



THE IASME CYBER BASELINE STANDARD VI

© IASME Consortium Limited 2023

All rights reserved.

The copyright in this document is vested in IASME Consortium Limited. 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 IASME Consortium Limited 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 but no liability whatsoever can be accepted by IASME Consortium Limited arising out of any use made of this

MODIFICATION HISTORY

Revision	Date	Revision Description
V1	May 2023	Initial publication

CONTENTS

Modification History	2
Contents.....	3
Chapter 1 - Introduction.....	5
The need for information security	5
What are the business drivers for applying the IASME Cyber Baseline standard?	5
Relationship with IASME Cyber Assurance	5
How to use this document	5
Chapter 2 – How the IASME Cyber Baseline standard works.....	7
Making changes to become more secure.....	7
The assessment and certification process	8
Who governs the Standard?	10
Chapter 3 - Scope	10
An overview of the IASME Cyber Baseline scope.....	10
What is in Scope for certification?	10
How to scope your organisation for certification	10
Scope descriptions.....	11
What if I must use operating systems or software that is no longer supported?.....	12
Chapter 4 - The themes: requirements and guidance	13
How the thirteen themes are formatted	13
Taking the next steps.....	14
Theme 2 – Organisation.....	15
Theme 3 – Assets	17
Theme 5 – Secure architecture.....	21
Theme 7 – People.....	23
Theme 9 - Managing access	25
Theme 10 - Technical intrusion.....	28
Theme 11 - Backup and restore	30
Theme 13 - Resilience: business continuity, incident management, and disaster recovery	32
Appendices	35
Appendix A – Compatibility with regulation and other cyber and information security standards	35
Appendix B – Glossary	36
Appendix C – Common scoping scenarios and examples	38



Appendix D – The Themes for guidance only	39
Theme 1 - Planning information security	39
Theme 4 – Legal and regulatory landscape	40
Theme 6 - Physical and environmental protection	41
Theme 8 - Policy realisation.....	42
Theme 12 - Secure business operations: monitoring, review, and change management	42
Appendix E - The IASME family of practical information and cyber security certifications.....	43

CHAPTER 1 - INTRODUCTION

The need for information security

Organisations of all sizes need to keep their data safe and prevent breaches of information that would expose their customers, clients and investors to negative impacts.

While there is a lot of good practice which can be put in place within an organisation to give a good level of cyber security, many organisations struggle to get started. IASME has found that it is important to have a baseline certification level which covers a core set of controls for keeping an organisation secure against common internet threats. A certificate at this baseline level will indicate that a core set of cyber security controls are in place.

What are the business drivers for applying the IASME Cyber Baseline standard?

The IASME Cyber Baseline standard enables organisations to:

- Understand a core set of controls designed to protect against common internet threats
- Be independently reviewed by an assessor against this standard and be awarded a certificate to confirm a core set of controls have been implemented.
- Give themselves, customers – including government procurement departments, and their supply chain a level of assurance that they have implemented a core set of cyber security controls.
- Demonstrate that your organisation aligns with global cyber hygiene and cyber security frameworks* (*such as Cobit, CIS Controls v8)
- Take the first important step towards IASME Cyber Assurance certification which will open doors to procurement frameworks, allowing your organisation to compete for contracts

Once certified to the standard, applicants can use the certificate to confirm to customers/clients, supply chains and others that they have a core set of controls in place to protect against common internet threats.

Relationship with IASME Cyber Assurance

IASME Cyber Baseline works closely with IASME Cyber Assurance and is a prerequisite to gaining IASME Cyber Assurance certification. IASME Cyber Baseline uses the IASME Cyber Assurance Themes but is based purely on a core set of technical controls. It has been compiled by SMEs for SMEs, providing a core set of controls designed to protect SMEs from the most common internet threats.

The IASME Cyber Baseline scheme allows every size of organisation in every sector to start their cyber security journey with simple cyber security measures along 9 themes. As organisations increase their maturity, they may choose to continue developing their security posture towards including the full 13 themes of IASME Cyber Assurance

How to use this document

The remainder of this document is organised into the following sections:

- **Chapter 2** – explains how the IASME Cyber Baseline standard works. In this section:
 - The IASME Cyber Baseline themes are introduced.
 - The process of implementing the controls and improving your security is outlined, alongside an overview of how the assessment process works to measure and demonstrate your compliance.
- **Chapter 3** – covers how to define an appropriate scope, to realise the IASME Cyber Baseline standard's themes.
- **Chapter 4** – sets out the IASME Cyber Baseline themes: requirements and guidance.

CHAPTER 2 – HOW THE IASME CYBER BASELINE STANDARD WORKS

Making changes to become more secure

The IASME Cyber Baseline scheme allows every size of organisation in every sector to start their cyber security journey with simple cyber security measures along 8 themes. As organisations increase their maturity, they may choose to continue developing their security posture towards including the full 13 themes of IASME Cyber Assurance.

The themes are divided into four categories which should be a logical progression:

Identify and Classify:

This category helps you to identify your assets, classify the importance of each one, and begin to protect your assets by looking at a core set of controls.

Protect:

This category focuses on putting in place a core set of controls controlling access to information, preventing technical attacks and backing up your information.

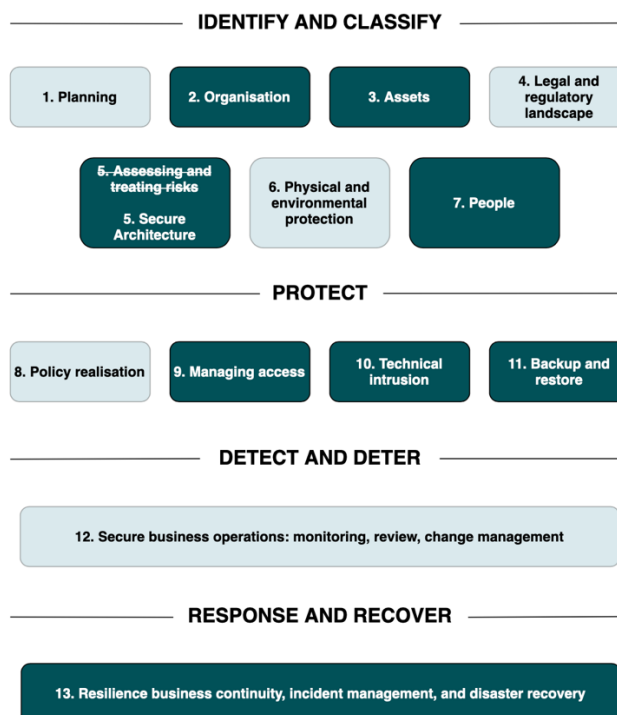
Detect and Deter

This category looks at monitoring to detect attacks, reviewing and managing changes to systems.

Respond and Recover

This category looks at how you can respond to incidents and recover from them through business continuity and disaster recovery processes.

Figure 1: Highlighted are the Themes of IASME Cyber Baseline



The assessment and certification process

Certification Bodies and Assessors



IASME owns and operates the IASME Cyber Baseline standard, but the assessment of organisations is carried out by IASME's Certification Bodies.

The Certification Bodies are companies with in-depth knowledge of cyber security who have met the high security, quality and skills requirements set by IASME. Each Certification Body has a number of Assessors, who are skilled and experienced information and cyber security experts who carry out the assessments.

The process

Although accessible to organisations of all sizes, the Standard is designed specifically to accommodate the needs of SMEs and ensure the certification and compliance process does not place an onerous burden on smaller organisations.

Table 1: Awards achievable

Following online self-assessment by an IASME Certification Body (Level 1)	
	A certificate based on a verified self-assessment
Following an audit by an IASME Certification Body (Level 2)	
	A certificate based on both a verified self-assessment and also a technical audit of your IT systems.

An organisation can certify to IASME Cyber Baseline at two levels (see table 1):

- Level 1 (Verified self-assessment)
 - The organisation completes the online IASME Cyber Baseline assessment by answering a set of questions through IASME's online portal. The questions are marked by an Assessor who provides useful feedback and determines pass/fail for the assessment.
- Level 2 (In-person or remote audit)

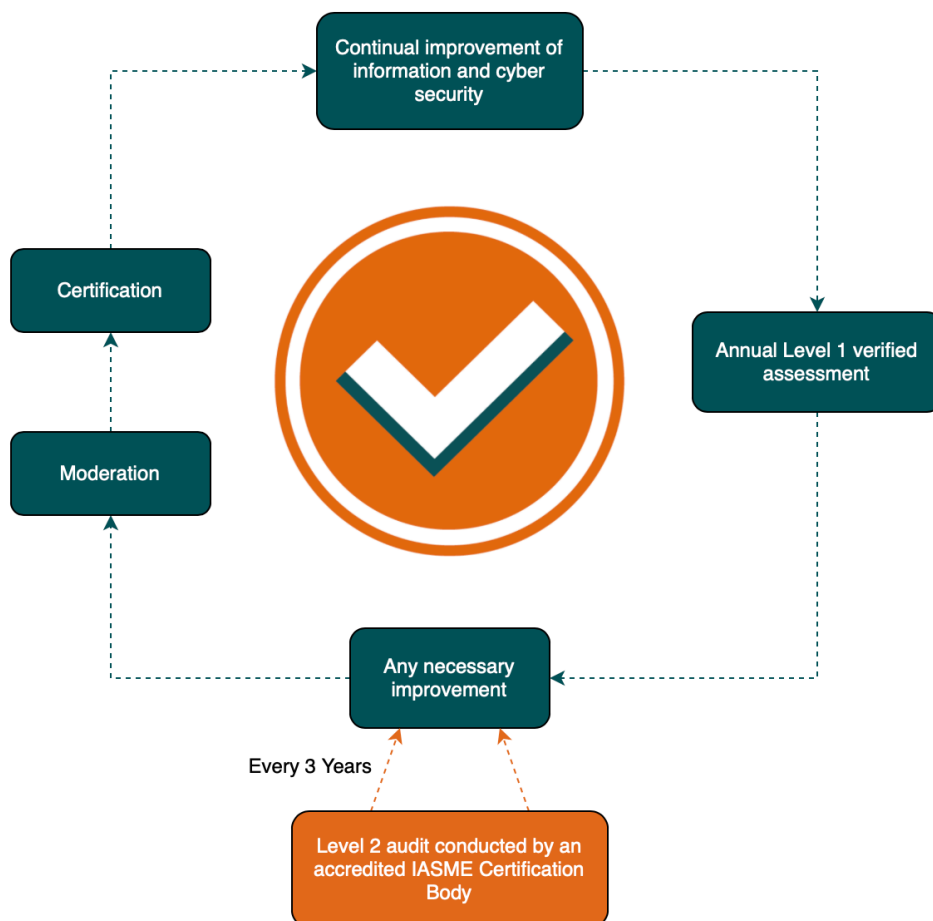
- After completing and achieving a pass in the Level 1 assessment, an Assessor carries out an audit of the organisation. The audit will include a technical audit. This can be done in person or sometimes remotely (such as via a video call).
- The organisation will achieve pass/fail depending on how well the organisation meets the standard.

The standard relies on a process of annual assessment.

For Level 1 certification, the certificate is valid for a year and recertification requires an annual re-assessment.

For Level 2 certification, organisations are required to complete the IASME Cyber Baseline verified assessment using the online portal in years two and three after achieving their audited (Level 2) certification, in year four, they go through the full audit process afresh (see Figure 2).

Figure 2: IASME Cyber Baseline Implementation Cycle



Who governs the Standard?

The development of the IASME Cyber Baseline standard is reviewed by an advisory panel and updated as a result of changes to the threat landscape, drawing on the latest expertise from across industry sectors.

IASME is an ISO 9001 certified organisation and follows a strict set of quality policies and processes to ensure consistency within the certification process.

The Certification Bodies meet strict security and quality requirements, and the Assessors meet specific skills and experience requirements, as well as receiving ongoing training and support from IASME. All Assessors are required to comply with a code of conduct.

The certification process itself includes ongoing quality control with sample auditing of assessments and feedback to Assessors and clients as needed.

CHAPTER 3 - SCOPE

IASME Cyber Baseline certification is available to organisations internationally. Organisations legally registered within the United Kingdom or working with the UK government will need to apply for Cyber Essentials and not IASME Cyber Baseline.

**This exclusion does not apply to UK registered Certification Bodies licensed to deliver the Cyber Baseline standard.*

An overview of the IASME Cyber Baseline scope

Scoping can be the most difficult part of certification. Ideally organisations should look at certifying their “whole organisation” because this gives you the most protection and ensures you have embedded the controls appropriately. However, we understand that this is not always possible, and the borders of the assessment must be defined.

As part of your IASME Cyber Baseline application you will have to complete a scoping statement.

NOTE: The scoping statement appears on your organisations' public facing certificate.

What is in Scope for certification?

- All devices including BYOD and cloud services which connect to and accessed using the internet are in-scope for your assessment.
- All devices including BYOD must be installed with an operating systems which is supported and receiving regular security updates from the vendor. Unsupported operating systems will result in an automatic failure of assessment.
- All software and cloud services installed and accessed by the devices in scope must be supported and receiving regular security updates from the vendor.

How to scope your organisation for certification

The borders of your scope will be created by your firewalls and routers.

- Network at an office location - you will need to be using a firewall or router device to create the border between the internet and your devices.
- Remote working - the software firewall in the operating system of the device will create the border. The software firewall only offers protection for a single device, where you have multiple remote workers the software firewall will need to be configured on all of their devices to create border between the device and the internet.
- Cloud Services - where cloud services are providing organisational or platform services, the virtual firewall included with the services needs to be configured to create the required border.

Any devices protected by your firewalls and routers will need to meet the theme requirements outlined in IASME Cyber Baseline.

Where devices are using unsupported operating systems or software, they cannot be included in the scope of your assessment. In a network these devices would need to be separated from the scoped network by using a firewall device or Vlan creating a new network segment with no access to the internet.

Where you are using Cloud services all connecting devices must meet the theme requirements of IASME Cyber Baseline.

Scope descriptions

The scope descriptions for IASME Cyber Baseline certification is split into two areas. This will ensure you have considered both areas when scoping and identifying any exclusions. Both scoping statements will all be included on your Certification certificate once successful.

Locations/Authorities included within scope

You need to provide details of any physical locations within scope, including home or flexible workers. You should also include the organisation names or authorities that are included.

Example: London and Sydney offices to include ZYX Ltd and YZX Plc.

Networks included within scope. How do I define the borders for my network(s)?

You need to include details of each network used in your organisation include its name, location, and its purpose. You do not need to provide IP addresses or technical information.

Example: Main network at Head Office for administrative use, development network at New York office for testing software or home workers network based in Belgium.

As part of your scoping statement you will be asked to provide details of any networks or locations that are excluded from certification. There must be clear segregation between anything included within scope of certification, and anything that has been excluded.

Common scenarios and scoping examples can be found in Appendix C.

Excluded: IoT, OT, non-internet connected technology is not included in the assessment but need to be placed onto a separate network which is separate from the network being assessed.

The devices IASME Cyber Baseline requires you to include splits into 2 groups:

- end user and storage devices, and

- networking equipment.

What if I must use operating systems or software that is no longer supported?

Some organisations have to use operating systems and software that may no longer be supported by the vendor. When this is the case there it can become a vulnerable because no updates or patches are being supplied to fix security flaws, introducing weaknesses into your systems. When this is the case the solution is to place the devices with the unsupported operating system or software, in an alternative network with no internet access. This process is referred to as network segmentation. There are two methods that can be used to achieve the required level of network segmentation.

- Place an additional firewall device between the devices with unsupported operating systems or software and the internet creating an additional layer of protection on a new network segment. The new network segment should not have access to the internet.
- Place the device onto a virtual network also known as VLAN, that is again isolated from the internet.

CHAPTER 4 - THE THEMES: REQUIREMENTS AND GUIDANCE

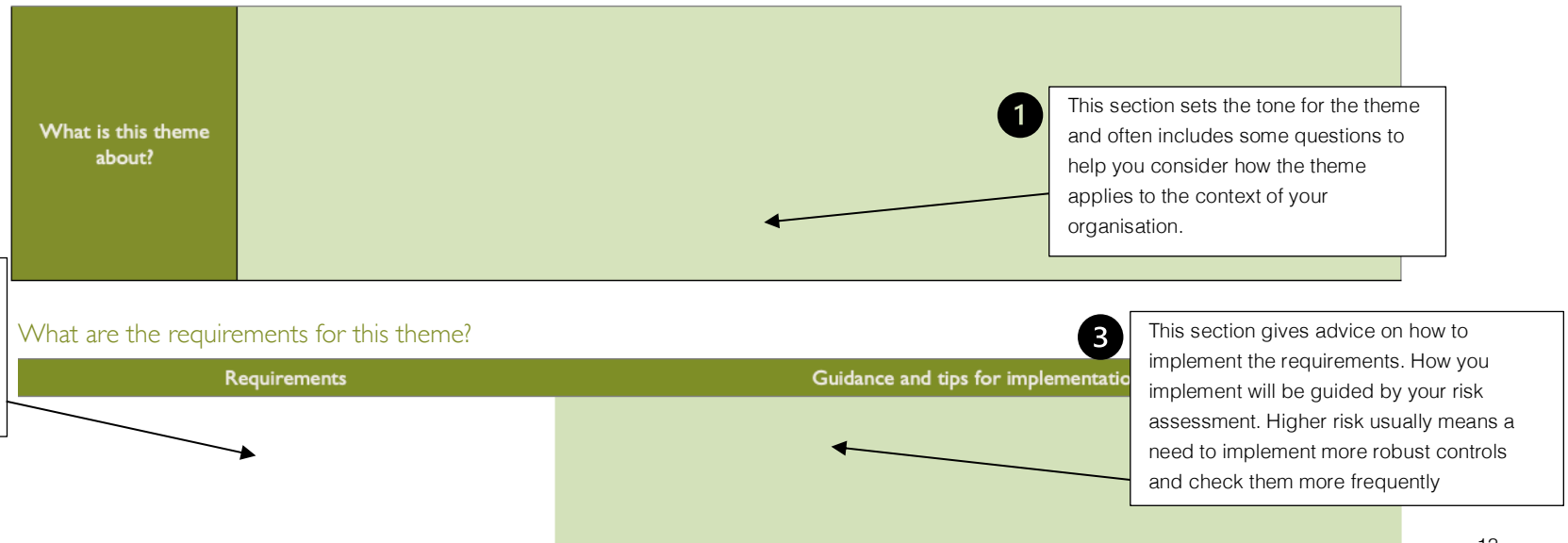
The IASME Cyber Baseline standard comprises of controls that are broken into 8 themes. Your organisation needs to meet the requirements of all of these themes in order to achieve compliance with the standard. There are 5 themes that are for guidance purposes and for readiness to progress to IASME Cyber Assurance certification. These are detailed in Appendix D.

To provide some additional context, we have included some references and placeholders from the more advanced IASME Cyber Assurance standard. These are not mandatory requirements, but they illustrate possible next steps to improving your cyber security. Both the IASME Cyber Baseline and IASME Cyber Assurance utilise the same structure of themes, to help highlight how you may logically progress from this baseline standard, which is prerequisite for the IASME Cyber Assurance standard.

How the thirteen themes are formatted




The core activities within the themes are formatted in three sections:

Theme [Number] - [Theme Name]



Taking the next steps

IASME Cyber Baseline covers measures that allow you to establish a basic level of cyber hygiene and resilience. To help you in your cyber security journey we have included additional tips in boxes like the one below. These tips have mostly been adapted from the IASME Cyber Assurance standard which builds on your foundation of basic cyber hygiene into more comprehensive information security management. You **do not** have to implement these suggestions to meet the IASME Cyber Baseline requirements.

 <p>IASME CYBER BASELINE</p>   <p>IASME CYBER ASSURANCE</p>	<p><i>Taking the next step...</i></p> <p>As an example, the information provided in these boxes will give you information relating to IASME Cyber Assurance and considerations you can take to progress towards this certification.</p>
---	---




Theme 2 – Organisation

<p>What is this theme about?</p>	<p>Most organisations use an IT product or service that is provided by a third party. This will inevitably interact with your IT network. An intentional or unintentional security gap, weakness or ‘vulnerability’ in the systems of one of your third party suppliers, contractors or partners may undermine your security, no matter how good it is.</p> <p>It is important you take account of who your third-party suppliers, contractors and partners are and understand what cyber security measures they have in place.</p>
<p>Question Set Reference</p>	<p>C3.1 to C3.4</p>

What are the requirements for this theme?

Requirements	Guidance for implementation
<p>1. Keep an up-to-date list of your partners, suppliers, and contractors.</p> <p>a. Record contact details for each party in your list.</p> <p>b. Verify that your third-party suppliers implement cyber security controls and carry out a review at least once a year.</p>	<p>Maintaining a list of partners, suppliers, and contractors with their up-to-date contact details can help you identify and address any relevant security requirements .</p> <p>It is recommended that you check out the cyber security controls a third-party has in place.</p> <p>Security certifications demonstrate that an organisation has met a defined standard of cyber security and are usually available to see on their company website.</p> <p>Certifications your third-party suppliers may hold:</p> <ul style="list-style-type: none"> • IASME Cyber Baseline • IASME Cyber Assurance • ISO27001 • SOC2 • COBIT5 • PCI-DSS

<p>2. Third Party Data Access</p> <p>a. Your organisation must understand and manage the access third parties have to your organisations data.</p>	<p>You should ensure that any partners, suppliers and contractors are only given access to your organisations data/information that is needed, as well as conducting frequent reviews on the access they hold.</p>

 <p>IASME CYBER BASELINE</p>   <p>IASME CYBER ASSURANCE</p>	<p><i>Taking the next step...</i></p> <p>Consider the risks and opportunities presented by your partner, supplier, contractor relationships beyond the minimum IASME Cyber Baseline requirements. For example, are your suppliers reliable enough to meet your needs in time? What vulnerabilities may you be introducing to your partners? Can you help each other improve security or respond and recover from an incident?</p>
--	---

Theme 3 – Assets

<p>What is this theme about?</p>	<p>Assets are your laptops, computers, servers, mobile phone, tablets, firewalls, routers, software, and cloud services used in your organisation to create, read, store and process data in your organisation. In order to apply the IASME Cyber Baseline controls, it is important you understand what assists you have.</p> <p>A regular review of your assets is important to help you identify those that have become unsupported (no longer receiving updates from the vendor/manufacturer) and can no longer meet the requirements outlined in Cyber Baseline.</p> <p>An asset register is a document or series of files that lists what you have, where it is and who is responsible.</p> <p>IASME can provide an asset register template.</p>
<p>Question set reference</p>	<p>C4.1 to C4.4</p>

What are the requirements for this theme?

<i>Requirements</i>	<i>Guidance for implementation</i>
<p>1. Keep an up-to-date register of your devices used to create, read, store and process data.</p> <p><i>Please note</i> - Your asset register must include any personal end user devices (BYOD) if you allow staff to use them for business purposes.</p>	<p>IASME Cyber Baseline requires you to include the following devices:</p> <ul style="list-style-type: none"> · End user devices. Examples include laptops, computers, mobile phones and tablets. · Networking equipment - Examples include firewalls and routers · Server devices

	<p>BYOD (Bring Your Own Device) is a widespread term for when a company allows employees to use their own laptops, tablets or phones for work purposes. This can introduce security issues because personal devices are less likely to be managed in the same way as organisation owned device. You should be aware of BYOD devices and keep a record of who has been allowed access to organisational data or services. You can restrict access of BYOD devices by checking they are running a supported operating system.</p> <p>IASME can provide an asset register template that can be adapted for most organisations.</p>
<p>2. Maintain a software inventory and implement this as an approved list of software that can be installed on your devices.</p>	<p>You should understand and maintain an asset register or inventory of the software you use within your organisation. By understanding what software is used will help you understand when it becomes unsupported and no longer receiving security updates.</p> <p>There are different types of software in use with in organisations, below is list of different types of software that need to be included in the register.</p> <ul style="list-style-type: none"> · Operating Systems on your end user devices such as Windows, macOS, IOS, Android, Linux · Commercial applications and other software programs such as, internet browsers, anti-malware, office applications, accounts packages etc. · Commercial extensions and plugins for software e.g., to add features to email clients or internet browsers

· Server Software including operating systems, virtualisation software(Hypervisors), virtual desktop software, email software, databases etc.

What does supported or unsupported software mean?

All software contains errors (often called, 'vulnerabilities') which cyber criminals can potentially use as openings to access data. Within a piece of software's functioning life span, as soon as an error or 'vulnerability' is discovered, the manufacturer creates some additional code to correct the error. This is known as 'patching'. All modern software will need to 'update' on a regular basis (at least every 14 days) as part of its maintenance. This 'support' ensures that the latest vulnerabilities that have been discovered are patched within 14 days of the update being made available by the software vendor. When software gets to a certain age, the manufacturer will cease to create and send out patches. At this point, the software is classed as no longer supported or 'end of life' (EOL). It is no longer secure to use and not compliant for Cyber Baseline. What is an 'approved list'?

What is an 'approved list'?

An 'approved list' is a list of software that is identified as necessary and appropriate for use within the organisation and is approved to be installed on your devices. You can achieve this with a technical solution or maintain a documented software asset register.



Taking the next step...

As you track your devices and software, begin to think about the different types of information you use such as customer/employee details and product information. Consider where it used and who should be able to access it.

When you have implemented the IASME Cyber Baseline controls, you can expand your device and software registers to track data based on its sensitivity and value to your organisation to help you manage it securely.

Theme 5 – Secure architecture

<p>What is this theme about?</p>	<p>IT Systems are often designed for ease of use or accessibility, but they are not secure by default. It is important to understand how your systems work together and how they are configured, in order for the controls of IASME Cyber Baseline to be applied and the different components to be protected.</p> <p>There are a number of easy to apply technical controls that need to be applied to your devices, that will help reduce the chances of a cyber-attack. Always check that these secure configurations are in place and monitored, rather than assume they are applied by default.</p>
<p>Question set reference</p>	<p>C5.1 to C5.6</p>

What are the requirements for this theme?

<p><i>Requirements</i></p>	<p><i>Guidance for implementation</i></p>
<p>1. Understand how your IT systems work together and any dependencies between them.</p> <p><i>You could achieve this by developing a simple diagram</i></p>	<p><i>What aspects of your network do you need to understand?</i></p> <p>IASME Cyber Baseline expects you to be able to understand where the boundary is between your organisation's IT systems and the wider internet, and how your networks and devices connect to each other.</p> <p><i>Cloud only organisations</i></p> <p>Not all organisations have their own private networks, instead, many use the internet to connect all their devices to access the cloud services. In this setup, the software firewall on the devices is the boundary.</p>

<p>2. Device management</p> <ul style="list-style-type: none"> • Ensure that all software not in use has been removed or disabled on all devices • Ensure that all devices only contain necessary user accounts 	<p>When devices and operating systems are new or first installed they often include software that won't be used. This software should be removed. Having software that is not used and maintained can introduce vulnerabilities to your devices and by removing this software, you reduce the options for an attacker. For older systems regular checks should be made to review what software is no longer used or required, and it should be removed.</p> <p>In a similar way, accounts that are not required or no longer in use should be removed.</p>
<p>3. Change default passwords</p> <ul style="list-style-type: none"> • Default passwords must be changed on all devices before they are used. 	<p>Many devices out of the box are set up with default configurations which includes a default access password. These default passwords can be easy to find on the internet and are known by attackers. It is important to change the password to something unique, that is hard to guess before the device is used.</p>
<p>4. Disable any features that will allow applications to run automatically on all your systems.</p>	<p>In common operating systems, there is a feature known as 'auto-run' or 'auto-play'. This allows programs, media and storage devices to run automatically when detected. When enabled, the auto-run feature can allow automatic installations of unauthorised software e.g. malware.</p> <p>It is important to check that this feature has been disabled, rather than assuming it has been disabled by default.</p>
<p>5. Lock devices</p> <ul style="list-style-type: none"> • All devices that require user interaction must be set to lock after a set period of time. 	<p>There needs to be a locking mechanism in place on each device to access the software and services installed. It is recommended that the device locks after 10 minutes of inactivity and users should be required to unlock the device using a password, PIN or biometrics.</p>




Theme 7 – People

<p>What is this theme about?</p>	<p>This theme is about making sure your staff are aware of your cyber security policies and processes and know what to do to keep your systems and data safe.</p> <p>How does your organisation understand its people and make them aware of your cyber security protections and incident management?</p>
<p>Question set reference</p>	<p>C6.1 to C6.3</p>

What are the requirements for this theme?

Requirements	Guidance for implementation
<p>1. Staff awareness</p> <ul style="list-style-type: none"> • Ensure all staff are aware of your policies and processes that protect your organisations services and data. • Staff awareness must be conducted at least annually. • Ensure staff are aware of how to create passwords that are difficult to guess. • Appropriate training should be given to all staff during induction and upon changes to company policies and processes. 	<p><i>Who do you need to include in security awareness?</i></p> <p>You need to provide awareness training to all permanent and temporary staff, whether full or part time, on contract, paid or unpaid. If you use contractors/third parties, ensuring awareness should be included within your contractual agreements.</p> <p><i>How should I deliver security awareness, and what does it need to cover?</i></p> <p>The awareness training you provide can be delivered by live or pre-recorded courses or workshops - in person or online, using 'how to' documents or good practice guides.</p> <p><i>How often should you repeat security awareness activities?</i></p> <p>It is recommended that any activity is carried out annually.</p>

	<p>As part of your awareness training you must ensure that staff are aware of password creation best practices.</p> <p>This should cover:</p> <ul style="list-style-type: none"> • Use of unique passwords for each system • Generation of secure passwords that are difficult to guess and are a minimum of 12 characters. A recommended method is to choose a password or passphrase made up from three random words. • The use of password management applications.
--	---

 <p>IASME CYBER BASELINE</p>   <p>IASME CYBER ASSURANCE</p>	<p><i>Taking the next step...</i></p> <p>As your cyber security capabilities develop, your training will become more tailored to also cover topics relating to specific security roles, responsibilities, and risk-based organisational policies.</p>
---	---

Theme 9 - Managing access

<p>What is this theme about?</p>	<p>In order to conduct your organisations day to day business on your IT systems, your staff will need to have user accounts. An important security principle is that they have just enough access to carry out their duties, but no more. If a user account with too much access is compromised, it can lead to a data breach or malware attack.</p> <p>Administrator or admin accounts are used by people who are responsible for the settings and controls of the computer and IT systems. These accounts have extra permissions to access files, install software and manage other user accounts. Protecting and controlling access to administrator accounts is very important for preventing any unauthorised access and system changes. In IASME Cyber Baseline the principle of ‘just enough’ access on user accounts is required. Carrying out work with a user account will prevent most malware and other malicious programs and apps from installing. This is because the malware will have the same privileges as the account you are logged in as and a user account does not have the privilege to download new software.</p> <p>This leads on to the second principle of using separate accounts for different tasks. Everyone should use standard user accounts for day-to-day activities, such as reading and writing emails, creating documents etc. The administrator account should only be used when a task absolutely has to be done that a standard user account is prohibited from doing. During normal use it is always best to log in to a regular user account.</p> <p>As the usage of cloud services has increased, it is important to protect your user and administrator accounts with multi-factor authentication (MFA).</p>
<p>Question set reference</p>	<p>C7.1 to C7.12</p>

What are the requirements for this theme?

Requirements	Guidance for implementation
<p>1. Inventory of accounts</p> <ul style="list-style-type: none"> You must have a record of all accounts that are used for carrying out day-to-day business activities. 	<p>It is important your organisation understands the user and administrator accounts that are in use within your organisation. Having an inventory of accounts will help to keep track of when accounts are no longer used or required. It is important this inventory is regularly reviewed, and the recommended review period is every 6 months.</p>

<ul style="list-style-type: none"> You must have a record of all accounts that have administrator privileges 	<p><i>Template available:</i></p> <p>IASME can provide an <i>administrator privilege tracker</i> template that can be adapted for most organisations.</p>
<p>2. Ensure that people only have access to your data if they need it.</p> <ul style="list-style-type: none"> You must have a clear process for granting individuals access to your organisations data and services. Restrict the provision of administrator privileges to dedicated accounts. Accounts with administrator privileges must be used for administrator tasks only. Disable dormant accounts and delete accounts that are not needed. Account access including administrator access, must be reviewed at every 6 months. 	<p>When assigning access to your organisations data and services, you should create user accounts that provide staff with ‘just enough’ access to carry out their day-to-day activities.</p> <p>All users should be issued with a unique user account assigned to them as an individual. User accounts where more than one individual share a username and password are not compliant.</p> <p>You should have an understanding of what access is required for different roles and an awareness of when these access permissions are assigned to individual users.</p> <p>What are dormant and unnecessary accounts?</p> <p>A dormant account is one that hasn’t been used for some time, and after a set period of time should be removed from devices and services. It is recommended that an account is considered dormant after 30 days of inactivity.</p> <p>It is important to be aware of and track all accounts used to access your organisations data and services. User access and administrator accounts must be reviewed at least once every 6 months.</p>
<p>3. Password Management</p> <ul style="list-style-type: none"> You must have a password policy in place, which must contain password requirements and what to do in the event of a suspected password compromise. 	<p>All passwords should be set to a minimum of 12 characters and be hard to guess. Avoid ‘guessable’ information such as pet and children’s names, favourite football teams, home address and date of birth, all of which can all be easily discovered from a trawl through social media and online.</p> <p>In addition to username and passwords, multi-factor authentication must be used where available.</p>

	<p>It is also recommended that additional protections are put in place to reduce the risk of password guessing or misuse. These include:</p> <ul style="list-style-type: none"> · Throttling of attempts. This is where the user has to wait longer between each failed attempt and the account locks after 10 failed attempts · Blocking commonly used passwords, such as password123 QWERTY etc. and not allowing the user to reuse their last 5 passwords. <p>With the increasing use of passwords businesses may want to consider allowing their staff to use password management applications. Password managers can be user to generate hard to guess passwords.</p>
<p>4. Multi-factor authentication (MFA)</p> <ul style="list-style-type: none"> • MFA must be enabled on all cloud services for users and administrators <p>This is subject to being provided by the vendor. Where it is available it must be enabled.</p>	<p>Multi-factor authentication (MFA) is now common across cloud services and provides an extra layer of protection against common compromise. Having MFA enabled is considered cyber security best practice.</p>

Theme 10 - Technical intrusion

<p>What is this theme about?</p>	<p>This is all about how you are protecting your systems and data.</p> <p>By applying technical configurations on your device to operating systems, firewalls and malware protection you are creating layers of protection. This is often referred to as 'defence in depth'.</p> <p>This theme outlines the technical configurations required for IASME Cyber Baseline</p>
<p>Question set reference</p>	<p>C8.1 to C8.11</p>

What are the requirements for this theme?

Requirements	Guidance for implementation
<p>1. Firewalls</p> <ul style="list-style-type: none"> • Implement and manage firewalls at your internet border on all computers, laptops and servers • Default passwords must be changed on all firewalls before use. • Inbound communications must be blocked by firewall configurations. • Multi-factor authentication must be used to access routers and firewalls. 	<p>If the firewalls can be accessed over the internet, it is a good idea to have mechanisms in place to permit only the people who need to access your configuration. For example, the firewall or router might be configured to allow access to an external IP address or range that only your supplier uses, or it might be configured to require multi-factor authentication.</p> <p>Firewalls are the first line of defence between your devices, networks and the internet. These need to be configured correctly to prevent an attacker gaining access to your devices or networks.</p> <p>Firewalls can come in two forms:</p> <ol style="list-style-type: none"> 1. Physical - a physical firewall or router is a device designed to specifically provide you with a connection the internet and create a security border. 2. Software - most computers and laptops have a firewall built into their operating systems. Software firewalls are also common on virtual server networks.

	<p>The following requirements must be configured on all of your firewalls.</p> <p>Make sure all devices and networks are protected with a correctly configured firewall, and don't just assume they have been setup correctly by default.</p> <ol style="list-style-type: none"> 1. Default password - Change the default password on all of your physical firewalls and routers. The default password for physical firewalls and routers are often available on the internet 2. Multi-factor authentication - Where possible enable multi-factor authentication to access all firewalls and routers. 3. Change any default passwords on your operating systems as this can give an attacker access to your software firewall. 4. Remote access to a firewall or router device must be configured securely using MFA of a trusted IP address. Ideally remote access to these devices should be blocked and only configured from within your networks and not across the internet. 5. Most firewalls are set to block all inbound connections, this need to be checked and turned on incase it has not been set by default.
<p>2. Operating systems and applications</p> <ul style="list-style-type: none"> • All operating systems, applications and cloud services in use must be correctly licensed and supported by vendors. • Critical and High security updates released by vendors must be installed within 14 days. 	<p>All software including operating systems, applications and cloud services can contain vulnerabilities and these can be exploited by attackers to gain access to your data and systems.</p> <p>Only install licensed and supported software that is receiving security updates. These updates will be free or included as part of the support package from the software provider.</p> <p>All critical and high security updates must be applied within 14 days of being released by the vendor.</p> <p>Unsupported software must not be installed or be in use as this will introduce vulnerabilities that can be used by attackers to gain access.</p> <p>Unsupported operating systems will not be accepted for the IASME Cyber Baseline standard and will result in an automatic failure of the assessment.</p>
<p>3. Anti-malware</p>	<p>Malware is software that is designed to damage, disrupt, or give unauthorised access to laptops, computers, servers and mobile devices.</p>

<ul style="list-style-type: none"> • Anti-malware protection must be deployed on devices • Anti-malware software must be set to automatically update • Anti-malware software must be configured in line with the vendors best practices and recommendations • You must maintain an application allow list for mobile phones and tablets. 	<p>To protect your devices and provide another layer of protection against cyber attacks, malware protection should be deployed. This can be achieved by installing or using the pre-installed malware protection on laptops, computers and servers. There are many providers of malware protection, but best practice is to:</p> <ul style="list-style-type: none"> • configure against the vendors best practices and recommendations • Auto update <p>For mobile phones and tablets, limiting downloads to apps that are listed on an application allow list can help prevent malware to those devices. The list must be maintained by the organisation and identify approved apps that can access the organisations data. The list must use apps from a reputable trusted sources from which the apps can be downloaded e.g. Google play store or Apple App Store.</p>
--	--

Theme 11 - Backup and restore

<p>What is this theme about?</p>	<p>In the event of a cyber incident where data has been lost, deleted or encrypted, having a backup will help you recover to a point in time before the event happened. Regularly backing up your data and systems, and being able to restore is the most effective way to recover from data loss.</p> <ul style="list-style-type: none"> • Does your organisation back up data regularly? • How does the organisation create and secure backup copies? • Can the organisation show its confidence in the restoration of backups to complete, operational capability?
<p>Question set reference</p>	<p>C9.1 to C9.4</p>

What are the requirements for this theme?

Requirements	Guidance for implementation
<p>1. Back up</p> <ul style="list-style-type: none"> • Back-ups of all data and systems must be created at least weekly • All backup data should be stored securely • Back-up data must be clearly segregated from working and live data. • You must have a back-up restoration process that is tested at least quarterly 	<p>Regularly backing up data, and having the ability to restore the backup, may be one of the most effective methods of protecting your business from the effects of accidental or malicious tampering such as deleting data, hardware failure, or ransomware.</p> <p>Important: Usage of a cloud system does not guarantee that your data has been backed up. You should check with your cloud service provider if your data is backed up and stored separately from your working data. Replication of data is not a separate backup, and you may need to find alternative ways to back up your data held in cloud services</p> <p>Backing up weekly means that you may only lose up to one weeks worth of data if something goes wrong. If losing a weeks data would be too costly, you should consider backing up your data daily.</p> <p>IASME Cyber Baseline only requires you to have one backup, though you may decide to increase your resilience to incidents by keeping multiple backups.</p> <p>Backup Storage</p> <p>Protect backups so that they cannot be altered or deleted once created, especially whilst your backup mechanism is connected to your IT systems. When using USB devices for backup data, disconnect these devices when the backup has completed and store in a secure location. Alternatively, use a backup service or store your backup data at a different secure location.</p> <p>Test and restore</p> <p>A backup that fails during a data restore process will not help you recover from data loss. You must carry out regular backup tests to ensure you can recover from data loss and regular restore tests should be carried out quarterly to verify the backup is usable.</p>




Theme 13 - Resilience: business continuity, incident management, and disaster recovery

<p>What is this theme about?</p>	<p>No security measures are 100% effective so you need to be prepared for what to do if an incident happens. A cyber security incident means that the IT systems or data has been threatened. Examples include unauthorised access, compromised accounts and malware attacks.</p> <p>Creating and testing an incident management plan will help you manage an incident.</p> <p>It is important to make users of your IT systems aware of how to identify and report cyber incidents.</p>
<p>Question set reference</p>	<p>C10.1 to C10.3</p>

What are the requirements for this theme?

Requirements	Guidance for implementation
<p>1. Incident reporting</p> <ul style="list-style-type: none"> Ensure all staff know how to report security incidents and to whom. 	<p>It is essential that people know how to report cyber security incidents. This should be included as part of your organisations cyber security awareness activities.</p>
<p>2. Incident management plan</p> <ul style="list-style-type: none"> You must have a documented incident management plan that includes how to respond to security incidents. You must ensure that your plan is reviewed at least annually 	<p>If an incident occurs you will need a plan to deal with it. In order to be prepared, this plan should be tested on a regular basis.</p> <p>The IASME Cyber Baseline themes include controls that are required for your incident management plan.</p> <p>The key areas you should include in your plan are:</p> <ul style="list-style-type: none"> The steps to be taken once reported, including any calls for help you make take to a third party Who will be responsible for specific activities How will you communicate internally and externally

	<ul style="list-style-type: none"> • The business functions that you will need to remain operational during the incident. These may have to revert to manual processes. • How you manage lessons learned <p>Whether you have your own cyber-incident response capability or rely on external services, having a list of contact numbers prepared in advance can really help during the stress of dealing with an incident. Preparation allows you to contact support immediately, rather than potentially let incidents worsen whilst you look for someone who can help. Some IASME Certification Bodies can provide an incident response service, and your cyber liability insurance provider may have preferences or recommendations too.</p> <p>Consider your responsibilities for reporting incidents to customers and external authorities, as well as how you will contact supply chain partners and other stakeholders.</p> <p>Review</p> <p>Test and review your plan at least annually and keep it up to date to account for changes to your business, or to the services and authorities that you might need to involve when incident occurs.</p>
--	--

 <p>IASME CYBER BASELINE</p>   <p>IASME CYBER ASSURANCE</p>	<p><i>Taking the next step...</i></p> <p>As you develop your plans for responding to incidents, think about any specific roles that may need assigning such as handling incident communications.</p> <p>Consider which systems you might need to prioritise recovering first in an incident so that your organisation can continue day-to-day operations.</p>
---	---



	<p>You can find free guidance on developing incident response plans in the IASME Cyber Assurance Standard [INSERT LINK] and in our Business Impact Assessment and Business Continuity and Disaster Recovery Plan template that can be adapted for most organisations.</p>
--	---



APPENDICES

Appendix A – Compatibility with regulation and other cyber and information security standards

Center for Internet Security (CIS) Controls

This is a catalogue of 18 controls – or control areas – set out by the USA's Center for Internet Security (CIS) and the SANS Institute. Formerly known as the Critical Security Controls, and designed with critical infrastructure in mind, they comprise a detailed set of activities commensurate with fighting 'most pervasive and dangerous attacks'.

For an SME in particular, the IASME Cyber Baseline standard provides the foundations for adopting these protective measures for high impact assets such as Industrial Control Systems (ICS), including supervisory control and data acquisition (SCADA) systems which collect and process data for control processes.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS compliance is mandated by the payment card suppliers for businesses handling payment card data. It is essentially risk agnostic and dictates that if you handle payment card data, you must implement specific controls (as set out in that standard).

Appendix B – Glossary

Term	Definition
Business	See <i>organisation</i>
Business continuity	The activity of keeping your business operational with your regular expectations of quality, and preserving the <i>confidentiality, integrity, or availability</i> of your information assets.
BYOD	Bring Your Own Device. A term often used to describe people using their own, personal devices (such as mobile phones and computers) for work rather than equipment supplied by the organisation.
Cloud services	A service provided from one or more remote servers that is available for use in another location. Providing computer resources for processing, storage, or applications as a utility on demand.
Third party	Third parties are often taken on to carry out a specific task for your organisation. This Standard uses the term third party to refer to when you have a relatively close relationship with the other party. Consequently, you are more likely to undertake relevant activities to ensure they meet security requirements, such as providing training. The terms “third party”, “contractor” and “supplier” are closely related and have become increasingly blurred. See <i>supplier</i> .
Control	The practical measures that you put in place to protect your information assets from risks.
Cyber security	The assurance of confidentiality, integrity, and availability of information stored and processed on electronic devices that are usually interconnected.
Data Breach	An incident that leads to a compromise of the confidentiality, integrity, or availability of information. This may be accidental or deliberate.
Data subject	Any individuals identifiable from either a single piece of data or where multiple items are combined.
Devices	For the purposes of IASME Cyber Baseline ‘devices’ are the following laptops, desktop computers, servers (physical and virtual), mobile phones, tablets, firewalls and routers.
Disaster recovery	The process of returning to a state of business-as-usual after a significant incident. This may mean a change in working practice as a result of the incident to meet expectations of quality and preserving the confidentiality, integrity, of availability of your information assets.
Boundary	The physical or virtual areas where your organisation has a presence.
Information asset	Processed and unprocessed data and the equipment that is used to store, process, or transmit it, that has value and impact to a business, its stakeholders, its supply chain, or other interested parties. This includes your intellectual property.
Information risk	The magnitude, and likelihood, of a loss of information’s confidentiality, integrity, and availability.
Information security	A state of confidentiality, integrity, and availability commensurate with the value of the information under scrutiny.

Integrity	The state of information being accurate, consistent, and untampered with.
Organisation	A single person, or a group of people, that can be defined as an entity for private, public, or third sector objectives. This term is used interchangeably in this standard with 'Business'.
Personal data	Any information relating to an identified or identifiable natural person – a 'data subject'. (Source: EU Regulation 2016/679, Official Journal of the European Union EN 4.5.2016)
Policy	A premade decision that sets out the rules, guidelines, and regulations that you require people to follow.
Privilege	The ability to do something with information. This can range from accessing, viewing, changing, or creating information assets, to destroying or deleting them. Note that privileges may be granted by default and a physical or virtual control may be needed to remove this if appropriate.
Resilience	The ability to adapt to a change in circumstances whether in response to planned or predicted events, incidents, or opportunities.
Responsible	The person, or group of people, conducting a set of tasks under the authorisation of an accountable individual. Note that the accountable individual may take on the responsibility to complete tasks themselves.
Risk	The magnitude, in terms of impact, and likelihood of a particular threat event occurring.
Role	A defined set of responsibilities. One person may hold multiple roles, or sometimes a single role may be shared between a team. See responsible.
Security	A state of grace wherein the assets under scrutiny are adequately protected from the realisation of risks to them.
Security breach	See security incident.
Security event	Something that happens contrary to the accepted security policy. An event – or series of events – may lead to a security incident
Security incident	Something that happens to compromise the confidentiality, integrity, or availability of information assets.
Sensitive personal data	A subset of personal data which has greater ramifications if involved in a security incident. Sensitive personal data can include, but is not restricted to, racial or ethnic origin, personal political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning a person's health, sex life, or sexual orientation.
Software	
Supplier	Suppliers traditionally only supplied goods to an organisation, but increasingly also supply services. In this standard, we use the term "supplier" where the other party typically holds the responsibility for necessary security activities. The larger the supplier organisation, the more common this is, for example, due to practicality. The terms "third party", "contractor" and "supplier" are closely related and have become increasingly blurred. See contractor.

Threat actor	This can include, but is not restricted to, hacktivists, financial criminals, terrorists, industrial spies, disgruntled insiders, disgruntled former staff, well-intentioned insiders, information security professionals, and script kiddies.
Threat landscape	The collection of different threats that can be found within a particular context.
Vulnerability	A weakness that can be exploited.

Appendix C – Common scoping scenarios and examples

<p>Common scenario - Your organisation can manage the network infrastructure.</p> <p><u>Example:</u> office locations (shared or exclusive use) and where your organisation has provided remote workers with networking equipment.</p> <p>Where your organisation can manage the network infrastructure, the starting point for defining the network border is simpler. A network border will be at your router (the box your Internet Service Provider gave you unless you have purchased your own).</p> <p>Your router will typically include a firewall, although, you may also use a separate firewall device, or virtual equivalent on virtual networks.</p> <p>Where your organisation can manage the network infrastructure, the software firewall on individual end-user devices cannot be relied on.</p>
--

<p>Common scenario - Your organisation has limited or no ability to manage the network infrastructure.</p> <p><u>Example:</u> office locations (shared) and remote workers using personal (possibly home) networks.</p> <p>Remote workers</p> <p>Remote workers are people that access the organisations services and data from a network that is not managed by the organisation. An example of this is homeworkers.</p>

If a remote worker's device is connected via a single tunnel corporate VPN to an organisation-managed network, you should consider their devices as if they are inside the borders you defined for the organisation-managed network. This scenario will typically only be relevant to you where you have deliberately set this up.

In all other circumstances, remote worker devices should be considered connected to untrusted networks as you do not fully manage the infrastructure, including its security arrangements. Instead, you will need to manage these devices on an individual level. This will mean relying on software firewalls on the device to define your borders.

Managed Service providers

If the organisation is using a managed service provider that you have contracted directly to maintain a network, then this network should be considered under your organisation's control. All controls apply as and you should enforce this through your contracts with them.

Appendix D – The Themes for guidance only

Theme 1 - Planning information security

This theme in the IASME Cyber Baseline Standard is for guidance only.

What is this theme about?	Planning is about making decisions in advance. Some planning relates to your day-to-day activities, such as serving customers or manufacturing a product. Other planning might be focused on a particular project to ensure that you have considered its security impact. You also need to plan how to react to certain events such a cyber-attack or an error made by a member of staff or contractor. As part of this theme, you should consider:
----------------------------------	--

- How do you build right-sized security into all your business activities?
- How do you consider the security impact of change on your staff, customers, and other stakeholders, your working practices, hardware and software?

You will probably do some cyber security planning already, even if only informally. For example, in reading this standard you will think about how cyber security will affect your current and future activities and make decisions about how to implement the requirements in a way that harmonises security with your organisational objectives.

Theme 4 – Legal and regulatory landscape

This theme in the IASME Cyber Baseline Standard is for guidance only.

What is this theme about?

Every business has certain legally enforceable obligations associated with company registration, accounting, managing customers, use of technology, handling data, and other business processes. There will be other obligations that may be sector specific, for example, those relating to contractual or licensing agreements. You must be aware of what these are and ensure that you are fulfilling your responsibilities.

Theme 6 - Physical and environmental protection

This theme in the IASME Cyber Baseline Standard is for guidance only.

<p>What is this theme about?</p>	<p>Protection of your information assets extends to the physical protection needed to prevent theft, loss, or damage. Protective measures are often common-sense actions such as locking doors and windows, installing window bars, and video surveillance, as determined by a risk assessment. However, protective measures include controlling environmental conditions like temperatures or humidity, where needed, to safely operate certain equipment. Consider:</p> <ul style="list-style-type: none">· How does the business protect its information assets from the exposure and realisation of physical threats and environmental harm?· Have the risks of different working environments been considered, such as, operating at your usual premises, traveling, or working elsewhere?· How does the business lock away confidential information that isn't in use and keep it out of sight from those unauthorised to see it when it is?
----------------------------------	--

Theme 8 - Policy realisation

This theme in the IASME Cyber Baseline Standard is for guidance only.

What is this theme about?	<p>Policies specify the rules, guidelines, and regulations that you require people to follow. They also reflect the values and ethics your business holds dear. Your information security policies should be comprehensive, yet also be 'right-sized'. This will enable you keep to the decisions about how you manage security at your fingertips. Consider:</p> <ul style="list-style-type: none">• How does the business create policies and distribute them on a need-to-know basis?• How does the business support the implementation of these policies and check that they are not only being implemented but that they still satisfy its risk appetite pragmatically?
---------------------------	---

Theme 12 - Secure business operations: monitoring, review, and change management

This theme in the IASME Cyber Baseline Standard is for guidance only.

What is this theme about?	<p>Secure business operations means the carrying out of security activities in a 'business-as-usual' way. Consider:</p> <ul style="list-style-type: none">• How does the business nurture the way that business is done so that it is done securely?• Which business scenarios does the business track and monitor for acceptable activity and how does it identify the unacceptable?• How does the business manage and monitor its information systems, including policies and processes to ensure they remain contemporary and effective?
---------------------------	---

	<ul style="list-style-type: none"> How does the business keep an eye on who is trying to access its information and where they are trying to access it from? <p>You should be prepared and ready to act on the intelligence your monitoring provides, yet you must ensure that changes are done in a controlled manner to ensure that any corresponding risks are identified and addressed.</p>
--	--

Appendix E - The IASME family of practical information and cyber security certifications

The IASME Cyber Baseline standard is part of a family of information security standards offered by IASME Consortium, often in partnership with external organisations. The table below provides further information on IASME's other schemes and how they fit alongside IASME Cyber Baseline

Scheme	Description	Level 1 Verified assessment	Level 2 Third party testing/audit
IASME Cyber Baseline	Core set of technical cyber security controls for organisations	✓	✓
IASME Cyber Assurance	Complete set of cyber security and information security controls for organisations	✓	✓
IASME IoT Cyber Assured	Complete set of cyber security controls for IoT devices	✓	✓
IASME Maritime Cyber Baseline	Core set of cyber security controls for ships (to meet IMO requirements)	✓	✓