the answers demonstrate sufficient maturity in the implementation of their cyber security, a Self-Assessed IASME certification will be issued. The client is not audited.

Audited Fast-track assessment

Micro businesses (less than 20 staff) which typically have been assessed as demonstrating a Low Risk Profile *may* adopt the Fast-track assessment process at the discretion of the assessor and with the agreement of the moderator. This involves assessing the maturity (*Table 2*) of the high-level controls contained in the completed Business Information Security Policy and management processes, the effectiveness of the Business Continuity Plan and the attitude of the business to their security issues, rather than assessing the maturity of the full control set. This enables a very small, low risk business to complete the process at lower cost.

Businesses to which this cannot be applied will be subject to assessment of the full set of information security controls.

Audited Full matrix control set assessment

The full set of information security controls consists of 112 individually weighted risk management activities in 13 domains (*Organisation*

Manage information resources within the organisation and in the organisation's relations with partners.

Risk Understand and manage the risk to your business information.

Policy and Compliance

Establish legal and regulatory requirements, management direction and communications. Know what is required and monitor compliance

Assets

Know the value of your information assets, and acquire and dispose of them securely.

Planning

Build security and privacy in at the start; make sure you have the right-sized information systems.

Access

Control who and what can access your information.

People

Know your people and educate them in business security.

Physical and Environmental

Protect your information assets from physical and environmental harm.

Disruption

Defend your information from hostile attack and be ready to recover from the effects.

Operations

Manage and monitor your information systems effectively.

Incident management

Ensure breaches of confidentiality, integrity or availability of your systems are detected and dealt with; learn the lessons.

Continuity

Make sure you can recover quickly from partial or total loss of key information assets.

Table 1), grouped and weighted in relation to the three Risk Profiles (Simple, Intermediate, and Complex). There is a subset of Essential controls which apply to all three profiles. All businesses must demonstrate the correct level of maturity (*Table* 2) in these controls before an IASME certificate can be awarded.

The assessor will score each observed control according to its maturity within the appropriate control set. The control weighting is different in the three profiles; requirements and applicability being generally lower in the lower profiles and higher and more comprehensive in the higher profiles. These weightings are initially for the guidance of the assessor, who is able to adjust control applicability individually for each business if there are any special circumstances arising from the risk profile. Thus the control assessment profile may be different for each business assessed.

Certification Process

Certification is carried out independently of the assessor who assisted the organisation in developing its security profile.

The weighted maturity scores from the assessment of the relevant set of Business Information Security Control determine the level of certification (Bronze, Silver and Gold), and may be subject to adjustment by the moderator. The business may opt to take the appropriate certificate, or to carry out an improvement plan to achieve a higher level of IASME certification. The IASME methodology – from the controls to the assessment processes – that are described in this standard has been developed, and their efficacy proven, with the help of SMEs including micro businesses. Case studies can be found on the IASME website

.

Annex D: The Risk Assessment process

Fact finding

The following information is collected and assessed using a balanced scorecard to describe your business to the IASME programme. It helps the assessor make sure that the assessment is tailored to the complexity of what you do.

(1) Number of staff (permanent and temporary), contractors, and the scale of any outsourcing.

The number of staff and their relationship to the business contributes to your information security assessment.

(2) Locations and physical attributes.

Information collected includes physical protection, for example fences, secure doors, security lighting, and cameras and so on.

This is to identify any physical vulnerabilities to your information security.

(3) Information and communication technology (ICT).

Data processing, data storage, access terminals, networks (including access points to the Internet and other external connections). Information collected includes number and locations of servers and workstations, inter and intra-site communications, use of Cloud or personal devices and whether you are using protective measures such as encryption that hides the information you store on hard drives, CD ROMs or DVDs, or memory sticks.

This is to identify any technical vulnerabilities in your information security.

(4) Environmental plant

Information collected includes what you have by way of environmental equipment such as air conditioning, fire suppressants and uninterruptable power supplies (UPS) and anything else which might be helpful.

This is to identify any environmental vulnerabilities to your information security.

(5) Personnel who must take a special interest in information security.

Information collected includes management responsibilities for information security, identified risk owners, and staff with special security responsibilities.

This is to establish the level of security responsibilities.

(6) Legal and regulatory requirements.

Information collected covers the laws or regulations that apply to the information your business handles. It will include contractual or organisational agreements relating to information security and industry-specific information security controls or measures.

This is to identify any particular legal or regulatory issues.

Risk analysis

The information from the fact-finding is combined with the following information and is analysed using a balanced scorecard to describe your business to the IASME programme. It helps the assessor make sure that the assessment is tailored to how your business works.

(1) Use of IT systems.

Information collected includes how complex your IT, attitude to change and innovation, use of the Internet, mutual access to partners' IT systems is and how much of your business is conducted by home, remote or mobile working.

(2) Risk exposure.

Information collected includes exposure to inappropriate disclosure of business data, damage or loss to hardware or software or paper filing systems. IASME also pays close attention to your exposure to people-related incidents. IASME considers threat actors (who might do inappropriate things to your business?) and threat vectors (how will they do it?).

(3) Key asset values.

Information collected includes the impact of a loss of confidentiality, the impact of data corruption, and the impact of data loss.

(4) Importance of ICT to the business.

Information collected includes the significance of business ICT to meeting business objectives and the significance of business ICT to clients, partners and external stakeholders.

Taken together, these can indicate the relative value of the business information processing and storage facilities, and the business risk appetite.

Risk profiling

The fact-finding, risk analysis above and most importantly, interviews with the business, enables the assessor to decide the relative complexity of the business risk profile and any issues which require particular scrutiny.

The balanced scorecard analysis places the business in one of three risk profile categories: Simple, Intermediate or Complex. The Assessor has the flexibility to use expert judgment to vary the category in borderline situations, ratifying this judgement with one of the IASME scheme moderators.

Simple profile

A typical Simple profile may be applicable to a business with less than 20 employees with one or two offices, all located in the UK, with little or no outsourcing or remote working. The size and nature of the ICT is likely to be small and uncomplicated, and the offices secured in the normal way with sturdy locks, fire alarms and so on. Typically, the managing director or finance director will be responsible for security, and ICT will be looked after by a member of staff with some relevant interest or expertise, or a local IT contractor. Even if there are one or two complicating factors such as managing highly sensitive client data, or particular legal requirements, the business may still be classified as Simple by the assessor (the size of the business focuses the sense of duty of the employees and reduces the threat vectors).

Intermediate profile

Intermediate profiles are typically those which cannot be classified as Simple, but do not have many of the factors which would classify them as Complex. Assessors are instructed that if in doubt, classify to the level above if the business has a low risk appetite, and to the level below if they exhibit a high risk appetite. This allows the business to choose the level of risk management suitable for itself.

Complex profile

A Complex profile can be a business with any number of employees, although larger businesses are more likely to be classified as Complex because of the increased number of internal potential threat actors. The business may have offices or personnel overseas and considerable remote working and outsourcing, where partners or clients have access to the business information systems. Responsibility for security may be organisationally difficult or unclear. The business may handle a considerable amount of sensitive material owned by the business, clients or partners. The information systems will be vital to the business. The information handled will have significant impact on the business, its customers, or those who the information pertains to.

Profile assessment

Risk profiling enables the assessor to assist the client in the development of key controls and documentation. The aim of the Standard is to minimise the amount of documentation required from the business, but a certain amount is necessary both for the client and to provide continuity for the on-going certification process. The aim is to make the level of documentation both achievable by the business and appropriate for the assessment process.

The assessor can help the business to develop their policy and other documentation, suggest improvement measures not already in place, and will assess the results and inform the client. Allowance is made for iteration of all these processes, for example clarification of key information assets may often emerge during the construction of the Business Continuity Plan.

The value of all controls in the model is varied by the assessor in consultation with the business under scrutiny and so each assessment is unique.