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


Information Assurance for Small to Medium-sized Enterprises

<table>
<thead>
<tr>
<th>Document</th>
<th>IASME Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue:</td>
<td>1.1</td>
</tr>
<tr>
<td>Date:</td>
<td>April 2012</td>
</tr>
<tr>
<td>Author:</td>
<td>David A. Booth</td>
</tr>
<tr>
<td>Technical Approval:</td>
<td>Daniel G. Dresner</td>
</tr>
<tr>
<td>Quality Approval:</td>
<td>Richard Henson</td>
</tr>
</tbody>
</table>

Modification History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Revision Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>1 April 2011</td>
<td>For issue</td>
</tr>
<tr>
<td>1.0e</td>
<td>March 2012</td>
<td>Review</td>
</tr>
<tr>
<td>1.1</td>
<td>April 2012</td>
<td>Reissue</td>
</tr>
</tbody>
</table>

© The IASME Consortium Ltd and David A. Booth 2011
All rights reserved.

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

Information contained in this document is believed to be accurate at the time of publication. 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.

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

1. Introduction ................................................................................................................................. 5
2. Business risk factors ................................................................................................................... 5
3. How IASME works ...................................................................................................................... 6
   3.1. Assessing the risk .................................................................................................................... 7
   3.2. Fact finding ........................................................................................................................... 7
   3.3. Risk analysis ......................................................................................................................... 8
   3.4. Risk profiling ....................................................................................................................... 9
       Simple profile .......................................................................................................................... 9
       Intermediate profile ............................................................................................................... 9
       Complex profile ..................................................................................................................... 9
       Profile assessment ............................................................................................................... 9
4. Scoring and certification ............................................................................................................... 10
   4.1. Assessment options ............................................................................................................... 11
       Fast-track control assessment ............................................................................................... 11
       Full matrix control set assessment ...................................................................................... 11
   4.2. Certification ....................................................................................................................... 11
5. Endnote: it works! ....................................................................................................................... 11

Annex A. Information security objectives ....................................................................................... 12
Annex B. The IASME Certification Process .................................................................................. 15

Figures

Figure 1: Continuous assessment .................................................................................................. 6

Tables

Table 1: The IASME Checklist ....................................................................................................... 6
Table 2: Maturity levels ................................................................................................................ 10
This page intentionally blank.
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 usually because assigning a value to information is 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 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 formal certification 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.

2. Business risk factors

There is a common set of factors to be considered when assessing the effectiveness of an organisation’s information security, which are summarised below and described in more detail at Annex A.

The importance of these factors varies from organisation to organisation, but all apply to some extent. The IASME process reduces the complexity inherent in this list using a structured method suitable for SMEs.
1. **Organisation**  
   Manage information resources within the organisation and in the organisation’s relations with partners.

2. **Risk**  
   Understand and manage the risk to your business information.

3. **Policy**  
   Establish management direction and communications.

4. **Assets**  
   Know your information assets, and acquire and dispose of them securely.

5. **People**  
   Know your people and educate them in business security.

6. **Things**  
   Protect your information assets from physical harm.

7. **Malware**  
   Defend your information from hostile attack and be ready to recover from infection.

8. **Access**  
   Control who and what can access your information.

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

10. **Operations**  
    Manage and monitor your information systems effectively.

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

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

13. **Legal compliance**  
    Know what is required and make sure you comply.

### Table 1: The IASME Checklist

#### 3. How IASME works

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

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 (see Annex B).

IASME expects a set of documentation that is right-sized for you. 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.
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.

3.1. Assessing the risk

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 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.

3.2. 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 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.

3.3. 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.

3.4. 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.
In order to assist the business in implementing the most important information security controls, the assessor provides a document pack including a model Business Information Security Policy (which includes an outline management process) and Business Continuity Plan. These are designed for businesses that do not have these items in use or would like to compare what they do with the good practice of others. They are to be customised to fit the level of complexity of the business, and contain statements of all key security requirements.

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.

Risk profiling allows the assessor to choose the category of control implementation customised for the business. As stated above, all controls are deemed necessary unless proved otherwise. The requirements in the Business Information Security Policy map onto the subsequent more complex assessment process which addresses the implementation of each control.

The set of risk management controls accommodates the Simple, Intermediate and Complex risk profiles. The subset of the controls for each profile places a different emphasis on each control, according to the degree of complexity of the profile. A small number of the full set of controls are generally considered inappropriate for the Simple profile (and an even smaller number for the Intermediate profile), but will be introduced by the assessor if they think it necessary. For example, such controls include management committees (if the business is very small), however it should be noted that some very small businesses may prefer this approach if it is in their culture. Equally, some controls are essential to all sizes and complexities and must be implemented properly in all cases.

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.

4. Scoring and certification

The assessor scores the quality 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:

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

Table 2: Maturity levels
4.1. Assessment options

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

**Fast-track control 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 with commensurate effort.

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

**Full matrix control set assessment**

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

4.2. Certification

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.

5. Endnote: it works!

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 A. Information security objectives

<table>
<thead>
<tr>
<th>Domain</th>
<th>Control Set Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security organisation</td>
<td>To manage information assurance within the organisation and in the organisation’s relations with partners</td>
</tr>
<tr>
<td>Risk assessment and management</td>
<td>To understand the information risk to the organisation and provide information assurance to the business</td>
</tr>
<tr>
<td></td>
<td>To determine the business risk tolerance</td>
</tr>
<tr>
<td></td>
<td>To manage the risk in accordance with the risk tolerance</td>
</tr>
<tr>
<td>Security policy</td>
<td>To provide management direction and support for information security in accordance with business requirements and relevant legislation</td>
</tr>
<tr>
<td>Asset management</td>
<td>To achieve and maintain appropriate protection of information assets</td>
</tr>
<tr>
<td></td>
<td>To maintain a record of key organisational assets</td>
</tr>
<tr>
<td></td>
<td>To dispose of assets securely</td>
</tr>
<tr>
<td>Personnel security</td>
<td>To ensure that all employees</td>
</tr>
<tr>
<td></td>
<td>• Are suitable from a security viewpoint before and during employment.</td>
</tr>
<tr>
<td></td>
<td>• Are aware of, and adequately trained in, their security responsibilities</td>
</tr>
<tr>
<td></td>
<td>• Security privileges reflect business need.</td>
</tr>
<tr>
<td></td>
<td>• Are suitably debriefed on termination of employment.</td>
</tr>
<tr>
<td>Physical and environmental security</td>
<td>To prevent:</td>
</tr>
<tr>
<td></td>
<td>• Unauthorised physical access, damage and interference to the organisation’s assets and information.</td>
</tr>
<tr>
<td></td>
<td>• Loss, damage, theft or compromise of assets which might interrupt the organisation’s activities.</td>
</tr>
<tr>
<td></td>
<td>• Loss of environmental control which might affect availability.</td>
</tr>
<tr>
<td>Prevention and detection of malicious code</td>
<td>To protect systems and information from malicious code and unauthorised mobile code</td>
</tr>
<tr>
<td></td>
<td>To recover from the effects of malicious code</td>
</tr>
<tr>
<td>Physical and technical control of access to information</td>
<td>To establish the business requirements for access to information</td>
</tr>
<tr>
<td></td>
<td>To ensure access by authorised users and prevent access by unauthorised users</td>
</tr>
<tr>
<td></td>
<td>To establish user responsibilities to prevent compromise or theft of information and information processing facilities</td>
</tr>
<tr>
<td></td>
<td>To prevent unauthorised access to internal and external networked services</td>
</tr>
<tr>
<td></td>
<td>To prevent unauthorised access to operating systems’ facilities</td>
</tr>
<tr>
<td></td>
<td>To prevent unauthorised access to information held in applications systems</td>
</tr>
<tr>
<td></td>
<td>To ensure information security when using mobile computing, teleworking or home working</td>
</tr>
<tr>
<td>Domain</td>
<td>Control Set Objectives</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Planning and Acquisition    | To ensure that security is an integral part of the business technical systems architecture  
To ensure that security is included in the specification for information systems as required by a risk assessment  
To prevent unauthorised access or loss of integrity or availability by including specific controls during the development of applications  
To prevent unauthorised access to particularly sensitive data by specifying e.g. encryption controls  
To ensure that security as part of the system functionality is properly implemented before the system is operational  
To carry out adequate systems capacity planning and acceptance procedures to maintain future systems integrity or availability |
| Operations and Management   | To control access to system files and source code  
To ensure optimum and secure operation of information systems  
To implement and maintain appropriate and agreed levels of security and service delivery with third parties and home workers  
To maintain the integrity and availability of information and information processing facilities by backup and restore capability  
To ensure the protection of information in networks and the protection of the supporting infrastructure  
To protect information on removable media  
To maintain the security of information and software exchanged within the organisation and with any external entity  
To maintain the security of electronic commerce services  
To detect unauthorised information processing by accounting and audit of activities |
| 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 |
| Business 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 |
<table>
<thead>
<tr>
<th>Domain</th>
<th>Control Set Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance with legal, statutory, regulatory and contractual obligations and security requirements</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>To ensure that organisational records are protected from loss, destruction or falsification in accordance with the organisation’s legal and other obligations.</td>
</tr>
<tr>
<td></td>
<td>To prevent or deter the use of an organisation’s information systems from misuse.</td>
</tr>
<tr>
<td></td>
<td>To ensure compliance of information systems with organisational policies and standards.</td>
</tr>
<tr>
<td></td>
<td>To ensure that system audits are effective and minimise impact on the business.</td>
</tr>
<tr>
<td></td>
<td>To limit access to audit tools and audit information.</td>
</tr>
</tbody>
</table>
Annex B. The IASME Certification Process

Registration
Tell us who you are.

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

Preparation and self-assessment
Where you collate evidence Preparing any new activities to manage risk

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

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

Use in tenders; continuous self appraisal
Successful businesses are awarded a bronze, silver, or gold marque

Annual light touch reviews
Is information security maintained and keeping up with your risk profile.

3–6 months correction period if necessary