



**IASME
CYBER
ASSURANCE**

THE IASME CYBER ASSURANCE STANDARD V6.0

(Formerly known as IASME Governance)

© IASME Consortium Limited 2022

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 |
|----------|------------|---|
| 6.0 | April 2022 | Detailed revision, restructure, and full update of the standard. Rename of standard from IASME Governance. |
| 6.0a | May 2022 | Re-name Assured to Assurance |

CONTENTS

| | |
|---|----|
| Modification History | 2 |
| Contents | 3 |
| Chapter 1 - Introduction..... | 5 |
| The need for information security..... | 5 |
| The aims of the IASME Cyber Assurance standard..... | 5 |
| What are the business drivers for applying the IASME Cyber Assurance standard?..... | 6 |
| Compatibility with regulation and other standards..... | 6 |
| How to use this document..... | 7 |
| Normative references..... | 7 |
| Chapter 2 – How the IASME Cyber Assurance standard works | 8 |
| Understanding your organisation – and defending it..... | 8 |
| Learning from your risk assessment and making changes to become more secure | 9 |
| Showing customers, suppliers...and yourself..... | 10 |
| The assessment and certification process | 11 |
| Who governs the Standard?..... | 13 |
| Chapter 3 - Scope..... | 14 |
| How to scope your organisation for certification..... | 14 |
| Chapter 4 - The thirteen themes: requirements and guidance..... | 16 |
| How the thirteen themes are formatted | 16 |
| Available templates and supporting guidance | 17 |
| Duplication | 17 |
| Theme 1 - Planning information security..... | 18 |
| Theme 2 - Organisation..... | 19 |
| Theme 3 - Assets | 22 |
| Theme 4 – Legal and regulatory landscape | 27 |
| Theme 5 – Assessing and treating risks | 31 |
| Theme 6 - Physical and environmental protection..... | 39 |
| Theme 7 - People | 42 |
| Theme 8 - Policy realisation | 47 |
| Theme 9 - Managing access | 52 |



| | |
|---|-----------|
| Theme 10 - Technical intrusion | 56 |
| Theme 11 - Backup and restore | 59 |
| Theme 12 - Secure business operations: monitoring, review, and change management..... | 63 |
| Theme 13 - Resilience: business continuity, incident management, and disaster recovery | 70 |
| Appendices | 75 |
| Appendix A – Compatibility with regulation and other cyber and information security standards | 75 |
| Appendix B – Carrying out your information risk assessment | 79 |
| Appendix C – Information security policies..... | 83 |
| Appendix D – Glossary | 94 |
| Appendix E – The IASME family of practical information and cyber security certifications..... | 99 |

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.

Increasing reliance on information systems has made good information security a fundamental requirement. The types of data that need protecting have grown over the years and include information about customers, clients, finances, details of how products are manufactured, communications via instant message/email and so on.

Organisations often overlook the need to protect information in their spending priorities because information (a term which we will use interchangeably with “data”) is often difficult to value; its true worth may only be realised after it has been lost or damaged.

While there can be no guarantees for information security, we can use security frameworks and standards to guide organisations on how to reduce the risks to information – and their impact – to an acceptable level to prevent disruption to the organisation.

Unfortunately, many security frameworks have historically been created with large corporations in mind, where size and resources give them the ability to implement complex protective measures.

By contrast, smaller or more flexible businesses and organisations need to deal with information security with greater flexibility and with much smaller budgets. The structure of rigid procedures that support the internal communications in large organisations must give way to the informal cultures of small to medium-sized enterprises (SMEs), including where people are working alone or in a partnership.

The IASME Cyber Assurance standard was created specifically to address these needs.

The aims of the IASME Cyber Assurance standard

The Cyber Assurance standard is a formal information security methodology that is particularly accessible to SMEs but can be applied successfully to any organisation. It is sector agnostic and provides a working framework to assure information security against the background of contemporary threats.

The standard is designed to provide clear, simple to understand guidance to applicants and then to provide a high-quality, independent assessment of the level of maturity of an SME's information security.

Once assessed to the standard, applicants can use the certificate to assure customers/clients, supply chains and others that information stored and handled by the certified company is protected to a reasonable level for most practical purposes.

The IASME Cyber Assurance standard is an organised way for a business to implement new ways of securing its information, improve existing ones, and be recognised in its sector for having done so. It is also a great opportunity for those operating the business to improve their knowledge of security.

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

The IASME Cyber Assurance standard enables organisations to:

- Identify risks to their information and information systems
- Apply adequate barriers and controls to reduce the likelihood and impact of cyber incidents
- Reduce information risk at an acceptable level
- Proactively verify that the security controls that they implement provide the intended level of security
- Be independently reviewed by an assessor who will be sympathetic to their size and level of business risk to verify the effectiveness of their security activities
- Raise awareness of information risks with partners, stakeholders, the wider supply chain of which they may be part
- Work to a standard of information security within a supply chain regardless of size
- Give themselves, customers – including government procurement departments, and their supply chain – a level of assurance akin to ISO/IEC 27001 and similar standards
- Demonstrate to legal authorities the actions taken towards complying with applicable legislation and regulation such as GDPR

Compatibility with regulation and other standards

The standard has been compiled by SMEs for SMEs, originally with the support of the Technology Strategy Board (now Innovate UK). It provides common ground for SMEs alongside other information security standards – which are either not comprehensive or are too prescriptive in their level of complexity for an SME.

The standard maps closely to several widely recognised cyber security and assurance standards and guides. This means it can be used to demonstrate compliance to many of these standards. Some of these standards are put into context in Appendix A and mappings to standards are available at <https://iasme.co.uk/iasme-cyber-assurance/mapping-to-other-standards/>

The IASME Cyber Assurance standard requires attention to the respective laws and regulations that are applicable to the target of evaluation in general and those applicable to information security and safety arising from information collection, storage, processing, and disposal in particular.

The standard predicates itself on good practice and so avoids having to be reissued as legal systems change to deal with new technology or changes in its use.



GDPR:

The General Data Protection Regulation (GDPR) enshrines the basic principle of the IASME Cyber Assurance standard in law. It requires you to know what you are protecting and understand its relative value to its subjects and the impact of a security breach. Through this, protective measures can be put in place and routes to recovery planned in case of an incident. Additional supporting guidance for those seeking to implement the IASME Cyber Assurance standard in tune with the nuances of EU and/or UK GDPR is available at <https://iasme.co.uk/gdpr/>

How to use this document

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

- **Chapter 2** – explains how the IASME Cyber Assurance standard works to help you achieve a state of information security. In this section:
 - The thirteen IASME Cyber Assurance themes for information security 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 Assurance standard's thirteen themes, to create and manage your information security management system.
- **Chapter 4** – sets out the thirteen themes: requirements and guidance.
- **Appendices**
 - Appendix A – outlines the IASME Cyber Assurance standard's compatibility with other standards
 - Appendix B – includes guidance on carrying out your risk assessment with sample topics
 - Appendix C – contains guidance on creating an appropriate set of information security policies in line with Theme 8 - Policy realisation
 - Appendix D – glossary of information security terms used in this standard
 - Appendix E – details of IASME's family of information security standards

Normative references

- Cyber Essentials: Requirements for IT infrastructure
- IASME Cyber Assurance self-assessment questions

Depending on applicability:

- Ministry of Defence, Defence Standard 05-138, Cyber Security for Defence Suppliers

CHAPTER 2 – HOW THE IASME CYBER ASSURANCE STANDARD WORKS

Understanding your organisation – and defending it

The IASME Cyber Assurance standard is a route to maintaining a balanced state of information security so that you can focus on your core business objectives, without either limiting your activities by restrictive practices, or leaving yourself vulnerable to avoidable losses.

The standard is risk-led and your risk assessment (see [Theme 5](#)) will provide guidance on how you prioritise your activities. The controls within the standard form the baseline for protection of your organisation, with your risk assessment always guiding the depth of protection and any additional controls that may be needed.



Template available:

IASME can provide a risk assessment template that is suitable for smaller organisations

The depth of protection you need is not always linked to the size of your organisation – a small organisation with highly sensitive information assets may need to put more effort into protecting them than would a large company that deals with less sensitive information.

You will need to consider any number of threat ‘actors’¹ and potential events that might vary from invisible technical skulduggery to social engineering. Do they have the capability, the intent, and the opportunity to cause harm? And if they did, would the impact matter? Might you be the conduit to your customers who are the ‘high value’ targets for the attackers?

When reviewing risk, consider:

- How information systems are used
- How outsourced (including ‘cloud’) facilities are used
- Whether you and the people you work with use your own equipment for business (BYOD)
- How remote and mobile systems are used
- Awareness and attitude to the threat environment
- Estimated value of the business’ information assets, including physical equipment used and the data itself

¹ Including hacktivists, financial criminals, terrorists, industrial spies, disgruntled insiders, disgruntled former staff, well-intentioned insiders, and script kiddies.

Learning from your risk assessment and making changes to become more secure

Your risk assessment will guide the decisions made about the information security controls you need to put in place to keep it safe and resilient. These controls are the practical measures that you put in place to protect your information and technology.

It is best for these controls to be built into business processes so that security operates in harmony with the business and is indistinguishable from it as much as possible. You choose the controls based on your risk assessment and you can make adjustments at any time as the risks change.

The controls 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, look at the legal landscape, your risks, and begin to protect your assets by looking at physical security and the people involved in your security.

Protect:

This category focuses on putting in place good policies, controlling access to information, preventing technical attacks and backing up your information.

Detect and Deter

This category looks at business processes, including 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 good business continuity and disaster recovery processes.

The IASME Cyber Assurance standard breaks these four categories down into thirteen manageable, bite-sized themes, allowing you to easily control the pace at which you implement, improve, and measure the effectiveness of your information security (see Figure 1 below).

These controls are built upon the foundation of the organisation having achieved a basic level of technical cyber security. This comes from the mandatory requirement to achieve one of the pre-requisite schemes (Cyber Essentials or IASME Cyber Baseline), before applying for certification to IASME Cyber Assurance.

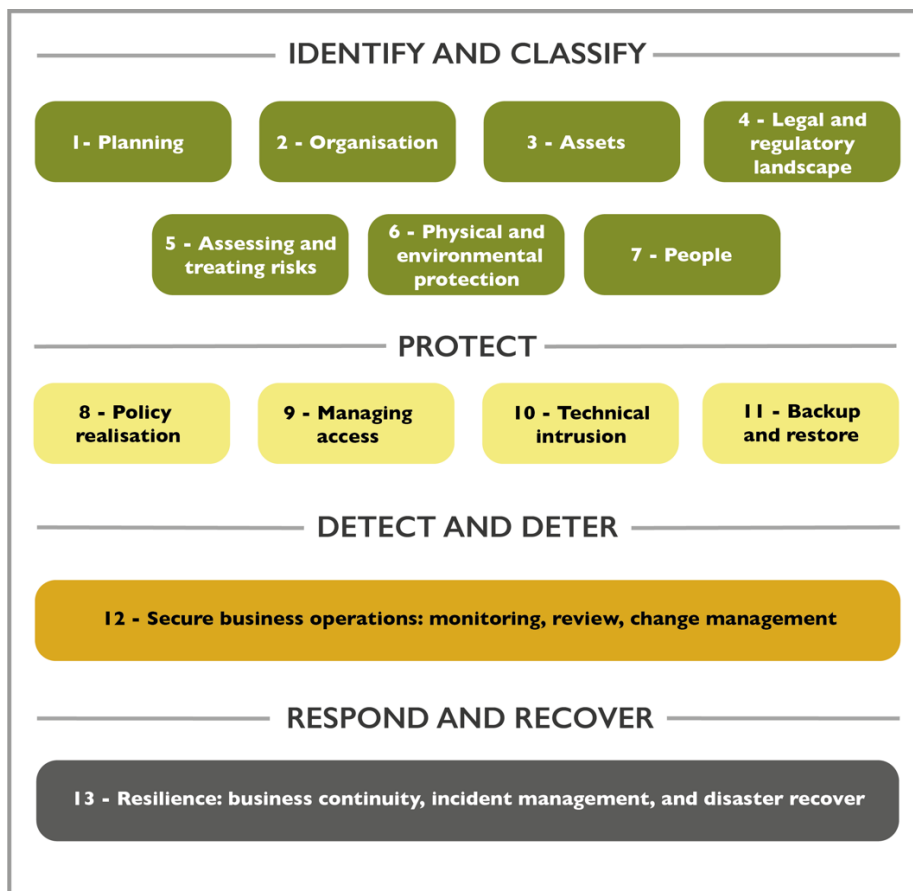


Figure 1 - The thirteen Themes of the IASME Cyber Assurance standard

Showing customers, suppliers...and yourself

The standard is a simple to understand process that produces a documented and objective measure of the level of security in your organisation. This is important and useful because it can be used to reassure your customers and supply chain that you will keep their information secure and that the products and services that you supply will not be interrupted by avoidable information security incidents. You can also reassure yourself that your company information is safe.

The standard and the question set are freely available to anyone who wants to download them from the IASME website (<https://iasme.co.uk/iasme-cyber-assurance/>). This means that your customers and suppliers can see exactly what is involved in the certification process and use it to verify your security.

The assessment and certification process

Certification Bodies and Assessors

IASME owns and operates the IASME Cyber Assurance standard, but the assessment of organisations is operated by IASME's Certification Bodies.

The Certification Bodies are companies with in-depth knowledge of information 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 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) | |
|---|--|
|  | <p>An award demonstrating an organisation's proactivity towards maintaining a reasoned state of cyber and information security.</p> |
| Following an audit by an IASME Certification Body (Level 2) | |
|  | <p>An award independently confirming that an organisation's achievement in cyber and information security is in line with industry expectations.</p> |

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

- **Level 1 (Verified self-assessment)**
 - The organisation achieves one of the pre-requisite schemes² (Cyber Essentials or IASME Cyber Baseline).
 - The organisation completes the online IASME Cyber Assurance 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.

² The prerequisite schemes are prescriptive and cover the foundations of cyber security with regards to the types of technology used. Further details can be found in [Chapter 3 - Scope](#).

- **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 looking at documentation, interviewing key staff and observing activities. This can be done in person or sometimes remotely (such as via a video call).
 - The draft report can be shared with the client to allow any issues identified to be addressed before ratification by IASME's moderators.
 - After the audit has been ratified by IASME's moderators, the organisation will achieve pass/fail depending on how well the organisation meets the standard.

The standard relies on a process of continuous assessment, with an initial cycle leading to your first certification, and continuing with assessments annually.

For Level 1 certification, the requirement is an annual resubmission of the IASME Cyber Assurance self-assessment using the online portal and maintenance of the pre-requisite scheme (Cyber Essentials or IASME Cyber Baseline).

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

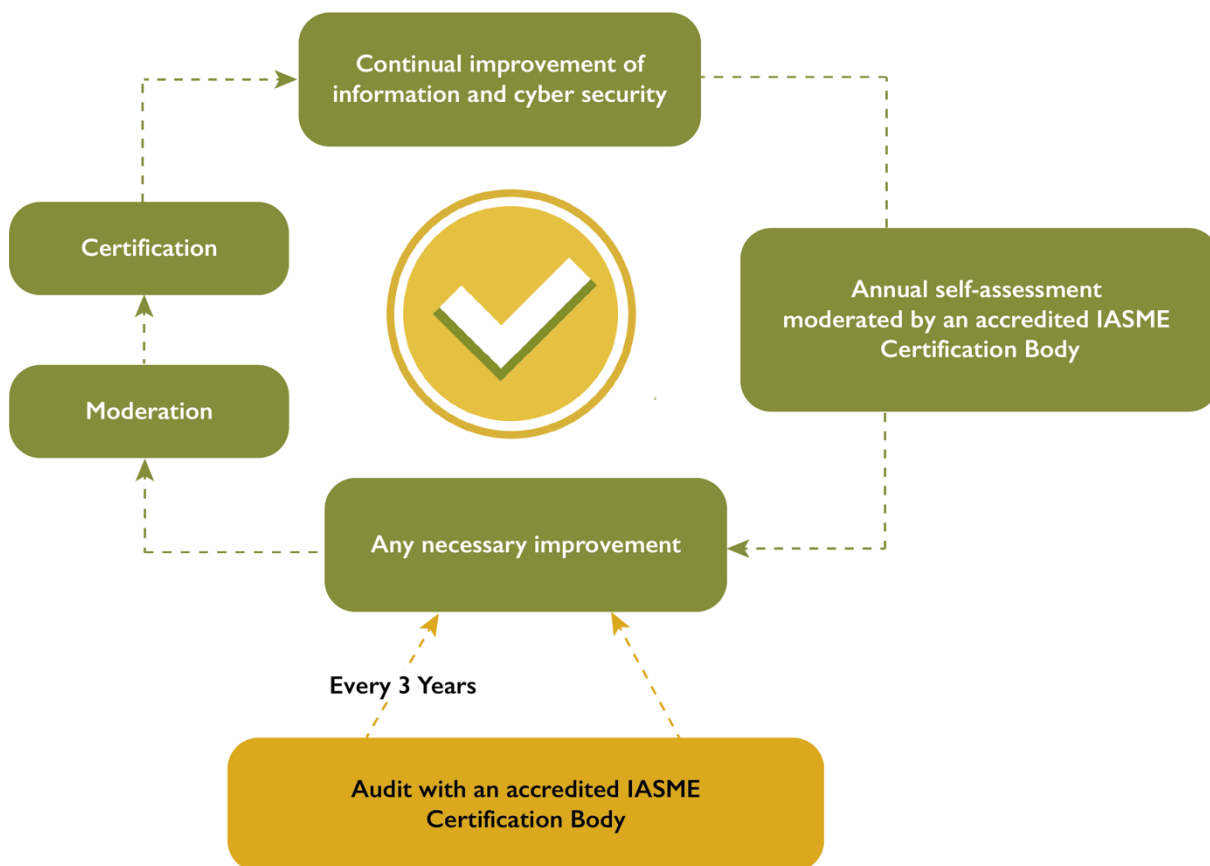


Figure 2: Round-tripping with the IASME Cyber Assurance implementation cycle

Who governs the Standard?

The development of the IASME Cyber Assurance standard is reviewed by an independent 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's dedicated support and customer services team. All Assessors are required to comply with a code of conduct which is accessible from IASME's website (<https://iasme.co.uk/wp-content/uploads/2020/03/Schedule-18-Assessor-Code-of-Conduct.pdf>).

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

A key part of the IASME Cyber Assurance standard is the role of the IASME moderators. These are experienced security auditing professionals who act as custodians of consistency and quality for the assessment process. Assessors act as a proxy for the moderators. It is the moderators who make the ultimate decision on certification for a particular organisation, which allows more flexibility for the Assessors to provide guidance and support to the client on how to comply with the standard.

This is a deliberate and important part of the standard – we believe that an end result of better information security is achieved if the Assessors are able to provide detailed guidance to clients on how to improve their security. The role of the IASME moderator allows this to happen whilst retaining the integrity and simplicity of the assessment process.

CHAPTER 3 - SCOPE

How to scope your organisation for certification

Perhaps surprisingly, scoping can be the most difficult part of certification! The ultimate aim of the standard is to certify your 'whole organisation' because this gives you the most protection and ensures you have embedded the controls appropriately.

But, the details of scope can be confusing, particularly for more complex organisations. The information below will guide you on what needs to be in scope for assessment.

There are three elements to consider for the scoping boundaries:

1. the technology used (both internet and non-internet connected technology)
2. the locations from which you operate
3. the people who can access your information assets

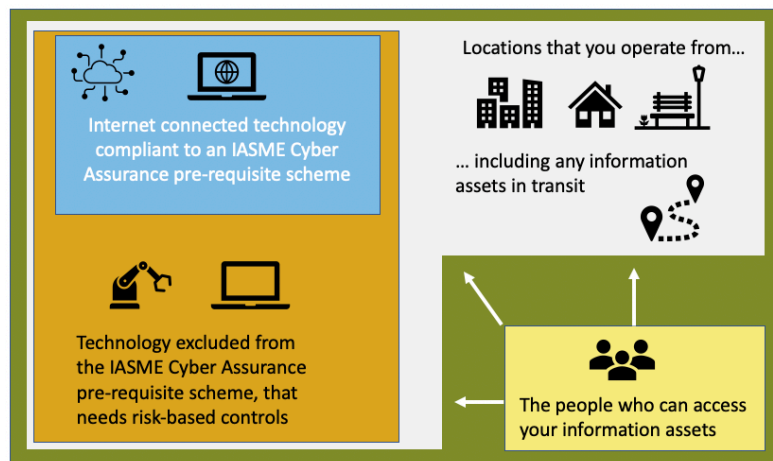


Figure 3 - The three components for defining the IASME Cyber Assurance scope

I – Your technology

The security of your technology is mostly covered by your achievement of one of the pre-requisite security schemes in table 2 below. For UK organisations, the pre-requisite scheme will be Cyber Essentials at the self-assessed level. We use these schemes to ensure that your organisation has basic technical cyber security in place. The IASME Cyber Assurance standard then builds on these foundations.

In all instances, any IT equipment within the scope of your certification must meet the scoping requirements from your chosen prerequisite scheme.

Table 2: Prerequisite schemes

| Scheme name ³ | Requirements and availability |
|---|--|
| Cyber Essentials self-assessment | Mandatory if the organisation is in the United Kingdom |
| IASME Cyber Baseline self-assessment | Optional alternative to Cyber Essentials for organisations not in the United Kingdom |

In addition to the requirements of your chosen pre-requisite scheme, all systems that contain information are in scope for IASME Cyber Assurance, including those that don't have an internet connection such as offline servers, air-gapped systems, and production networks. Paper-based systems are covered too.

2 - Locations from which you operate

If your organisation has multiple locations, then all locations must be in scope for assessment. You should apply tools, techniques and policies to all areas of the business and consider all locations as part of your risk assessment.

If you share a location with other businesses (such as at a co-working space or share office building), ensure that you have sufficient security controls to cover the risk of other businesses activities affecting the security of your own. For example, you might need your own segregated network or separate physical security system.

3 - People that can access your information assets

Franchises, agents, and resellers need their own certification if they are accessing your data, and this should be managed through your contractual agreements with them. However, you must include them in your risk assessment alongside all your staff and any other people who have access to your business information on a regular basis, such as contractors. This allows you to consider how best to apply your security controls consistently throughout.

For example, although contractors will likely still need their own certification to an information security standard, your close relationship with them means you are likely to undertake relevant activities to ensure they meet security requirements, such as providing training regarding keeping your data safe and managing their access to your data.

³ Further details about the schemes can be found in [Appendix A – Compatibility with regulation and other cyber and information security standards](#) and at <https://iasme.co.uk/cyber-essentials/>

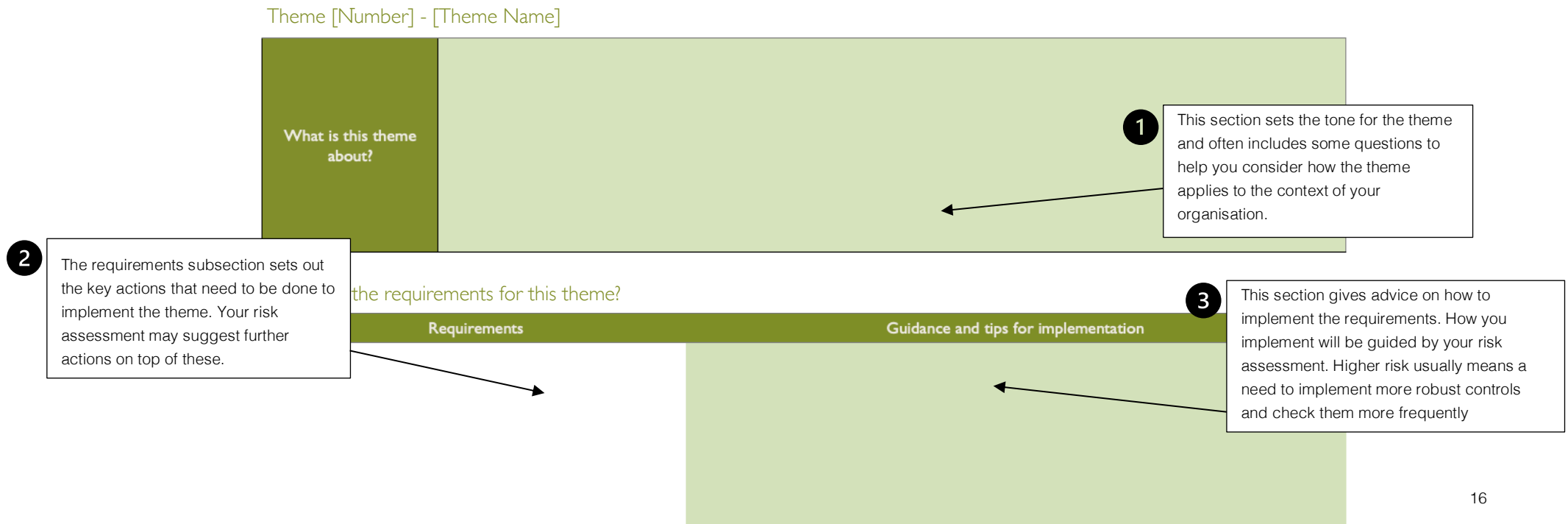
CHAPTER 4 - THE THIRTEEN THEMES: REQUIREMENTS AND GUIDANCE

The IASME Cyber Assurance standard comprises of activities which are divided into thirteen themes. Your organisation needs to meet the requirements of all the themes in order to achieve compliance with the standard. You may wish to start with a couple of themes and build up your activities from there. The themes are in a logical order, so we would suggest starting with the first theme and progressing forward with your activities as time and resources permit.

Once you have implemented each theme, it is important to maintain it on an ongoing basis.

How the thirteen themes are formatted

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



Available templates and supporting guidance

IASME has compiled a range of templates and supporting guidance documents to assist implementing each theme. These can be adapted for most organisations and are available at <https://iasme.co.uk/iasme-cyber-assurance/helpful-templates/>



This icon has been used to highlight where a relevant template or guidance document is available

Duplication

Some controls require consideration within the context of two or more themes. These have usually been replicated across the respective themes as a reminder to consider the control in each instance. You may wish to follow the themes in numerical order when using this standard for the first time because that is likely to reduce any duplication of activities.

Theme 1 - Planning information security

| | |
|----------------------------------|---|
| <p>What is this theme about?</p> | <p>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 as a cyber-attack or an error made by a member of staff or contractor.</p> <p>As part of this theme, you should consider:</p> <ul style="list-style-type: none"> • 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? |
|----------------------------------|---|

What are the requirements for this theme?

| Requirements | Guidance and tips for implementation |
|---|---|
| <p>1. Make provisions for information security as part of your business planning.</p> <ul style="list-style-type: none"> a. Plans should be achievable with specific dates for delivery. b. Sufficient funding must be allocated to information security as part of the planning process. | <p>It is important to include information security considerations within your planning so that it doesn't become a surprise – possibly a very expensive one. You must consider security when planning projects, procurement, contracting, suppliers, and when dealing with partners, and other interested parties.</p> <p>Planning recurs throughout the themes and is fundamental to good information security, see especially Theme 12 - Secure business operations: monitoring, review, and change management.</p> <p>The next themes in the standard will help you organise and formulate your plans.</p> |


Theme 2 - Organisation



















| | |
|----------------------------------|---|
| <p>What is this theme about?</p> | <p>A clear structure within your organisation is the foundation for effective and successful security. Consider:</p> <ul style="list-style-type: none"> • Who has the rights to make decisions that affect your information security? • Who is responsible for making information safe and who is accountable when incidents happen? • Who provides the leadership if there's a dispute? What is the escalation path through that leadership? • How do you manage all the information resources to which you have access? This includes your own information and that belonging to partners or your supply chain. |
|----------------------------------|---|

NOTE: Theme 7 - People provides further requirements and guidance on roles and responsibilities. You may find it helpful to read both themes before acting.

What are the requirements for this theme?

| Requirements | Guidance and tips for implementation |
|--|--|
| <p>1. Ensure there is commitment, funding, and accountability for information security activities from the top, which includes providing a suitable number of appropriately skilled staff.</p> <p style="padding-left: 20px;">a. Review information security activities with board members/directors/partners/trustees so that they can understand and take responsibility for security risks.</p> | <p>This includes directors, board members, partners, trustees and top-level day-to-day management in the organisation. Security should be a standing agenda item at strategic and tactical meetings and should include reviewing any recent incidents. However, it is important that security should not 'wait' until the next meeting; meetings should be brought forward or specially convened when needed.</p> <p>You must prioritise funding for security and data protection initiatives and ensure that you have suitable skills within the organisation to keep your organisation secure.</p> <p>You don't necessarily need dedicated staff for security, particularly in a small or micro business. It's quite reasonable for people dealing with information security to have other roles and responsibilities too.</p> |
| <p>2. Appoint a suitably skilled leader with the authority to coordinate and act on information security activities.</p> | <p>The leader must be internal to the organisation and involved in day-to-day activities; they should not be an employee of an outsourced service provider.</p> |

| | |
|--|---|
| <p>a. Define the responsibility of directors to make clear their direct involvement in setting levels of acceptable risk.</p> | <p>Consider who has the most appropriate technical appreciation and is best placed to take on this role. There is little value appointing a director who has no interest or knowledge in information security, versus a skilled manager who understands and is interested in the topic.</p> <div data-bbox="1019 391 1120 502" style="text-align: center;">  </div> <p><i>Important:</i> You should avoid assigning too much responsibility for information security activities to the person responsible for IT in your business. This is a common mistake made by organisations.</p> <p>The decisions on how to address security need to come from the leadership team for the organisation, while the IT person must contribute to the discussion to ensure that practical decisions are made, and the right technologies are chosen.</p> <p>a. This will depend on the decisions you have made for <i>Requirement 2</i> on who is most appropriate to hold the authority to coordinate and act on information security activities.</p> |
| <p>3. Form a group – or a network of people – from across the organisation to coordinate and implement information security activities.</p> <p>a. Make responsibilities clear. If you have a system of staff appraisal, include the information security work within objectives.</p> | <p>Micro organisations, with only a few members, can implement this informally; larger organisations need more formal structures to preserve the group communication channels.</p> <p>Your group's activities can include:</p> <ul style="list-style-type: none"> • maintaining a knowledge of emerging threats and countermeasures • evaluating the impact of changes across the organisation including to external stakeholders such as contractors, customers, and suppliers <p>Manage the cost of the group by assigning responsibilities to existing posts. This allows you to efficiently use your security budget and increase the ease of obtaining support from management.</p> <p>However, ensure that people can handle their responsibilities and workload and consider the appropriate segregation of roles.</p> <p>a. Your staff appraisal system can be used to determine whether security responsibilities are being met, including the possibility that they are not being met at all. This can help you</p> |

| | | | | | | | |
|---|--|--|---|--|--|---|--|
| | <p>identify any changes needed to roles and responsibilities and identify any relevant training or additional support needed for the role.</p> <p><i>(Further direction on securely managing personnel, including segregation of roles, will be provided in <u>Theme 7 - People</u>)</i></p> | | | | | | |
| <p>4. Define Service Level Agreements (SLAs), or other contracts, that set expectations for service provision and responsibilities with your partners and supply chain.</p> | <p>Security vulnerabilities – weak spots – may manifest through one of your (direct or indirect) suppliers, contractors, partners, or customers. They may be undermining your organisation’s security whether intentionally or unintentionally.</p> <p>Supply chains need governing diligently, and contracts ensure there is a legal basis for your security requirements. Contracts also enable you to clarify the responsibilities you hold to others. Some examples may include:</p> <table border="0" data-bbox="1008 686 2016 989"> <tr> <td data-bbox="1008 686 1299 782">  Agencies and agency staff </td> <td data-bbox="1299 686 1612 782">  Data centre and cloud service providers </td> <td data-bbox="1612 686 2016 782">  E-commerce and payment service providers </td> </tr> <tr> <td data-bbox="1008 845 1299 989">  Hardware and software support services </td> <td data-bbox="1299 845 1612 989">  Maintenance services, such as, alarm systems, fire suppressants, HVAC </td> <td data-bbox="1612 845 2016 989">  Insurance providers, such as cyber liability </td> </tr> </table> <p>Conducting and maintaining your risk assessment will help you to understand the information security requirements you need to put in your agreements.</p> <p><i>(Further direction will be provided in <u>Theme 5 – Assessing and treating risks</u>)</i></p> |  Agencies and agency staff |  Data centre and cloud service providers |  E-commerce and payment service providers |  Hardware and software support services |  Maintenance services, such as, alarm systems, fire suppressants, HVAC |  Insurance providers, such as cyber liability |
|  Agencies and agency staff |  Data centre and cloud service providers |  E-commerce and payment service providers | | | | | |
|  Hardware and software support services |  Maintenance services, such as, alarm systems, fire suppressants, HVAC |  Insurance providers, such as cyber liability | | | | | |

Theme 3 - Assets

| | |
|----------------------------------|---|
| <p>What is this theme about?</p> | <p>It is important to understand what you have and how to protect it. Consider:</p> <ul style="list-style-type: none"> • How does the business know what it needs to protect? What information has the business got to lose? • You can't protect something that you don't know you have. How would you know if information has already been stolen, lost, or damaged or access to your systems has been compromised? • What is the relative value of the information assets to your business? How can these assets be proportionately and sufficiently protected throughout their lifecycle (from creation or acquisition through to safe disposal)? |
|----------------------------------|---|

What are the requirements for this theme?

| <i>Requirements</i> | <i>Guidance and tips for implementation</i> |
|---|--|
| <p>1. Keep an up-to-date register of <u>all</u> your information assets.</p> <p style="margin-left: 20px;">a. Your asset register must include any personal devices (BYOD) if your security policies allow staff to use them for business purposes.</p> | <p>Having a good understanding of your key information assets and how they fit together is essential. It gives you knowledge of your exposure to threats and what you've got to lose. You need this knowledge to carry out a risk assessment and to recover from information security incidents, such as a data breach.</p> <p>An asset register could be a simple list for a small, low-risk organisation, whereas for a large, complex organisation, you would expect to use a more sophisticated, centralised tracking system.</p> <p>Your information assets may be physical, like a laptop, or intangible, such as data you hold about your customers. Information assets include any processed and unprocessed data that has value and impact to a business, its stakeholders, its supply chain, or other interested parties. It includes the equipment that is used to store, process, or transmit the data and also includes any intellectual property.</p> <p style="margin-left: 20px;">a. Ensure personal devices can be used securely in line with your risk assessment and are tracked in the asset register. Any personal devices must be approved before use.</p> |

(Further direction on change management will be provided in Theme 12 - Secure business operations: monitoring, review, and change management)



Template available:

IASME can provide an *asset register* template that can be adapted for most organisations.

2. For each asset, your records must include at least:

- a. A category name that groups similar asset types
- b. The location. You must be aware of any assets that have been moved around
- c. The relative value of the asset
- d. The asset owner

Your asset register should record relevant information about each asset.

- a. For physical assets, the category might be 'laptop', 'server', or 'removable media'. For data, the categories might be 'employee information' or 'customer contact details'. These are just examples.
- b. Where is this asset located? Is it being moved around?
Are your assets on a local computer, 'cloud' storage, on social media, a member of staff's computer, a USB stick, a database, or in a filing cabinet? Is it located at home, the main office, or in a storage unit? With the proliferation of so much recordable media – including memory cards, mobile telephones, 'USB sticks', and tablets, and the distribution of intellectual property across private and public 'cloud' computing resources – this is a task requiring meticulous attention.

If the asset is fixed, record the location. If the asset is mobile, record who uses it on a day-to-day basis and where it is typically used; mobile assets may be governed more by ownership than place (*see Requirement 2d*). It may also be possible to track portable assets through use of mobile device management (MDM) software.
- c. Evaluate what the impact would be if your information assets were lost, stolen, or damaged. Use this to establish the relative value to one another, and which are most important (valuable) to your business so that you can apply adequate protection for them through their life cycle - from creation or acquisition through to safe disposal. Common systems to record this include: [high, medium, low], [public, confidential, secret], or [red, amber, green].

| | |
|---|---|
| | <p>The most severe information security incidents may be where they impact assets which are critical to business operations. You need to understand the relative values of your information assets so that you can spend your security budget effectively to protect the most important assets and – in the case of an incident – know the order of priority in which to recover them.</p> <p><i>(Further direction on resilience will be provided in Theme 11 – Backup and restore and Theme 13 – Resilience: business continuity, incident management, and disaster recovery)</i></p> <p>d. Having a named owner for each asset ensures that someone is accountable for the activities required to keep it secure. Information asset owners will set the rules around data assets, such as, classification, who can access them, and retention periods.</p> |
| <p>3. Sensitive assets must be clearly identifiable.</p> | <p>Sensitive assets are those where a loss of confidentiality or accidental deletion would have a major impact upon either the business, or in the case of personal data, on the person about whom the sensitive data is held.</p> <p>You must have the ability to easily identify all sensitive assets within your company so that you can make sure they are protected. Common systems to record this include: public, confidential, secret or red, amber, green.</p> <p>Consider that marking a document with a ‘Confidential’ or ‘Secret’ marking may draw more attention to it. This can have positive and negative impacts.</p> <p>You don't have to use protective marking if you have other ways to keep sensitive information identified and protected.</p> <p><i>(Further direction on access controls will be provided in Theme 9 – Managing access and Theme 6 – Physical and environmental protection)</i></p> |
| <p>4. Encrypt by default:</p> <ul style="list-style-type: none"> a. Sensitive personal data b. Removable media (if allowed by your security policies) | <p>IASME does not require a specific method of encryption. Your decisions regarding how you implement and manage your encryption should be based off your risk assessment which should include consideration of any legal requirements (as set out in Theme 4 – Legal and regulatory landscape and Theme 5 – Assessing and treating risks). Guidance on suitable methods of encryption for your particular situation can be provided by IASME's Certification Bodies.</p> |

| | |
|--|--|
| <p>c. Portable devices</p> <p style="padding-left: 40px;">i. Configure a remote wipe capability on portable devices where practicably possible</p> <p>d. Data stored on, and in transit to and from, the cloud</p> | <p>For simple organisations, the “default”, industry- standard encryption provided by most popular products and services is likely to be sufficient, although it is important to check that any product or service you are using does use encryption – some do not.</p> <ol style="list-style-type: none"> a. Sensitive personal data can include 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. b. Removable media can include USB sticks, USB hard drives and DVDs/CDs, memory cards, or backup tapes. c. This can include mobile phones, tablets and laptops. Many devices often come with built-in tools that may suit your encryption needs. Alternatively, third-party mobile device management (MDM) software is commonly available. Both inbuilt tools and third-party MDM software usually have a ‘remote wipe’ feature that, if configured correctly and securely, can allow you to delete data on the device in the event it is lost or falls into the wrong hands. Enable this where practicably possible to do so, considering any usage of personal devices which are not configured to segregate personal and business data. d. Your data should be encrypted when it is being stored on the cloud systems whether you are running your own cloud services or using a cloud service provider. If you are using a cloud service provider, it is difficult to confirm this just by looking at the cloud service so you will need to contact your cloud provider or view their security documentation. Additionally, your data must be encrypted when it is being sent between your computers and the cloud provider. Many cloud services achieve this through using an encrypted web interface by default – look for the https:// in the address bar and a padlock icon. Make sure that your encryption settings are switched on, configured correctly, and are secure enough for your needs. |
| <p>5. Review the data you hold at least annually to ensure it is still relevant and accurate.</p> | <p>Data that is inaccurate or no longer relevant is potentially damaging for your business and its customers. You should treat this like any other information security risk. If you have a high-risk profile you may need to do more frequent reviews to ensure that the data you are collecting, including personal data, remains accurate.</p> |

-
6. Assets removed from your business estate must be removed from the asset register and disposed of securely.

Safe disposal methods may include erasure, shredding – particularly of paper and other physical media, or other methods of destruction. Don't rely on deleting data; most deletions of digital data are easily recoverable, so specialist software may be needed to erase the data permanently. You must also consider how *all* versions of an asset are destroyed and whether they can still be restored from a backup copy. You may physically destroy assets yourself, although this is not always effective; there are companies that are qualified to provide a secure destruction service.

Take into account the environmental impact of disposing the asset including requirements to comply with relevant environmental legislation, such as the UK and EU Waste Electrical and Electronic Equipment (WEEE) Regulations.

Theme 4 – Legal and regulatory landscape

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.

What are the requirements for this theme?

Requirements

1. Maintain a clear list of your business' security requirements set by legal, statutory, regulatory, and contractual obligations
 - a. Associated with company registration
 - b. For the use of information, intellectual property rights and legal use of software and other products

Guidance and tips for implementation

Every organisation has certain legally enforceable obligations associated with company registration, accounting, managing customers, use of technology, handling data, and other business processes.

Your list must include areas special to your organisation – for example Payment Card Industry Data Security Standard (PCI DSS) if you handle credit card data, the EU or UK General Data Protection Regulations if you hold personal data of European Economic Area (EEA), or UK residents, or your local implementation of the Network and Information Security (NIS) directive if you are an Operator of Essential Services such as critical infrastructure. You must also include any requirements set out in any contracts you have signed. As [Theme 2 – Organisation Requirement 4](#) sets out, some examples may include:



Agencies and agency staff



Data centre and cloud service providers



E-commerce and payment service providers



Hardware and software support services



Maintenance services, such as alarms, fire suppressants, HVAC.



Insurance providers, such as cyber liability

| | |
|---|--|
| | <p>See Table 3 below for a sample of information-related legislation which may be relevant to businesses operating in the UK.</p> |
| <p>2. Ensure that you have the support in your business processes to fulfil any legal obligations.</p> | <p>Your businesses processes should be designed to practically implement requirements such as deleting data or releasing it to its owners or the authorities within the timeframes that are specified in data protection legislation. However, this is just one example. Your policies and processes should be supportive of <i>all</i> your business objectives, including meeting legal requirements.</p> <p>(Further direction on policy creation and management will be provided in Theme 8 – Policy realisation)</p> |
| <p>3. Monitor compliance and do what needs to be done to counter deviations or to improve your business processes.</p> | <p>Your day-to-day activities should align with your processes and policies. If these are not being met – why not?</p> <p>Has the necessary training and resource been provided? Do your policies and processes need amending? Is your last resort – disciplinary action – needed?</p> <p>Collecting feedback from people involved with your business processes, such as employees, customers, or data subjects may identify how you can improve your business processes. Using a questionnaire may be one way to achieve this but consider the responsibilities and risks for any data that you collect.</p> <p>Further direction on these topics will be provided in Theme 7 – People and Theme 12 – Secure business operations: monitoring, review, and change management</p> |
| <p>4. Ensure that your business records are protected from loss, destruction, or falsification in accordance with your obligations.</p> | <p>This may include internal and external audit information, old versions of policies, contracts, service terms and conditions, and personal data. Draw up a retention schedule to keep track of these.</p> <p>Consider legal requirements and your business needs, particularly when the justification for keeping data may have expired, such as, when a customer stops using your product.</p> |



Important:

The table below is indicative only. Always check for the most recent version of legislation.

Table 3: A sample of information-related legislation which may be relevant to respective businesses in the UK

| | | |
|---|--|---|
| Civil Contingencies Act 2004 | Communications Act 2003 | Companies (Audit, Investigations and Community Enterprise) Act 2004 |
| Companies Act 2006 | Computer Misuse Act 1990 | Consumer Credit Act 1974 and 2006 |
| Consumer Protection (Distance Selling) Regulations 2000 | Consumer Protection from Unfair Trading Regulations 2008 | Consumer Rights Act 2015 |
| Copyright (Computer Programs) Regulations 1992 | Copyright and Rights in Databases Regulations 1997 | Copyright, Designs and Patents Act 1988 |
| Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002 | Data Protection Act 2018 | Defamation Act 2013 |
| Digital Economy Act 2017 | Electronic Commerce (EC Directive) Regulations 2002 | Electronic Communications Act 2000 |
| The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 | Equality Act 2010 | General Data Protection Regulation (EU) 2016/679 |
| Health and Safety (Display Equipment) Regulations 1992 | Health and Safety at Work etc. Act 1974 | Human Rights Act 1998 |
| Malicious Communications Act 1988 | Mobile Telephone (Re-Programming) Act 2002 | Network and Information Systems Regulations 2018 |


| | | |
|--|---|-------------------------------------|
| Patents Act 1977 and 2004 | Privacy and Electronic Communications (EC Directive) Regulations 2003 | Protection from Harassment Act 1977 |
| Regulation of Investigatory Powers Act 2000 | Sale and Supply of Goods Act 1994 | Sale of Goods Act 1979 |
| Supply of Goods and Services Act 1982 | Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 | Trade Marks Act 1994 |
| Waste Electrical and Electronic Equipment Regulations 2013 | | |

Theme 5 – Assessing and treating risks

| | |
|----------------------------------|---|
| <p>What is this theme about?</p> | <p>It is important to identify the threats to the organisation and assess the resulting risk so that you can treat them appropriately and reduce them to an acceptable level.</p> <p>The security controls you apply to your organisation should be influenced by your risk assessment and your risk appetite.</p> <p>Your risk management should be based on a comprehensive view of risk (including risks relating to people) and implementing a balanced set of relevant and tested policies to make information security fit your organisation.</p> |
|----------------------------------|---|

NOTE: [Theme 6 – Physical and environmental protection](#) provides further direction on evaluating and managing risks in your physical environment. You may find it helpful with your planning and implementation to read the sections together.

What are the requirements for this theme?


| Requirements | Guidance and tips for implementation |
|--|--|
| <ol style="list-style-type: none"> 1. Gain vigilant oversight of the risks in your business by creating and maintaining an up-to-date information risk assessment. <ol style="list-style-type: none"> a. This must be reviewed: <ol style="list-style-type: none"> i. At least annually ii. In anticipation of changes iii. Following any incidents | <p>There are lots of methods of doing risk assessments – some more complicated than others. If you already use a risk tool for topics such as health and safety risks or other business risks, you can expand this to include information risks. IASME has a risk assessment template that you can use.</p> <div style="display: flex; align-items: center; gap: 10px;">  <div> <p><i>Template available:</i></p> <p>IASME can provide a <i>risk assessment and treatment plan</i> template that can be adapted for most organisations. Additionally, Appendix B – Carrying out your information risk assessment compiles some of the topics and areas of risk referenced in the IASME Cyber Assurance standard's thirteen themes. It offers a starting point for conducting your own comprehensive review of information risk.</p> </div> </div> |

You must ensure that your risk assessment covers risks to data from events such as malware infection, criminal activity and staff making mistakes, in addition to the risks to, or from, customers, partners, contractors, and suppliers.

Separate the risk assessment from the risk treatment plan. This will allow you to consider the risks, look at what you need to do to address them, and then make an action plan of how to treat each risk.

- a. The review should consider risks and their impact to all areas of the organisation and any external stakeholders such as contractors, customers, and suppliers. You should involve people in the review who are knowledgeable of the risks to the various areas of the organisation (these people will often become the risk owners) and/or the information security group you formed in line with Theme 2 – Organisation. This may only be yourself if you are a sole trader, though you may find it helpful to seek external guidance with the review, such as from an IASME Certification Body.
 - i. Note that your risk assessment may dictate more frequent reviews are required.
 - ii. As set out in Theme 1 – Planning information security, you should ensure that you build ‘right-sized’ security into your business activities. Major changes to what your organisation does may alter the level of risk it faces.

Further guidance on change management will be provided in Theme 12 – Secure business operations: monitoring, review, and change management
 - iii. An incident is a test of your organisation’s information security processes and will sometimes identify threats and vulnerabilities of which you weren’t previously aware. This is a good time to review your risk assessment to ensure any newly identified risks are incorporated.

| | |
|---|---|
| |  <p><i>Important:</i></p> <p>Although an incident necessitates reviewing your risk assessment, it does not always need updating, particularly if your organisation deals with the incident well and no major changes were identified as needing to take place to your processes or policies.</p> <p><i>Further guidance on incidents will be provided in <u>Theme 13 – Resilience: business continuity, incident management, and disaster recovery</u></i></p> |
| <p>2. Pay attention to risks that are beyond the scope of the prerequisite schemes (Cyber Essentials and IASME Cyber Baseline).</p> | <p>The scope of IASME Cyber Assurance expands beyond the scope of the basic controls of the prerequisite schemes (which are Cyber Essentials or IASME Cyber Baseline).</p> <p>For this reason, some of your technology may require additional technical controls to ensure basic technical cyber security is in place. Good examples are systems that are not connected to the internet and devices only used for multi-factor authentication.</p> <p>You may wish to apply some of the controls in the prerequisite schemes (such as anti-virus and firewall controls) to these devices to decrease your overall risk.</p> <p>Paper-based systems should also be included in your risk assessment.</p> |
| <p>3. Keep up to date with emerging cyber threats and feed these into your risk assessment process.</p> <p>a. Maintain knowledge of emerging threats and countermeasures using expert advice.</p> | <p>Keep abreast of emerging threats and the constant, background risks which remain steadfast. Extend this to include awareness of new countermeasures that can be deployed against them.</p> <p>a. Resources include free governmental guidance like the UK National Cyber Security Centre’s (NCSC) weekly threat reports, specialist industry support groups, subscribing to a local Warning, Advice and Reporting Point (WARP - UK) or paid consultancy services, like those offered by IASME Certification Bodies.</p> |
| <p>4. Extend the risk assessment to customers, partners, contractors, and suppliers.</p> | <p>Consider:</p> |

Do customers, partners, contractors, and suppliers offer a route to access your systems and data remotely or onsite? Are they reliable enough to meet your needs in time? What would happen if they can't?

Which legal and contractual obligations must you meet?

(See Theme 4 – Legal and Regulatory Landscape)








Security vulnerabilities – ‘weak links’ – may manifest through one of your suppliers, partners, or customers. Organised attackers will exploit supplier relationships to reach valuable targets, whether this is your organisation as a customer or your own clients and partners trusting in your security. Supply chains link many parties together and so, security incidents can cascade exponentially from one organisation to the others connected to the chain.

Customers, partners, contractors and suppliers⁴ – particularly technology service providers - can confirm their security to you through security certifications such as ISO 27001, Cyber Essentials or IASME Cyber Assurance, although this is not a guarantee that they can meet your needs. You should expect your contractors and suppliers to be following information security procedures that are the equivalent to, or more comprehensive than, those used in your own organisation for the data involved in that contract.

The security requirements you define for your contractors and suppliers may be determined by your regulatory or business environment. For example, Ministry of Defence (MoD) suppliers and Operators of Essential Services such as critical infrastructure will be required to pass down certain

⁴ The terms “contractor” and “supplier” are closely related and have become increasingly blurred. Contractors are often taken on to carry out a specific task for your organisation. This Standard uses the term contractor 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.

Suppliers traditionally only supplied goods to an organisation, but increasingly also supply services. We use the term “supplier” where the other party typically holds the responsibility for necessary security activities.

| | |
|---|--|
| | <p>security requirements to their supply chain. The requirements you set would usually be documented in SLAs or contracts you created in line with Theme 2 - Organisation.</p> |
| <p>5. Be aware of other business risks being addressed at director level and integrate these with your information risk assessment.</p> | <p>Other business risks may include:</p> <ul style="list-style-type: none"> <li style="width: 33%; text-align: center;"> Environmental risk <li style="width: 33%; text-align: center;"> Operational risk <li style="width: 33%; text-align: center;"> Legal and regulatory risk <li style="width: 33%; text-align: center;"> Market risk <li style="width: 33%; text-align: center;"> People risk <li style="width: 33%; text-align: center;"> Health and safety risk <li style="width: 33%; text-align: center;"> Political risk |
| <p>6. Agree your organisations level of acceptable risk (or risk appetite).</p> | <p>How much risk are you willing to accept? Understanding your risk appetite can help you decide what to do about each risk. For example, if your organisation is willing to accept a lot of risk (or has a high-risk appetite) you are more likely to accept each risk on your risk register, rather than take action to try to reduce the likelihood of the risk event occurring.</p> <p>Options for treating each risk vary but may include taking out proportionate insurance cover, like cyber liability, to assist recovery should a risk materialise. Your organisation may already be used to accepting a lot of risks due to the sector in which you work, and your customers and investors understand and accept this. In some other industries, customers and investors may expect you to reduce all risks as much as possible. Consider the role directors have in setting risk appetite as set out in Theme 2 - Organisation.</p> |
| <p>7. Assign the ownership of each risk and its treatment to a named owner.</p> | <p>Having a named owner for each risk helps to ensure that someone is accountable for decisions relating to the risk. Find the person who has the best understanding of potential impacts to that business area. If you are a small company or a sole trader, the risk owner for most risks is likely to be you!</p> |

Note that responsibility for necessary actions, such as those related to risk treatment, can be delegated to other people as appropriate. The risk owner does not need to undertake (all) actions themselves, but they must approve any work completed by others.

8. Use your risk assessment to set rules on how people can use technology in your organisation.

One option for reducing the risks identified in your risk assessment is to set rules on how people use technology in your organisation. For example, you might decide that a major threat is that people are using portable USB sticks on work computers and bringing in viruses, so you could set a rule that people are not allowed to use USB sticks or have to only use company-issued ones.

Your decisions on how resources may or may not be used can be documented in an acceptable usage policy that staff and contractors must follow. Technology covered by your policy can include



Personal devices - BYOD⁵



Portable storage media



Smart devices



Social media



Public, private, and hybrid cloud computing resources



Template available:

IASME can provide an *acceptable usage* policy template that can be adapted organisations.

Note: further direction on this topic will be provided in [Theme 7 - People](#) and in [Theme 8 - Policy realisation](#).

⁵ As set out in [Theme 3 - Assets](#) Requirement 4c, consider the practical implications of balancing encryption, remote wiping capabilities, and the data stored in personal devices.

9. Evaluate how you will implement encryption. Consider:

- a. The risks of encrypting, or not encrypting other assets beyond the IASME Cyber Assurance standard's basic encryption requirements, set out in [Theme 3 - Assets](#), Requirement 4
- b. Which encryption technology you will use and the corresponding encryption and decryption processes

a. The IASME Cyber Assurance standard's basic encryption requirements are - encrypt by default: sensitive personal data, removable media (if removable media are allowed by your security policies), portable devices, data stored on, and in transit to and from, the cloud. Refer back to [Theme 3 - Assets](#) for further direction. Your risk assessment may reveal risks to other assets that may be addressed by further use of encryption. Assets to be considered may range from policies, business plans, to desktop computers and servers.

b. IASME does not require a specific method of encryption. The minimum requirements for your encryption technology may be imposed by contractual obligations with other parties or set by legal authorities, such as complying with a particular encryption standard. Your choices of encryption will vary depending on the assets, the risks to them, and the practicalities of implementing and managing encryption. For example, free encryption included with operating systems may suit your security needs for less sensitive assets. For other, more sensitive assets, it may be more appropriate to utilise specialist encryption packages.

Guidance on suitable methods of encryption for your particular situation can be provided by IASME's Certification Bodies.

Store and protect your encryption keys to ensure that they are only available to authorised people. You must be able to handle scenarios when the day-to-day encryption key manager might be unavailable.

10. Create an action plan to implement any actions that were identified during your risk assessment.

An action plan lets you prioritise the changes that are needed to treat the risks identified in your risk assessment, in accordance with your risk appetite (*see Requirement 6*). [As Theme 1 – Planning information security](#) set out, your plans should be achievable with clear timeframes; when you make changes, ensure you do them in line with the direction in [Theme 12 - Secure business operations: monitoring, review, and change management](#).


| | |
|--|---|
| | Remember that responsibility for actions can be delegated to other people but the relevant risk owner must approve any work (<i>see Requirement 7</i>). |
| 11. Have your risk assessment and risk treatment plan signed off by someone who is authorised to make decisions for your organisation. | This may be a director, board member, partner, trustee, or you, if you are a sole trader. Note: this is likely to be the leader you appointed to coordinate and act on information security activities in <u>Theme 2 - Organisation</u> . Following the earlier input of the individual risk owners, the person signing off the risk assessment must agree to accept any residual risk that will remain after the risk treatment actions have been implemented. |

Theme 6 - Physical and environmental protection

| | |
|----------------------------------|---|
| <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 your 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? |
|----------------------------------|---|

What are the requirements for this theme?

| Requirements | Guidance and tips for implementation |
|---|--|
| 1. Ensure that your risk assessment covers risks of physical harm to information assets. | As with all risk, physical risks and their treatment should all be traceable to your risk assessment and risk treatment plan respectively. |
| 2. Incorporate any physical security requirements that may be dictated by law or third parties. | <p>Consult your list of legal obligations compiled for Theme 4 - Legal and regulatory landscape. You may only need the basic measures expected by your insurance policy which may include door and window locks, window bars, or video surveillance – all appropriate to the places that your business operates.</p> <p>In some cases, physical protection – like other security requirements – may be dictated by your customers or just the practical compliance with legal requirements such as data protection legislation.</p> <p>The measures you take – such as smoke and fire detection and suppression, intruder alarms –</p> |

| | |
|---|--|
| | <p>will be traceable to your risk assessment. This will similarly cover common sense actions such as placing equipment off the ground to avoid water damage (in the event of flood, leak or burst pipe).</p> |
| <p>3. Consider which physical access controls are needed to protect your regular office environment</p> <ul style="list-style-type: none"> a. For people internal to your organisation b. For people external to your organisation who may wish to access your premises | <p>Ensure that access to areas containing information systems or stored data is only provided to people who have valid needs. Restrict access to any other people by using locks, alarms, security cages, or any other form of physical access control and record who has the ability to access sensitive areas. Your risk assessment may require you to support these controls with additional surveillance and monitoring, for example, with CCTV or additional staff.</p> <div style="text-align: center;">  <p><i>Template available:</i> IASME can provide a <i>keyholder tracker</i> template that can be adapted for most organisations.</p> </div> <ul style="list-style-type: none"> a. Refer to the roles assigned to personnel in line with the direction set out in <u>Theme 2 - Organisation</u> and <u>Theme 7 - People</u>. b. Consider people that may have valid needs such as contractors, those with innocent intentions like a lost delivery driver, or those with malicious intentions such as criminals or competitors. |
| <p>4. Restrict access to wired and wireless networks to authorised users.</p> | <p>Ensure that physical access to networking equipment such as routers and network sockets is only provided in locations that you control or use network access control technology to prevent unauthorised access or accidental network reconfiguration. If you use wireless networks, ensure that wireless security is enabled, such as WPA2 or WPA3, so that only authorised devices are able to access your network.</p> |
| <p>5. Keep confidential information away from those that are not authorised to see it and store the information securely when it is not being used.</p> | <p>Use your risk assessment to guide you on which measures you need to retain the confidentiality of information during its use. These may include, but are not restricted to, use of privacy partitions and room dividers, angling screens away from windows, applying screen filters, or installing blinds. Additionally, consider whether confidential discussions may be overheard.</p> |

6. Extend physical and environmental protection to cover information assets taken outside your regular premises.
- a. Ensure your policies can cope with rules that potentially conflict with those determined by parties in control of the external environment.

Special attention is likely to be required if staff take equipment or documents into public places, work from home, or work away overnight. Your risk assessment should support your decision as to the suitability – from a security perspective – of where you work. Beware of people ‘looking over your shoulder’ in these circumstances when working in unprotected places. Be careful where you put your equipment in vulnerable places like whilst waiting in the queue in a restaurant or placing bags on a luggage rack.

- a. Policy decisions will need to cover portable devices such as what to do with laptops while travelling. For example, if equipment is left unattended in a car it must be locked away out of sight; remember that portable devices must be encrypted and where practicable, have remote wipe capabilities enabled (*See Theme 3 - Assets Requirement 4*). Policies must cope with potential conflicts like rules about checking equipment into aircraft holds. Your policies should state what to do when other requirements override, for example, notifying a line manager or contacting someone else with the authority and expertise to advise on what should be done. This would usually be the relevant risk owner.

7. Make sure your environment is suitable to accommodate the needs of your equipment.


If your equipment requires any specific working conditions – such as heating, ventilation, or air conditioning (HVAC) – be careful to maintain these within the guidelines set out by the respective manufacturers. Your risk assessment will guide you what level of monitoring and redundancy you might need.

Theme 7 - People

| | |
|----------------------------------|---|
| <p>What is this theme about?</p> | <p>People are your greatest allies in protecting your organisation's information. Your direct colleagues – and the people in your supply chain – are almost certainly going to form part of your front-line defences. They can also present a risk because they have privileged access to information. Consider:</p> <ul style="list-style-type: none"> • How does your organisation understand its people and educate all its staff, colleagues, contractors, partners, and co-workers in the risks associated with their responsibilities? • How does your organisation remind people of the value of data and make the culture of information security business as usual? • If the worst comes to the worst, is there a clear path for redress? How is it used? |
|----------------------------------|---|

What are the requirements for this theme?

| Requirements | Guidance and tips for implementation |
|---|---|
| <ol style="list-style-type: none"> 1. Clearly assign specific roles and responsibilities relating to information governance to named individuals. <ol style="list-style-type: none"> a. Segregate work – and access to the resources needed – to match these responsibilities, according to the associated risks. b. If you have a system of staff, supplier, or contractor appraisal, include the information security work within objectives. | <p>You may have already assigned some roles whilst following the direction set out in Theme 2 - Organisation. Common examples include – Data Protection Officer, and in British health care, the Caldicott Guardian. Roles that may not have formal titles such as the person(s) responsible for security and data protection training should also be considered.</p> <p>Remember that one person may have multiple roles but ensure that people can handle their responsibilities and workload, and consider the appropriate segregation of roles -</p> <p>Provided access control privileges are assigned appropriately, dividing responsibilities between people reduces the ability for accidental changes to be made without someone noticing or for privileges to be abused without requiring collusion. For example, the person responsible for implementation should usually not be responsible for any corresponding audits. This reduces their ability to cover up events that occurred during implementation.</p> <p><i>Further direction on access controls to support role segregation will be provided in Theme 9 – Managing access and Theme 6 - Physical and environmental protection</i></p> |

| | |
|---|--|
| | <p>You may not need formal appraisals. Your appraisal system can be used to measure to what level security responsibilities are being met, including the possibility that they are not being met at all. This can help adjust roles and responsibilities as necessary and identify any relevant training or additional support needed for the role.</p> |
| <p>2. Establish explicit rules for the acceptable use of your company assets. These must include at minimum:</p> <ul style="list-style-type: none"> a. Whether personal use is allowed, and if relevant, what level of personal use is permissible b. What can or can't be said about your business and the people involved in it on internet platforms | <p>Use your risk assessment, legal responsibilities, and asset register which define relative asset values to guide you⁶.</p> <ul style="list-style-type: none"> a. Document the requirements within your Acceptable Usage Policy (see Theme 5 - Assessing and treating risks). This may also be supported by your access control policies (which will be covered later in Theme 9 – Managing access). <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p><i>Template available:</i></p> <p>IASME can provide a suite of security policy templates, which cover acceptable usage and access control, that can be adapted for most organisations.</p> <p>Note: that further direction on policies will be provided in Theme 8 - Policy realisation.</p> </div> </div> <ul style="list-style-type: none"> b. Consider if different platforms like email, social-media, or face-to-face, should have different requirements. Your policy should cover how to deal with communications around incidents. <i>(Further information will be provided on this in Theme 13 – Resilience).</i> |
| <p>3. Ensure that everyone who has access to the data in your information systems:</p> | <p>This includes permanent and temporary staff, whether full or part time, on contract, paid or unpaid.</p> |

⁶ These were set out respectively in [Theme 5 - Assessing and treating risks](#) and [Theme 6 - Physical and environmental protection](#), [Theme 4 - Legal and regulatory landscape](#), and [Theme 3 - Assets](#)

- a. Is suitable from a security viewpoint before and during employment
- b. Is contractually obligated:
 - i. To respect and implement your security policies in the work that they do
 - ii. To leave intellectual property ownership with the business unless otherwise agreed
- c. Is aware of, and adequately trained in, their security responsibilities
 - i. Appropriate training should be provided during induction and upon changes to responsibilities
 - ii. Reminders must be given at least annually
- d. Is aware of current threats
- e. Is able to report vulnerabilities and incidents without receiving blame and make suggestions on how your security may be improved

- a. Refer to your list of legal obligations⁷ that may indicate requirements such as checking visas and the 'right to work', as well as verifying someone's identity. Further references and screening may be necessary for some roles.



Important:

You must ensure that you have consent for such checks and that you have a legal basis for carrying them out.

Ensure that suitability remains – do visas have an expiration? Is the person susceptible to outsider influences? Are they unhappy or unmotivated at work?

An appraisal system, if used, can help you achieve this.

(Further direction on monitoring will be provided in [Theme 12 - Secure business operations: monitoring, review, and change management](#))

- b. Contracts ensure there is a legal basis for your security requirements.
 - i. Some policies will apply to everyone; consider any policies that may be role-specific.
(Further direction on creating and managing policies will be provided in [Theme 8 - Policy realisation](#))
 - ii. You may wish to support contractual obligations regarding intellectual property ownership with a supplementary Non-Disclosure Agreement.

⁷ [Theme 4 - Legal and regulatory landscape](#), Requirement 1

- f. Is only given access to the information assets they need to carry out their responsibilities
 - i. If roles change, access privileges must be updated accordingly

- c. Responsibilities include: how to use assets, reporting discovered vulnerabilities or incidents immediately. If you have a system of staff, supplier, or contractor appraisal, consider any training requirements that may have been identified. Qualifications do not need to be formal and may be replaced by setting requirements on experience in a particular sector.

Distribute policies to all people responsible for implementing them; many policies will apply to everyone although some may be role specific. Policy distribution could be of a physical copy or a virtual copy via email/instant messaging. You cannot just place the policy in a shared area, unless employees also receive an email/instant message with a link to the shared area and a request to click the link and view the policies.

Verify that all training and guidance given has been understood. Provide trainees the opportunity to give feedback. This can offer insight into training effectiveness and identify areas for improvement. Maintaining a record of who is attending training and keeping details of any test scores or other performance indicators, particularly for informal training sessions, will enable you to understand how effective training is being. Retaining details of training scores or other performance indicators over time can help you assess if knowledge is improving.

Your risk assessment and the respective responsibilities may dictate reminders are required more frequently. Further training may include training courses - in person or online, on-screen reminders, 'how to' documents and good practice guides.

- d. Threats include those arising from manipulation of social media, infected websites and use of personal devices. Use your information security group, if you have one, and your risk assessment to guide any messages; consult your risk treatment plan. Consider – do people require additional training as a result of changing risks? Have any of your security policies changed that they need

| | |
|---|---|
| | <p>to be informed about? The direction set out in <i>Requirement 3c</i> can help you keep on top of this.</p> <ul style="list-style-type: none"> e. People can be both the front line and the last line of protection for your information. It essential that they know how to, and feel comfortable to, report any concerns, incidents, or ideas about improving security. As everyone has a degree of responsibility for security, this facilitates creating an inclusive security culture. This will also allow you to remedy issues as quickly as possible before potential consequences worsen. An anonymous reporting option may be one way to achieve this. f. This policy is referred to as 'least privilege' or 'need to know' and adequate consideration should be given to full and part-time staff, contractors, suppliers, volunteers, and visitors. Note that seniority does not necessarily equate to a 'need' to access specific resources. <p>Whilst implementing this policy, it is important to ensure people are provided <i>all</i> resources they need. This means they don't have to resort to hacks or "get-arounds" to bypass security to do their day-to-day job. You may have already implemented some controls on resource access during Theme 6 - Physical and environmental protection; further direction will be provided in Theme 9 – Managing access</p> |
| <p>4. Upon termination, ensure that:</p> <ul style="list-style-type: none"> a. Access privileges are revoked in time to prevent unauthorised usage b. Employees are debriefed on their post-employment confidentiality responsibilities | <ul style="list-style-type: none"> a. Depending on the circumstances surrounding termination, it may be better for security to withdraw access privileges immediately before notifying the person of termination and/ or not require any notice period to be completed. For portable devices, mobile device management (MDM) software can help with this. Consider that you may need to keep evidence for disciplinary or legal proceedings. b. This may include reminders over the use of Intellectual Property or any Non-Disclosure Agreements that you may have in place (<i>see Requirement 3bii</i>). |

Theme 8 - Policy realisation

What is this theme about?

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:

- 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?

What are the requirements for this theme?

Requirements

1. Create:
 - a. An overall security policy setting out your commitment to information security and how you go about it
 - b. A comprehensive and right-sized set of information security policies that cover the security needs of your organisation


Guidance and tips for implementation


1. Policies need not each be in a separate document. A policy may cover multiple topics (Figure 4).



Figure 4 - Two examples of valid approaches to policies

Some of your policies may be documented in practical places such as business plans, a contract with a supplier, or a staff contract. The way you organise and implement your policies, including documenting and communicating them (*see Requirements 2 and 7*), will depend on the practical actions you take to match

| | |
|--|--|
| | <p>your risk assessment.</p> <p><u>Appendix C</u> provides a list of information security policies. Your risk assessment may suggest additional policies are relevant to your organisation that are not listed – the appendix is offered as a baseline only.</p> <div style="display: flex; align-items: center;">  <p><i>Template available:</i> IASME can provide a suite of security templates, covering many of the topics in <u>Appendix C</u>, that can be adapted for most organisations.</p> </div> |
| <p>2. Policies must be supported with a suitable level of documentation which can be easily understood by the people who need to implement them.</p> | <p>A documented policy can support business continuity. For example, if the person usually responsible for a particular area is absent or an incident occurs, it allows someone who is unfamiliar with that respective area to ‘take-over’. A documented policy can also provide assurance to suppliers, customers, and auditors, and additionally help to clarify any misunderstandings.</p> <p>There is no need for excessive documentation – often shorter policies are more effective because people are more likely to read and understand them. Bullet points are acceptable provided all necessary content is covered with suitable clarity.</p> <p><u>Appendix C</u> sets out which policies should be documented as a minimum.</p> |
| <p>3. Policies must cover:</p> <ol style="list-style-type: none"> a. The purpose of the policy b. The scope of the policy c. The requirements of the policy (“what people need to do”) d. When will the policy be reviewed for its continued fit to the business e. How it’s monitored to make sure that it’s implemented correctly and is working for the business | <p>This applies to each policy whether it covers only one, or multiple, areas.</p> <ol style="list-style-type: none"> a. Why does the business need it and what’s the risk of not having it? b. What does the policy apply to, and what – if anything – is excluded? c. The simpler a policy is, the easier it is to understand, implement, and monitor. Provide a clear, pithy, and concise description of what needs to happen, including any responsibilities for implementation. Remember to ensure that personnel are suitably qualified and aware of responsibilities as set out in <u>Theme 7 - People</u>. Consider how the policy will be practically implemented and enforced. Do not rely on disciplinary action – this should be a last resort only. d. See <i>Requirements 5 and 6</i> that cover how you should handle policy reviews. |

| | |
|--|--|
| <p>f. What happens if the policy is breached</p> | <p>e. This includes identifying where the policy, and its implementation, can be improved upon even if it is currently being implemented effectively. You may not need formal audits if you regularly keep an eye on whether the policy is working. However you monitor your policies, your findings should support your review cycle of the policy.</p> <p>f. Security incidents are inevitable. Be prepared with a business continuity element for every policy (<i>further direction on this will be provided in Theme 13 – Resilience: business continuity, incident management, and disaster recovery</i>). You may also need to invoke disciplinary procedures but enact this fairly and pragmatically to maintain a culture where people feel comfortable to report any concerns, incidents, or ideas about improving security.</p> |
| <p>4. Ensure your security policies can cope with potentially conflicting rules set by other relevant parties.</p> | <p>Sometimes the rules you need to follow in agreements with clients and other parties may conflict with your own security policies. For example, you may be required to check equipment into the aircraft hold regardless of your own policies that state equipment must remain with staff at all times.</p> <p>Your policy should state what to do when other requirements override, for example, notifying a line manager or contacting someone else with the authority and expertise to advise on what should be done. This would usually be the relevant risk owner⁸.</p> |
| <p>5. Each policy must be reviewed and updated (if necessary):</p> <ul style="list-style-type: none"> a. At least annually b. If a security incident occurs c. Changes in the risk landscape emerge | <p>Ensure that sufficient knowledge is available in the review to consider impacts to all areas of the organisation and any external stakeholders such as contractors, customers, and suppliers. Involve a representative group of people as necessary, for example, people who have approved existing policies, risk owners, and/or the information security group formed in Theme 2 - Organisation. Your risk assessment and risk treatment plan should be reviewed and if necessary updated.</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p><i>Important:</i> Although there are a number of triggers for conducting a review, policies do not always need updating. Sometimes a policy will still be fit for purpose as policies cannot always cover the</p> </div> |

⁸ [Theme 5 - Assessing and treating risks](#), Requirement 7

| | |
|---|--|
| <p>d. If monitoring reveals that the policy is no longer working for the business and/ or a good opportunity to improve your security is identified</p> | <p>plethora of nuances in which risk may realise. Policies should be based on your risk assessment and the practicalities of implementing corresponding countermeasures⁹. When you do update policies, keep a log of old policies in line with your retention schedule. This way you know what applied to whom/ what, and when¹⁰.</p> <p>a. Your risk assessment may dictate more frequent reviews are required. Bring review dates forward as necessary.</p> <p>b. Did the policy support you as intended before, during, and after the incident?</p> <p>c. Does the policy still support the new context?</p> <p>d. Is the policy constraining your practice or no-longer reflects your practice? Policies only need to be right-sized and beneficial to your organisation. You should not need to work for your policies; your policies should work for you. Improvements may address where your policy may not be working or where there is an opportunity to reduce risk further.</p> <p><i>(Further direction on changes will be provided in Theme 12 - Secure business operations: monitoring, review, and change management)</i></p> |
| <p>6. Each policy must be approved by someone in your organisation with the appropriate competency and authority.</p> <p>a. Document your policy review and approval process.</p> | <p>Suitable people are likely to be risk owners or members of the information security group, if you have one, as defined in Theme 2 - Organisation. The approval process should include a review before signoff.</p> <p>a. For documented policies, often the review and approval process is recorded in a 'document control form' at the beginning of the document. For policies that aren't documented, a high-level policy review and approval process may be recorded in your overall security policy which sets out your commitment to information security and how you go about it (<i>see Requirement 1a</i>).</p> |

⁹ Direction on this was set out in [Theme 5 - Assessing and treating risks](#) and [Theme 6 - Physical and environmental protection](#)

¹⁰ [Theme 4 – Legal and regulatory landscape](#), Requirement 4




| | |
|--|---|
| <p>7. Policies must be distributed to all people responsible for implementing them.</p> | <p>People can only be expected to follow a policy if they have been made aware of it; this aligns with necessity to provide adequate personnel training¹¹ and this is particularly relevant where policies may not have been documented.</p> <p>Many policies will apply to everyone although some may be role specific. Adequate consideration should be given to full and part-time staff, contractors, suppliers, volunteers, and visitors. Policy distribution could be of a physical copy or a virtual copy via email/instant messaging. You cannot just place the policy in a shared area and not tell anyone about it. Employees should also receive an email/instant message with a link to the shared area and a request to click the link and view the policies.</p> |
| <p>8. The people responsible for implementing a policy must be aware of the policy's contents and should be able to provide a clear description of the policy to others.</p> | <p>This is a strong initial indicator of whether policy is being followed and whether the person has been adequately trained to implement the policy.</p> |

¹¹ Theme 7 - People, Requirement 3

Theme 9 - Managing access

| | |
|----------------------------------|--|
| <p>What is this theme about?</p> | <p>Give users access to all the resources and data necessary for their roles, but no more. This applies equally to data stored on computer equipment as to physical locations. This theme builds on Theme 6 - Physical and environmental protection to consider:</p> <ul style="list-style-type: none"> • How does the business control whom and what can access its information? • Does the business prefer a 'need to know' way of working? If not, why not? |
|----------------------------------|--|

What are the requirements for this theme?

| Requirements | Guidance and tips for implementation |
|---|---|
| <p>1. Provide people access to all the resources and data necessary for their roles, but no more. This applies to:</p> <ol style="list-style-type: none"> a. Data stored on computer equipment b. Physical access to equipment and premises | <p>This policy is referred to as 'least privilege' or 'need to know' and adequate consideration should be given to full and part-time staff, contractors, suppliers, volunteers, and visitors. Note that seniority does not necessarily equate to a 'need' to access specific resources. Consider which resources are needed for the roles and training requirements you defined in Theme 2 - Organisation and Theme 7 - People. Certain privileges bring with them an increased risk of damage (deliberate or accidental) which can cause significant disruption.</p> <p>Whilst implementing this policy, it is equally important to ensure people are provided <i>all</i> resources they need. This allows them to fulfil their (security) responsibilities.</p> <ol style="list-style-type: none"> a. Ensure your access controls manage access to data on an individual or group basis. Consider – as applicable to your business – the need to create, read, update, or delete different pieces of data: <div style="display: flex; justify-content: space-around; align-items: flex-end; margin-top: 20px;"> <div style="text-align: center;">  <p>Customer information</p> </div> <div style="text-align: center;">  <p>Databases</p> </div> <div style="text-align: center;">  <p>Information about staff, contractors, and suppliers</p> </div> </div> |



Monitoring systems



Operating system files



Applications and other software programs



Management information



Software source code



Control systems

- b. Ensure that access to areas containing information systems or stored data is only provided to people who have legitimate needs. Restrict access to any other people by using locks, alarms, security cages or any other form of physical access control and record who has the ability to access sensitive areas. Consider the risk assessment and treatment decisions made in relation to the earlier section - [Theme 6 - Physical and environmental protection](#); you may have already implemented some physical access controls.



Template available:

IASME can provide *keyholder tracker* and *administrator privilege tracker* templates that can be adapted for most organisations.

2. Make sure that the access privileges for applications are setup to limit unnecessary access to device functionality.

Some operating systems have introduced free features to manage this requirement. Consider whether an application needs to access data in other applications on the device and peripherals such as cameras and sensors. For example, applications listed in mobile app stores will list the default permissions they have to access and modify other apps on your phone. These can often be manually adjusted in the settings but note that this can impact functionality.

Using a 'sandbox' – a virtual, isolated container on your device - can also be employed to segregate and manage the access one application has to another. You may already use sandboxes to fulfil the malware requirements from the prerequisite schemes such as Cyber Essentials or IASME Cyber Baseline.

3. Consider the need to segregate parts of your network to protect more sensitive assets.
 - a. Restrict access to wired and wireless networks to only authorised users.

If you run important business systems such as web servers containing client information, you may wish to segregate them from your main network in order to provide extra security. Usually, segregation is implemented by utilising routers, gateways, firewalls, virtualisation, or cloud-based technologies.

- a. You may have already implemented this whilst following the direction set out in the earlier section - [Theme 6 - Physical and environmental protection](#).

Ensure that physical access to networking equipment such as routers and sockets is only provided in locations you control or that it uses network access control technology to prevent unauthorised access. If you use wireless networks, ensure that wireless security is enabled, such as WPA2 or WPA3, so that only authorised devices are able to access your network.

4. Consider establishing restrictions on the locations from which data may be accessed.

If your risk assessment suggests this would help your situation. For example, you might want to only allow access to sensitive data from your business premises and not whilst working at home. This can be used to support the physical protection needed to prevent theft, loss, or damage.

5. Ensure that user accounts and devices do not remain signed-in indefinitely.

Devices or accounts which remained signed-in whilst not in use are vulnerable to exploitation. In such instances, no authentication method, such as a password, is needed to access the system or data. Most devices, however, such as phones and computers, support automatic locking after a period of inactivity and many applications and system accounts can be configured to do this.



Important:

Use your risk assessment and operating procedures to guide how you implement automatic locking – ensuring that systems and data remain available to those authorised to use them is essential for ‘good’ security. Overly restrictive practices may motivate people to attempt to disable and bypass your protection mechanisms.

-
6. Make sure that privileges to access information can be revoked in a timely manner when someone changes roles or is leaving your business.

You may have already created and implemented a process to achieve this whilst following the direction set out in [Theme 7 - People](#).

Depending on the circumstances surrounding termination, it may be better for security to withdraw access privileges immediately before notifying the person of termination and/ or not require any notice period to be completed. For portable devices, mobile device management (MDM) software can help with this.

Theme 10 - Technical intrusion

| | |
|----------------------------------|--|
| <p>What is this theme about?</p> | <p>Technology by default is extremely susceptible to unauthorised access and usage. Developing capabilities to monitor and respond to this is essential to keeping your information safe. Technical intrusion may originate from afar, often using malware - malicious code that is designed to steal or damage data. It may:</p> <ul style="list-style-type: none"> - Come through e-mail (often as a specific branch of social engineering called 'phishing'), portable media, poisoned websites – especially 'blogs' and social media – and documents - Obtain intelligence about what you do or what you do for your customers - Steal saleable information such as know-how, plans, or financial information - Disrupt your working facilities by denying access and leave you exposed to blackmail to regain them - Form the vanguard of a bigger, more sustained attack on your business or a more valuable target in the supply chain which you provide the path to <p>Notably, your technology and information systems are susceptible to intrusion from inside your organisation, including where staff negligence and/or misuse leaves your data vulnerable. Malware and other intrusion techniques are continually evolving to avoid detection so how does the business deploy anti-malware and other technical tools including intrusion detection and prevention methods?</p> |
|----------------------------------|--|

What are the requirements for this theme?

| Requirements | Guidance and tips for implementation |
|--|--|
| <p>1. Detect unauthorised activity. Deploy technical tools including intrusion detection and prevention methods.</p> | <p>Your firewalls which are already in place to comply with the prerequisite schemes (Cyber Essentials or IASME Cyber Baseline) often include features to assist you with this, such as being able to block access to a list of suspicious URLs to achieve this. Your risk assessment may indicate that further measures such as intrusion detection, data loss prevention, and honey pots or traps to distract attackers are necessary. You can also use a filtered Domain Name System (DNS) service such as (Quad9 or OpenDNS) which is often free to set up.</p> <p>Note: detecting unauthorised activity also includes internal sources. Examples include</p> |


| | |
|--|--|
| | <ul style="list-style-type: none"> • Staff accessing company data from personal devices without prior approval (<u>see Theme 3</u>). • People using accounts that should have been deactivated due to role changes • Attempts by staff to access systems or segregated sections of networks holding data that is not required for their respective role. <p><i>(Further direction on monitoring and change management will be provided in <u>Theme 12 - Secure business operations: monitoring, review, and change management</u>)</i></p> |
| <p>2. Scan your systems and network for vulnerabilities:</p> <ol style="list-style-type: none"> a. At least every six months b. After introducing major changes c. Following incidents where a vulnerability may have been exploited or created | <p>A vulnerability scan is a technical examination of the security status of your IT system. It can be performed by automatic tools, some common examples which are free or low cost for SMEs include OpenVAS, Nessus, or Qualys. Alternatively, vulnerability scans can be performed by an expert. IASME Certification Bodies also provide the service as part of Cyber Essentials Plus certification or offer this as an independent service.</p> <ol style="list-style-type: none"> a. Note that your risk assessment may dictate that more frequent reviews are required. b. Changing your systems or network configuration may introduce vulnerabilities. <i>(Further direction on change management will be given in <u>Theme 12 - Secure business operations: monitoring, review, and change management</u>).</i> c. Conducting a vulnerability scan may offer insight into the source of the incident and/or reveal any vulnerabilities that have been created as a consequence of the incident. <i>(Further direction on incident response will be provided in <u>Theme 13 - Business continuity: incident management, disaster recovery, and resilience</u>).</i> |
| <p>3. Extend your system and network scans to include penetration testing if deemed necessary by your risk assessment.</p> | <p>A penetration test is a more in-depth test of the security of your systems where experts attempt to gain access by exploiting vulnerabilities. Where you have high risk systems, such as a web server with customer information, you should carry out penetration tests to ensure that the system is secure from external attackers. Penetration tests should be carried out after major system upgrades or changes.</p> |

| | |
|---|--|
| <p>4. Prevent users from making changes to your systems (including introducing new hardware and software) without receiving prior approval. Ensure that they can seek approval for changes easily.</p> <p>a. Create an 'allow list' of approved applications that may be installed on your devices.</p> | <p>Changes to systems should be approved by a suitable person with a decision-making role in the business, subject to the outcome of reviewing any security impacts or provisions needed.</p> <p>If your risk assessment identifies a particular risk from removable media, you may choose to restrict device connectivity to removable media through use physical access restrictions or a technical solution. Some operating systems, like Windows Professional editions, include features to implement and manage this requirement. Third-party tools are also available which may offer more flexibility to define and manage the level of restrictions. Additionally, you may dedicate computers to scanning incoming USB devices for malware before allowing them to be used.</p> <p>a. You should maintain a list of software that is used within the organisation and ensure that only software from this approved list is installed on your devices. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff.</p> <p><i>(Further direction on change management will be provided in Theme 12 - Secure business operations: monitoring, review, and change management)</i></p> |
| <p>5. Pay attention to warnings and reports from your malware and technical intrusion controls, including vulnerability scans and any penetration testing, and take action.</p> | <p>Many systems will automatically generate alerts. Those that require manual monitoring must be checked at least weekly, although your risk assessment may dictate that more frequent reviews are required.</p> <p><i>(Further direction on monitoring will be provided in Theme 12 - Secure business operations: monitoring, review, and change management).</i></p> <p>Refer to the direction set by your policies when acting upon alerts. Consider the need to review the policies following any alerts. This also extends to your risk assessment and treatment plan, and the settings on your technology. Acting on potential issues early on can reduce their impact upon your customers, suppliers, contractors and employees.</p> <p><i>(Further direction on responding to incidents will be provided in Theme 13 – Resilience: business continuity, incident management, and disaster recovery).</i></p> |
| <p>6. Review the security settings on all your technology periodically to ensure that they are adjusted for current threats.</p> | <p>This may include keeping your software up to date or adjusting firewall settings based on recognised or predicted threats, according to your risk assessment.</p> |

Theme 11 - Backup and restore

| | |
|----------------------------------|--|
| <p>What is this theme about?</p> | <p>Regularly backing up information, 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> <ul style="list-style-type: none"> • Does the business back up as frequently as it can stand versus the amount of rework it can stand or afford to do? • How does the business create and secure backup copies to a degree commensurate with the risk to the data they contain? • Can the business show its confidence in the restoration of backups to complete, operational capability? |
|----------------------------------|--|

What are the requirements for this theme?

| Requirements | Guidance and tips for implementation |
|---|--|
| <p>1. Make sure you have a backup of all information and an easy way to restore it to your systems if a problem occurs.</p> | <p>You should keep three copies of your information:</p> <ol style="list-style-type: none"> 1) The day-to-day working original 2) A main back up (which may be the copy you store off-site away from the operational systems – <i>see Requirement 3</i>) 3) A local back up for easy retrieval <p>- but all tuned by the expectations of your risk assessment</p> <p>Consider whether any data is primarily paper-based and the respective capabilities to recover this if damaged or lost.</p> <div style="display: flex; align-items: flex-start; margin-top: 10px;"> <div style="text-align: center; margin-right: 10px;">  </div> <div> <p><i>Important:</i></p> <p>Usage of a cloud system does not guarantee that there is a backup mechanism in place. Many cloud providers offer replication rather than backup, which while useful against equipment failure, doesn't provide the</p> </div> </div> |

| | |
|---|--|
| | <p>same level of resilience as a backup against cyber attacks such as ransomware.</p> <p>You should verify with your cloud-provider(s) that segregated, one-way backups stored in a different physical data centre are available or make provisions for an alternative backup solution that meets the requirements set out in this theme. For example, this might be deciding to use a second cloud provider as a backup, or to store a local backup on your premises.</p> |
| <p>2. Back up as frequently as you can stand versus the amount of rework you can afford to do, though at minimum on a weekly basis.</p> <p>a. Back up as necessary before implementing significant changes.</p> | <p>Use your risk assessment to guide you. For example, if you can only afford to re-do 2 days work should there be an incident, then you must back up your data every 2 days <u>as a minimum</u>.</p> <p>a. If the change does not go as intended, this can enable you to revert back to the backup point, avoiding any loss of data.</p> |

-
- Maintain at least one backup off-site and at some distance from the working version of the data.

Keeping an off-site backup should mitigate the risk of the backup being affected by any incident that occurs at your main location. For example, if the main version of the data which was held in your office was destroyed by fire, you would still be able to access the backup copy if it is in a different location.

Alternatively, if your main working copy is stored in the cloud, a local back up (that is not stored in the cloud data centre) for example, would offer you similar protection. Your cloud provider may provide a segregated backup service that is stored in a different physical data centre; however, you should verify this with them.

4. Ensure backup copies are logically segregated from the main working copy and kept appropriately secured for the data they contain. Backups must be at least as secure as the working copy.
 - a. Ensure that backups are recorded and tracked in your asset register.

Backups must be segregated from the main working copy to prevent incidents spreading from your original system into the backup. Additionally, protect backups so that they cannot be unintentionally altered or deleted once created, especially whilst your backup mechanism is connected to the main system. For example, an external hard drive used for backups should only be connected to the main system when creating or restoring from a backup. Backups stored in the cloud should implement a one-way process so that if the main working copy is infected by malware, the backup copy stored in the cloud is not also impacted.

This may be achieved by taking cloud backups 'offline' when not being used or by configuring your backup solution with write-once privileges, so that existing backups cannot be overwritten.

Using multiple backups, can also offer protection provided that the multiple backups are segregated and not all connected simultaneously to your main system. Use your retention schedule to guide for how long to keep old backups (see [Theme 4 – Legal and regulatory landscape](#), Requirement 4).

Make sure that your backups do not become your 'weak link'. As you may not have sight of your back-ups on a daily basis, this is especially important. If your backups are compromised, the severity of consequences could be the same as if the original data was compromised. Your asset value classifications assigned to the main working copy should indicate a baseline for protective measures needed.

Remember to encrypt by default: sensitive personal data, removable media (if removable media are allowed by your security policies), portable devices, and cloud data. Your risk assessment may have identified other assets that need encrypting and how this should be implemented.

- a. Your asset register must include all information assets¹².

5. Backups must be tested at least monthly to be certain that they can be used to restore systems or information.

A backup that cannot be restored is of zero use. Use your risk assessment to guide the frequency in which you test data restoration. You don't need to restore the whole data set, only a selection of files to ensure accessibility is required. This process could be automated.

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


| | |
|----------------------------------|---|
| <p>What is this theme about?</p> | <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? • 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> |
|----------------------------------|---|

What are the requirements for this theme?

| Requirements | Guidance and tips for implementation |
|--|---|
| <p>1. Embed security activities into your 'regular' day-to-day practices. Ensure that you maintain the prerequisite scheme (Cyber Essentials or IASME Cyber Baseline) controls in addition to the requirements set out in this standard.</p> | <p>1. Security activities should be part of your 'business-as-usual' and not just reserved for particular projects. Pay particular attention to ensure:</p> <ul style="list-style-type: none"> • The data you hold is still accurate and relevant to the business¹³ • Your asset register remains up to date and asset usage reflects your acceptable usage policy |

¹² [Theme 3 - Assets](#), Requirement 1

¹³ [Theme 3 - Assets](#), Requirement 5

| | |
|---|---|
| | <ul style="list-style-type: none"> • Any controls from a prerequisite scheme (Cyber Essentials or IASME Cyber Baseline) are maintained such as checking that software remains supported and up to date • Encryption is used in accordance with the requirements defined in Theme 3 - Assets and Theme 5 - Assessing and treating risks • Policies are created, reviewed, implemented, and updated in line with the requirements set out in Theme 8 - Policy realisation • Your technology settings remain up to date in line with the Theme 10 - Technical intrusion requirements • Staff, contractors, and suppliers remain suitable for their role and have access to all the resources needed for their role but no more |
| <p>2. Know which business systems and processes you need to track and monitor for acceptable activity and how you will identify the unacceptable and/or where you can improve your security posture.</p> <ol style="list-style-type: none"> Ensure that your monitoring systems are calibrated correctly. Make sure that personnel are aware of any monitoring that may take place. Keep information which is forensically sound from a legal perspective. | <p>Your policies should provide a strong indication of what needs monitoring, and how deviations or opportunities for improvement can be identified¹⁴. Additionally, consider your written list of business' security requirements set by legal, statutory, regulatory, and contractual obligations created in line with Theme 4 - Legal and regulatory landscape.</p> <ol style="list-style-type: none"> This may include setting the time correctly on your devices so that logs and audit trails are in sync with each other (this can usually be done by setting date/time preferences to automatic or internet time) and making sure that CCTV cameras, if required by your risk assessment, record adequate quality for playback and time analysis and are suitably positioned. <p> <i>Important:</i> Consider relevant legal requirements to inform personnel and the public of any monitoring taking place. Refer to, and update as necessary, your list</p> |

¹⁴ [Theme 8 - Policy realisation](#), Requirement 3 outlines the areas that policies must cover.

- d. Pay attention to the reporting mechanisms provided with your security software.
- e. Make sure that people you work with, and the public, know how to report incidents and security vulnerabilities. Ensure they can do so without receiving blame.
- f. Keep an eye on who is trying to access your information and where they are trying to access it from.
 - i. Have the ability to trace who has access to particular information (such as strategic or Personally Identifiable Information).
- g. Review event logs (including alerts and errors) at least weekly.
- h. Review the data you hold at least annually to ensure it is still relevant and accurate.


of legal obligations created in line with [Theme 4 - Legal and regulatory landscape](#)

- c. Keeping information forensically sound means ensuring that it is reliable and that you are able to prove it hasn't been tampered with. If you have an incident to deal with, you can engage a computer forensics specialist who can review the information you have kept and use it to prove what happened in the incident in any legal case.
- d. This includes firewalls, anti-malware, and any other technical tools described in [Theme 10 - Technical intrusion](#).
- e. It is essential that people know how to report any concerns, incidents, or ideas about improving security. As everyone has a degree of responsibility for security, this facilitates creating an inclusive security culture. This will also allow you to remedy issues as quickly as possible before potential consequences worsen. An anonymous reporting option may be one way to achieve this. You should have a vulnerability disclosure policy covering your products and services that is publicly available, such as on your website, that covers at a minimum:
 - contact information for the reporting of issues; and
 - information on timelines for:
 - initial acknowledgement of receipt; and
 - status updates until the resolution of the reported issues



Template available:

IASME can provide a *vulnerability disclosure policy* template that can be adapted for most organisations.

| | |
|---|---|
| | <p>f. Consider this alongside the access controls and role segregations defined in Theme 7 - People and Theme 2 - Organisation.</p> <div data-bbox="1070 391 1169 486" style="text-align: center;">  </div> <p><i>Template available:</i> IASME can provide <i>keyholder tracker</i> and <i>administrator privilege tracker</i> templates that can be adapted for most organisations.</p> <p>g. Many systems will automatically generate alerts; those that require manual monitoring must be checked at least weekly although your risk assessment may dictate that more frequent reviews are required.</p> <p>h. You may already have designed and implemented a process whilst following the direction set out in Theme 3 - Assets or drawing up a retention schedule in line with Theme 4 - Legal and regulatory landscape</p> |
| <p>3. Protect access to your monitoring systems and preserve the records they produce according to a suitable retention schedule.</p> <p>a. Ensure that any logs are stored in a safe location and that error messages do not return sensitive information to external or internal users.</p> | <p>Strive to keep your records for at least six months as it often takes time to discover an incident, at which point they will assist your investigations¹⁵. Balance the business need to retain records against the additional security and legal risks associated with keeping this sensitive data unnecessarily – use your risk assessment to guide you.</p> <p>a. Consider the need for role segregation supported by the access controls set out in Theme 9 – Managing access and Theme 6 - Physical and environmental protection. Logs from multiple devices and systems can often be pulled into a central location using a cloud-based solution or a local server to reduce the likelihood of tampering by the person carrying out the activities being logged. Note that default error messages displayed to users can often map out your system and subsequent vulnerabilities that hackers can exploit.</p> |

¹⁵ Further direction on incidents will be provided in [Theme 13 - Business continuity: incident management, disaster recovery, and resilience](#)

| | | | | | | | | | | | | | |
|---|---|--|--|--|--|--|--|--|--|--|--|--|--|
| <p>4. Be prepared, ready, and take action based on the insight your monitoring provides.</p> | <p>Refer to the direction in your policies when acting upon alerts and consider the need to review this. This also extends to your risk assessment and treatment plan, the settings on your anti-malware and technical intrusion technology, vulnerability scans, and any penetration testing.</p> <p>Acting on issues early can reduce their impact on your customers, suppliers, contractors, employees, and the legal authorities. Further direction on responding to incidents will be provided in Theme 13 – Resilience: business continuity, incident management, and disaster recovery.</p> | | | | | | | | | | | | |
| <p>5. Make sure that the policies that you set to protect information and recover from a security incident are effective and remain supportive of your business objectives.</p> | <p>Remember that each policy should be reviewed, considering impacts to all areas of the organisation and any external stakeholders such as contractors, customers, and suppliers. See Theme 8 - Policy realisation for the full direction on reviewing policy suitability.</p> | | | | | | | | | | | | |
| <p>6. Keep Service Level Agreements (SLAs) and other contracts up to date.</p> | <p>Service Level Agreements (SLAs), or other contracts, that define expectations for service provision and responsibilities with your partners and supply chain should have been created and considered during your assessments of risks and legal obligations¹⁶. Examples include:</p> <table border="0"> <tr> <td data-bbox="1070 858 1120 906"></td> <td data-bbox="1146 858 1299 917">Agencies and agency staff</td> <td data-bbox="1384 858 1433 906"></td> <td data-bbox="1460 837 1635 933">Data centre and cloud service providers</td> <td data-bbox="1702 858 1736 906"></td> <td data-bbox="1780 837 1971 933">E-commerce and payment service providers</td> </tr> <tr> <td data-bbox="1070 1053 1120 1101"></td> <td data-bbox="1146 1029 1332 1125">Hardware and software support services</td> <td data-bbox="1384 1053 1433 1101"></td> <td data-bbox="1460 989 1668 1157">Maintenance services, such as, alarm systems, fire suppressants, HVAC.</td> <td data-bbox="1702 1029 1758 1101"></td> <td data-bbox="1780 1045 2016 1109">Insurance providers, such as cyber liability</td> </tr> </table> | | Agencies and agency staff | | Data centre and cloud service providers | | E-commerce and payment service providers | | Hardware and software support services | | Maintenance services, such as, alarm systems, fire suppressants, HVAC. | | Insurance providers, such as cyber liability |
| | Agencies and agency staff | | Data centre and cloud service providers | | E-commerce and payment service providers | | | | | | | | |
| | Hardware and software support services | | Maintenance services, such as, alarm systems, fire suppressants, HVAC. | | Insurance providers, such as cyber liability | | | | | | | | |

¹⁶ [Theme 2 - Organisation](#); [Theme 5 - Assessing and treating risks](#)

| | |
|---|---|
| | <p>Ensure that your agreements and risk assessment are amended as necessary so that they continue to support your organisation's objectives.</p> |
| <p>7. Set out a documented procedure for changes to working practices and technology.</p> <p>a. Ensure that all new or modified, hardware, software, and networks include appropriate security provisions to meet your requirements and are compatible with existing systems before they commence operation.</p> <p>i. Make sure that where personal devices (BYOD) are used for business, that suitable protective measures are in place.</p> <p>b. Consider and manage the risks when decommissioning assets.</p> <p>c. Prevent users from making unapproved changes to your systems (including introducing new hardware and software). Ensure that they can seek approval for changes easily.</p> <p>d. Ensure that your 'allow list' of approved applications that may be installed on your devices remains up to date.</p> | <p>Changes to working practices and technology must be approved by a suitable person with a decision-making role in the business. Suitable people are likely to be risk owners or members of the information security group, if you have one, as defined in Theme 2 - Organisation.</p> <p>The approval process should consider the impacts to all areas of the organisation and any external stakeholders such as contractors, customers, suppliers, and data subjects, before signoff. Your risk assessment and risk treatment plan should be reviewed and, if necessary, updated¹⁷.</p> <p>a. As set out in Theme 1 – Planning information security, you must incorporate security provisions into your decision making about new systems or new ways of working with existing ones. You can achieve this by having a review process for all new and modified systems which involves technical, security, and operational staff.</p> <p>Remember that changes can include introducing new removeable media such as USBs or personal devices (BYOD). Impacts you must consider may include the requirements set out in:</p> <ul style="list-style-type: none"> • Theme 3 - Assets - such as updating your asset register • Theme 8 - Policy realisation - such as updating your acceptable usage policy and explaining the changes of those effects to users • Theme 10 - Technical intrusion - such as the necessity to conduct a new vulnerability scan or penetration test |

¹⁷ [Theme 1 – Planning information security](#), Requirement 1; [Theme 5 - Assessing and treating risks](#)

| | |
|---|---|
| | <ul style="list-style-type: none"> • <u>Theme 11 - Backup and restore</u> - such as ensuring you can restore to an earlier point in case the change does not work as intended These are just examples which illustrate some of the wide-ranging impacts that changes may have. You may also need to update your business continuity and disaster recovery plans; further direction on this will be set out in <u>Theme 13 – Resilience: business continuity, incident management, and disaster recovery</u>. <i>b.</i> As per <u>Theme 3 - Assets</u>, safe disposal methods may include secure erasure and shredding. <i>c.</i> Users should not make changes without approval. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff. You may have already implemented a process whilst following the direction for <u>Theme 10 – Technical intrusion</u> . <i>d.</i> As determined in <u>Theme 10 - Technical intrusion</u>, you should maintain a list of software that is used within the organisation and ensure that only software from this approved list is installed on your devices. Ensure that this list remains updated with any changes; remember that software should be removed as it becomes unsupported or no longer needed. |
| <p>8. Ensure that personnel are updated as necessary when changes are made.</p> | <p>Remember that many policy changes will apply to everyone although some may be role specific; distribute policies to all people responsible for implementing them.</p> <p>This could be a physical copy or via email/instant messaging. You cannot just place the policy in a shared area, unless employees also receive an email/instant message with a link to the shared area and a request to click the link and view the policies. Consider if supporting training is needed and verify that all training and guidance given, both formally and informally, has been understood.</p> |


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

| | |
|----------------------------------|--|
| <p>What is this theme about?</p> | <p>No security measures can be fully effective all the time so you must be ready to keep working through, and recover from, the effects of deliberate attack, accidental damage, and natural disasters. This extends to a considered level of cyber liability insurance commensurate with the risk assessment to support recovery. Consider:</p> <ul style="list-style-type: none"> • How does the business ensure breaches of confidentiality, integrity, or availability of its data are detected and dealt with as required by law and decency to its customers, suppliers, contractors, and other stakeholders? • How does the business make sure that it can transform, renew, and recover in timely response from a partial or total loss of information assets? • How does the business learn the lessons following an incident and make improvements where necessary? |
|----------------------------------|--|


What are the requirements for this theme?

| Requirements | Guidance and tips for implementation |
|--|--|
| <ol style="list-style-type: none"> 1. Ensure breaches of confidentiality, integrity, or availability of your data are detected, recorded, and dealt with. <ol style="list-style-type: none"> a. Make sure that people you work with, and the public, know how to, and to whom, to report incidents. b. Make it clear who has the authority to invoke your business continuity measures and ensure everyone knows their responsibilities when dealing with incidents. | <p>This includes either partial or total loss of key information assets. Following the direction set out in Theme 12 - Secure business operations: monitoring, review, and change management will assist you to detect incidents.</p> <p>You should investigate incidents to identify the cause, repair the damage, and prevent the incident reoccurring. Investigate the incident and ensure those involved have sufficient knowledge and skills. The aim of the investigation is always to reduce the impact of the incident and to prevent its reoccurrence.</p> <p>Conducting a vulnerability scan may offer insight into the source of the incident and/or reveal any vulnerabilities that have been created by the incident. You can use an external company to provide an incident investigation service if needed, and this may be included with your cyber security insurance if you have any. It is important to keep an incident log of the actions taken by the investigations team because this can assist with subsequent investigations and reviews.</p> <ol style="list-style-type: none"> a. You may have created this already whilst following the direction set out in Theme 12 - Secure business operations: monitoring, review, and change management. |

| | |
|---|--|
| <p>i. Make sure it's clear who is responsible for disclosing details of a data breach.</p> | <p>b. It is important to act quickly during an incident. It must be clear who can make decisions when needed. You may have allocated some roles already whilst following the direction set out in Theme 2 - Organisation and Theme 7 - People.</p> |
| <p>2. Set out a communication policy which clearly defines:</p> <ul style="list-style-type: none"> a. Responsibilities for reporting incidents to customers and external authorities such as data protection agencies b. Responsibilities for handling any marketing or public relations implications c. Who is – and is not – allowed to talk about incidents outside the business | <p>Defining a communication policy is crucial to managing the incident and ensuring that clear and accurate messaging is released by your organisation. Consider your list of legal responsibilities including those to parties with which you have SLAs or contracts.</p> <p>Whilst following the direction for Theme 7 - People, you may have already outlined a communication policy regarding what can or can't be said about your business and the people involved in it on relevant platforms.</p> |
| <p>3. Create a Business Impact Assessment and prepare a Business Continuity and Disaster Recovery Plan about how you will deal with disruption to critical information assets. The plan must cover:</p> <ul style="list-style-type: none"> a. Preserving any information which may be required from a legal standpoint or disciplinary action b. Relevant responsibilities for personnel and management | <p>A Business Impact Assessment assesses the impact of a critical function being disrupted and outlines the actions to be taken to restore the function. A critical function might involve a combination of information, applications, systems, and people. Your contemporary risk assessment and risk treatment plan should provide the foundations for creating this, including highlighting where it may be prudent to take out insurance, such as cyber liability, to assist with recovery. Consider industrial action and natural phenomena such as flooding, as well as incidents like a data breach.</p> <p>Your Business Continuity and Disaster Recovery Plan should cover all areas of the organisation – your information security group, if you have one, can likely assist you with this. Draw on the expertise of your risk owners too. Your plan should be achievable and have specific timeframes for delivery, for example, to restore a critical system within 24 hours.</p> |

| | |
|--|--|
| <p>c. Useful contact numbers for any internal and external services or authorities you may need to involve</p> <p>i. Include copies (or references) to licence and Service Level Agreements</p> <p>d. Strategic priority for asset recovery and how this can be achieved</p> | <div style="text-align: center;">  <p><i>Template available:</i></p> <p>IASME can provide a <i>Business Impact Assessment and Business Continuity and Disaster Recovery Plan</i> template that can be adapted for most organisations.</p> </div> <p>a. Forensic examination of data can help identify the cause of an incident. You can use an external company to provide this service to you if needed.</p> <p>b. This includes reporting and communication responsibilities.</p> <p>c. Having a list of contact numbers prepared in advance can really help during the stress of dealing with an incident. Consider responsibilities for reporting incidents to customers and external authorities, as well as how you will contact supply chain partners and other stakeholders.</p> <p>d. Your Business Impact Assessment should enable you to understand and prioritise which assets are most critical to your objectives, and therefore must be 'recovered' first.</p> <p>For example, it may be more urgent to re-establish access to your email system to enable critical (incident) communication, rather than recover your sales records which may not be needed immediately. Use the 'asset importance ratings' (the relative value) recorded in your asset register¹⁸ to guide your prioritisation.</p> <p>In addition to utilising the backups of your data created in line with <u>Theme 11 - Backup and restore</u>, ensure your plan considers any software licenses, hardware, or other equipment needed for recovery. List where equipment can be purchased from, if it becomes necessary, and have the confidence that equipment can be securely configured to facilitate restoration within your defined timelines. Don't assume that (new) equipment will be easy to set up if, and when, it is needed.</p> |
| <p>4. Exercise your plan at least annually and keep it up to date to account for changes to your business.</p> | <p>You should carry out a table-top exercise where you create a plausible scenario (such as a staff member accidentally emailing confidential data to a client) and run through the incident response process to confirm that it works for your organisation. You can also treat any real incident as a test of the process.</p> |

¹⁸ Theme 3 - Assets, Requirement 2c

| | |
|--|---|
| |  <p><i>Important:</i> Don't wait for an incident to see if your plan works! An incident should not be the first time a new or updated plan should be rehearsed and benchmarked for its achievability.</p> <p>Ensure that sufficient knowledge of all areas of the organisation is included in the review. Involve a proportionate and representative group of suitable people - for example, members of the information security group, risk owners, or other individuals with specific security responsibilities. Representation must be made from the board/director/partner/trustee level. This will also assist with providing appropriate training. Your risk assessment may indicate that you need to rehearse your plan more frequently, even if your business has not changed.</p> |
| <p>5. Have your Business Impact Assessment and Business Continuity and Disaster Recovery Plan signed off by someone who is authorised to make decisions for your organisation.</p> | <p>This may be a director, board member, partner, trustee, or you, if you are a sole trader. Note: this is likely to be the leader you appointed to coordinate and act on information security activities in Theme 2 - Organisation. The approval process should consider the outcome of the review and test the plan's likely achievability.</p> |
| <p>6. Analyse your records for:</p> <ul style="list-style-type: none"> a. Recurring incidents b. Your effectiveness in dealing with an incident c. The effectiveness of your risk assessment and business impact assessment | <p>Identifying trends can indicate that security measures are ineffective and may need updating to address the causal problem. Some questions to consider include - how disruptive was the incident? Were your business continuity and disaster recovery plans effective? If not, why not?</p> |
| <p>7. Learn the lessons from the event(s)</p> <ul style="list-style-type: none"> a. Use the information gathered to review and update your risk assessment, and your risk treatment plan. | <p>View incidents as learning experiences. Use them to educate yourself and your staff, offering support through training where necessary.</p> <ul style="list-style-type: none"> a. Did the event provide new insight into the workings of your organisation? And does your risk assessment reflect this? Ensure that your risk assessment remains up to date as per Theme 5 - Assessing and treating risks . |

- i. Review incidents with top-level management at strategic and tactical meetings.
- b. Review your information security policies accordingly.

- i. Security (and reviewing any incidents) should be a standing agenda item at strategic and tactical meetings.
- b. Did the policy support you as intended before, during, after the incident? Refer to the direction set out in [Theme 8 - Policy realisation](#).



Important:

Although an incident necessitates reviewing your risk assessment and relevant policies, they do not always need changing; they may already accurately reflect the expected level of risk, the corresponding impacts that were realised during the incident, and the appropriate responses.



APPENDICES

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

The IASME Cyber Assurance standard provides a common benchmark and information security methodology which is achievable for SMEs. Certification to the Standard can be used to show compliance to many other standards.

Mappings to standards are available at <https://iasme.co.uk/iasme-cyber-assurance/mapping-to-other-standards/>

Cyber Essentials

Both the IASME Cyber Assurance standard and the international standard ISO 27001 are based on a risk-led approach. However, day-to-day information security risks are endemic within a wide range of organisations¹⁹ and it is challenging to set a baseline set of activities that are common to all.

Cyber Essentials was created to reduce the threat from common internet-based threats for all organisations. It is deliberately prescriptive and is aimed to provide a base level of controls. Cyber Essentials has similarities to the automotive 'MOT' – a test of basic roadworthiness not mechanical assurance. Whereas Cyber Essentials is about the basic technology, the IASME Cyber Assurance standard is about the technology, about you, and about where and how you work.

The IASME Consortium helped to develop the original Cyber Essentials requirements and is the sole partner for the National Cyber Security Centre's (NCSC) to operate the scheme.

To certify to IASME Cyber Assurance, your organisation must also achieve either Cyber Essentials or IASME Cyber Baseline (see below).

¹⁹ See NCSC (2016) *Common Cyber Attacks: Reducing The Impact*



IASME Cyber Baseline

IASME Cyber Baseline is a key cyber security certification which allows organisations to verify they have the basic technical cyber controls in place within their organisation. It has been developed by IASME to compliment the IASME Cyber Assurance scheme by providing the basic, secure virtual boundaries on which the IASME Cyber Assurance controls can build.

To certify to IASME Cyber Assurance, your organisation must also achieve either IASME Cyber Baseline or Cyber Essentials (see above).

ISO/IEC 27001:2017

ISO/IEC 27001 is the vanguard to a comprehensive set of standards comprising many titles, some of which address guidance for niche technologies or vertical markets. It sets out the components of an information security management system (ISMS) without giving specific direction on how to tailor the ISMS for a respective business. The IASME Cyber Assurance standard was created to bridge the gap between no ISMS and an ISO/IEC 27001-compliant ISMS.

There is a logical path for an SME to begin with the IASME Cyber Assurance standard and migrate to ISO/IEC 27001 when needed.

NCSC 10 Steps to Cyber Security

This is a set of high-level awareness guidance that centres on the information risk management regime (step one) and nine further steps to implement it. All these 10 elements are built into the IASME Cyber Assurance standard framework with a round-trip check to make sure that they are being done well enough.

Cyber Assessment Framework (CAF) and Security of Networks and Information Systems (NIS) directive

The Cyber Assessment Framework (CAF) is a cyber security benchmark created by NCSC for critical infrastructure organisations and their supply chain that must follow the EU Security of Networks and Information Systems (NIS) directive. The directive mandates activities that assure systems resilience with respect



to cyber attacks. An SME's involvement in critical infrastructure (CI) may be indirect through the supply of goods and services to operations higher up the CI supply chain.

The IASME Cyber Assurance standard provides a firm foundation to organise and present a demonstrable approach to information security that an SME's supply chain customers will expect by before they can engage and still meet the CAF benchmark.

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 Assurance 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. Like Cyber Essentials (*see above*), 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). Like DCP (see below) and the IASME Cyber Assurance standard, there is an element of risk profiling regarding the type of processing and storage that goes on in a business.

Defence Cyber Protection Partnership (DCPP) Cyber Risk Profiles

The IASME Cyber Assurance standard and the DCPP Cyber Risk Profiles specification (Defence Standard 05-138) have the common ground of basing the expected attention to security on the likely threats that risk the business' confidentiality, integrity, and availability.



General Data Protection Regulation (GDPR)

GDPR and the Network Information Security directive have certain nuances – such as the consent issues in GDPR or the breach reporting requirements of both GDPR and NIS. The IASME Cyber Assurance standard is about good security practice. Both legal instruments have at their core a requirement to follow good security practice. So, an entity which complies with the IASME Cyber Assurance standard passes straight along the line that these governmental requirements set out and have only to concern themselves with the nuances.

The IASME Cyber Assurance standard prepares a company for this with its requirements to match legal and regulatory expectations and to have the requisite set of policies that defines for itself how it does it (*see Theme 8 - Policy realisation and Appendix C – Explicit and implied information security policies*).

The core of GDPR enshrines, in law, the basic principle of the IASME Cyber Assurance standard– know what you are protecting and understand its relative value to its subjects and so the impact of a security breach. This way, honest protective measures can be put in place and counterbalanced with routes to recovery after an incident. Additional supporting guidance for those seeking to implement the standard in tune with the nuances of GDPR is available at <https://iasme.co.uk/gdpr/>

Appendix B – Carrying out your information risk assessment

Your objectives, and the risks to fulfilling these, will – on the whole – be unique to your organisation. Nevertheless, there are some risks that will be common to most organisations, regardless of the nature of their operations. The following table consolidates some of these risks that are referenced throughout the thirteen themes in this standard to set your risk assessment on the right path.



Important:

This table is not an exhaustive list of the risks (and corresponding risk treatment actions) that you should consider. It is designed as a starting point for conducting your own comprehensive review of information risk. The topics listed below alone are unlikely to produce a risk assessment that is adequate and comprehensive enough to be worthwhile.

Topics catalogued in [Appendix C – Information security policies](#) will overlap with this table; the policies you define and implement should be based on the thoughtful decisions taken whilst conducting your risk assessment.

Table 4: Topics for your comprehensive risk assessment

| Topics and risks for consideration | Key requirements and guidance |
|--|--|
| What is the value of your information assets? At least consider the relative values to one another. Which are your most critical business systems? | <ul style="list-style-type: none"> • Theme 3 - Assets (Requirements 1 and 2c) • Theme 13 – Resilience: business continuity, incident management, and disaster recovery (Requirement 3) |
| Which assets should, or should not, be encrypted? How will encryption be implemented and managed to balance asset confidentiality, with the requirement for information integrity, and availability? | <ul style="list-style-type: none"> • Theme 3 - Assets (Requirement 3) • Theme 5 - Assessing and treating risks (Requirement 9) |
| How can you practicably deploy mobile device management (MDM) technology on portable devices and manage this securely? | <ul style="list-style-type: none"> • <u>Theme 3 - Assets</u> (Requirement 3ci) |

| Topics and risks for consideration | Key requirements and guidance |
|--|--|
| <p>Based on your risk appetite, which information resources are secure to use? How can you use your information assets acceptably?</p> | <ul style="list-style-type: none"> • Theme 5 - Assessing and treating risks (Requirement 8) • Theme 7 - People (Requirement 2) |
| <p>What can and can't be said about the business on relevant platforms? Consider email, social-media, or even face-to-face. Is this different when an incident occurs? Do these rules differ for people depending on their role?</p> | <ul style="list-style-type: none"> • Theme 7 - People (Requirement 2) • Theme 13 – Resilience: business continuity, incident management, and disaster recovery (Requirement 2) |
| <p>What physical risks are your information assets exposed to? Consider events and incidents such as, theft, loss, or damage (accidental or deliberate). Can the environment(s) surrounding your information assets (including when traveling or working from home) affect their confidentiality, integrity, and availability?</p> | <ul style="list-style-type: none"> • Theme 6 - Physical and environmental protection • Theme 9 – Managing access • Theme 10 - Technical intrusion |
| <p>What is the likelihood that staff will make a mistake that impacts information security? What are the risks of privileges being abused? Can information-related mistakes pass unnoticed? What level of role segregation, and the corresponding access to resources, is needed to manage this to avoid contagion?</p> | <ul style="list-style-type: none"> • Theme 2 - Organisation (Requirement 1a) • Theme 7 - People • Theme 9 – Managing access (Requirement 1) |
| <p>What risk is presented to the organisation by devices that are not internet-connected and so might not be covered by controls from Cyber Essentials or IASME Cyber Baseline? Can you apply additional controls to these devices if they are important to your organisation? Does the organisation use paper-based systems?</p> | <ul style="list-style-type: none"> • Theme 5 - Assessing and treating risks (Requirement 2) |
| <p>What is a suitable time limit to set for devices and systems to sign out after a period of inactivity? How do you balance this with the potential inconvenience to</p> | <ul style="list-style-type: none"> • Theme 9 – Managing access (Requirement 5) |

| Topics and risks for consideration | Key requirements and guidance |
|---|--|
| the authorised user when they need to go through some level of authentication again? | |
| How will the business protect personal data? How do you make those measures compliant with relevant data protection legislation and regulation? | <ul style="list-style-type: none"> • Theme 3 - Assets • Theme 4 - Legal and regulatory landscape • Theme 5 - Assessing and treating risks • Theme 7 - People (Requirement 1) |
| <p>Do customers, partners, contractors, and suppliers have access to your systems and data remotely or onsite? Are they reliable enough to meet your needs in time? What would happen if they can't?</p> <p>Which data handling and security requirements should be included in the contracts with all your contractors and suppliers? (Include cloud providers and sub-contractors.)</p> | <ul style="list-style-type: none"> • Theme 2 - Organisation (Requirement 4) • Theme 5 - Assessing and treating risks (Requirement 4) • Theme 7 - People |
| What is the risk of malware infection? Which other cyber threats are present? Consider criminal activity. How quickly are new threats expected to emerge? | <ul style="list-style-type: none"> • Theme 5 - Assessing and treating risks • Theme 10 - Technical intrusion |
| How does your organisation utilise removeable media? Do you need a dedicated machine to scan 'new' removable media before allowing its use in day-to-day systems? What are the risks of unauthorised removeable media being connected to your systems? Are physical or technical controls needed to manage this? | <ul style="list-style-type: none"> • Theme 10 - Technical intrusion (Requirement 4) |
| Does the business have sensitive or critical systems and networks that require segregation? | <ul style="list-style-type: none"> • Theme 9 – Managing access (Requirement 3) |

| Topics and risks for consideration | Key requirements and guidance |
|--|---|
| Which intrusion detection and prevention methods and tools are needed to detect unauthorised activity, whether from internal or external sources? | <ul style="list-style-type: none"> • Theme 10 - Technical intrusion (Requirement 1) |
| How often should systems be scanned for vulnerabilities? Should any systems undergo further penetration testing? | <ul style="list-style-type: none"> • Theme 10 - Technical intrusion (Requirement 2 and 3) |
| Is the business planning to change working practices (as set out by policy), technology, or both (including where assets are decommissioned)? What are the associated risks? | <ul style="list-style-type: none"> • Theme 1 – Planning information security • Theme 5 - Assessing and treating risks (Requirement 1) • Theme 12 - Secure business operations: monitoring, review, and change management (Requirement 7 and 8) • Theme 8 - Policy realisation (Requirement 5) |
| How much work can the business afford to redo? How often does the business need to make backups and test that they can be restored? How will backups be protected so that they are at least as secure as the working copy? | <ul style="list-style-type: none"> • Theme 11 - Backup and restore |
| How long should the business retain information for? What are the risks of holding (and using) data that is inaccurate or no longer relevant? What processes are needed to manage this? | <ul style="list-style-type: none"> • Theme 3 - Assets (Requirement 2d, 5 and 6) • Theme 4 - Legal and regulatory landscape (Requirement 2 and 4) • Theme 12 - Secure business operations: monitoring, review, and change management (Requirement 3) |
| How often does the business need to rehearse the business continuity and disaster recovery plan to be confident that it's achievable and that everyone understands their responsibilities in the event of an incident? | <ul style="list-style-type: none"> • Theme 13 – Resilience: business continuity, incident management, and disaster recovery |

Appendix C – Information security policies

The IASME Cyber Assurance standard was designed for SMEs and recognises that SMEs thrive on their agility. Therefore, you are expected to hold only a fitting amount of guiding documentation and evidence of good information security practices to give assurance. The IASME Cyber Assurance standard is designed to show a balance of proactive measures and the capability to be resilient in the face of accidental or deliberate information security incidents.

Your business documentation must be right-sized for you and useful for maintaining a visible commitment to managing information security well. You will use the documentation to show commitment at the highest level, clear accountability, and responsibility.



Important

- You don't need to record every policy in a separate document (Figure 5) but you do need to ensure that your policies are successfully implemented across your business.
- If a contract calls for a policy to be documented, you would be expected to do so.
- Some of your policies may be documented in various practical places such as business plans, a contract with a supplier, or a staff contract.
- Bullet points are acceptable provided all necessary content is covered with suitable clarity including:
 - The purpose of the policy
 - A defined scope
 - The requirements of the policy ("what people need to do")
 - When the policy will be reviewed for its continued fit to the business
 - How it's monitored to make sure that it's implemented correctly and is working for the business
 - What happens if the policy is breached



Figure 5 - Two examples of valid approaches to policies

The following table provides a list of **explicit** and **implied** information security policies in line with the IASME Cyber Assurance standard.

- **Explicit** policies are those that **must be documented**. The  icon highlights these in the table.
- **Implied** policies are not required to be documented, unless your risk assessment suggests this would be a good approach.

Your risk assessment may suggest additional policies are relevant to your organisation that are not listed – the table is offered as a baseline only.








Template available:






IASME can provide a suite of security templates, covering many of the topics in table, that can be adapted for most organisations.




Note: The order and grouping of the policies listed in this table is just one view of the many interrelated topics. Your policies may group topics and areas differently to pragmatically address the needs of your organisation. Not every business – and certainly not all staff within a business – will find that every policy in the table is applicable to them. Policies, or specific areas of a policy in the table, may be justifiably excluded if they are not applicable to any part of your organisation. However, the policies listed below will usually apply to most.




Table 5: Information security policies

| Policy group | Policy topic | Areas covered | Key requirements and guidance | Must be documented? |
|--------------|---|---|---|---|
| Governance | Governance – an overall security policy | Detailing management commitment to security, policies, governance and organisation of policy, authority for enforcing policies and management review. | <ul style="list-style-type: none"> • Theme 2 - Organisation • Theme 5 - Assessing and treating risks • Theme 8 - Policy realisation • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| | Third party and supply chain | Expectations for how agreements will be set, reviewed, and updated with third parties in your supply chain. | <ul style="list-style-type: none"> • Theme 2 - Organisation • Theme 5 - Assessing and treating risks • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| | Risk management | This covers risk assessment, acceptable levels, treatment, business continuity and resilience including disaster recovery. | <ul style="list-style-type: none"> • Theme 1 – Planning information security • Theme 5 - Assessing and treating risks • Theme 6 - Physical and environmental protection • Theme 11 - Backup and restore • Theme 12 - Secure business operations: monitoring, review, and change management • Theme 13 – Resilience: business continuity, incident management, and disaster recovery | |






| Policy group | Policy topic | Areas covered | Key requirements and guidance | Must be documented? |
|-----------------------------|---|--|---|---|
| Information asset lifecycle | Acquisition of hardware, software, and data | How such items are evaluated, monitored, accepted and licensed/registered. | <ul style="list-style-type: none"> • Theme 1 – Planning information security • Theme 2 - Organisation • Theme 3 - Assets • Theme 4 - Legal and regulatory landscape • Theme 5 - Assessing and treating risks • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| | Classification of information assets | How information assets should be prioritised and marked in terms of risk to the business. | <ul style="list-style-type: none"> • Theme 3 - Assets • Theme 4 - Legal and regulatory landscape |  |
| | Ownership and responsibilities | Who owns different information assets (both intangible and physical). | <ul style="list-style-type: none"> • Theme 3 - Assets | |
| | Media handling | How to store and handle media containing information, including when assets are being transported. | <ul style="list-style-type: none"> • Theme 3 - Assets • Theme 5 - Assessing and treating risks • Theme 6 - Physical and environmental protection • Theme 7 - People • Theme 11 - Backup and restore |  |




| Policy group | Policy topic | Areas covered | Key requirements and guidance | Must be documented? |
|--------------------------------|---|---|--|---|
| | Mobile devices | Specific requirements for portable devices such as laptop computers, tablets, and portable storage. | <ul style="list-style-type: none"> • Theme 3 - Assets • Theme 6 - Physical and environmental protection • Theme 7 - People |  |
| | Retention | Covering how long you need to keep each type of data for items such as personal data, business records, old (versions of) policies and backups, and logs and records produced by your monitoring systems. | <ul style="list-style-type: none"> • Theme 3 - Assets • Theme 4 - Legal and regulatory landscape • Theme 5 - Assessing and treating risks • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| | Disposal of computer equipment and information assets | How to securely destroy information assets, both physical and intangible. | <ul style="list-style-type: none"> • Theme 3 - Assets • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| Legal and regulatory landscape | Legal and regulatory compliance | How the company will comply with relevant legislation and regulations. | <ul style="list-style-type: none"> • Theme 4 - Legal and regulatory landscape |  |
| | E-commerce and credit card handling | Compliance with e-commerce legislation and credit card standards such as PCI. | <ul style="list-style-type: none"> • Theme 4 - Legal and regulatory landscape | |
| | Intellectual property | How intellectual property should be managed and how to comply with relevant legislation. | <ul style="list-style-type: none"> • Theme 3 - Assets • Theme 4 - Legal and regulatory landscape |  |


| Policy group | Policy topic | Areas covered | Key requirements and guidance | Must be documented? |
|---------------------------------------|-------------------------|--|--|---|
| | Data protection | How the business will handle and protect personal data, including complying with relevant data protection legislation and regulation. | <ul style="list-style-type: none"> • Theme 2 - Organisation • Theme 3 - Assets • Theme 4 - Legal and regulatory landscape • Theme 5 - Assessing and treating risks • Theme 7 - People • Theme 13 – Resilience: business continuity, incident management, and disaster recovery |  |
| Physical and environmental protection | Physical security | Keeping assets safe from physical loss or damage considering, for example, physical access to locations and systems, and environmental conditions such as heating and cooling of equipment. | <ul style="list-style-type: none"> • Theme 6 - Physical and environmental protection • Theme 9 – Managing access |  |
| | Clear desk policy | Ensuring that office environment is regulated and controlled. | <ul style="list-style-type: none"> • Theme 6 - Physical and environmental protection | |
| People and acceptable usage | Data and account access | For permanent staff, temporary staff, contractors, and suppliers, detailing identity verification and vetting, new starter data access, data access for leavers, modifications and access privilege review and management. | <ul style="list-style-type: none"> • Theme 7 - People • Theme 9 – Managing access • Theme 6 - Physical and environmental protection • Theme 12 - Secure business operations: monitoring, review, and change management |  |

| Policy group | Policy topic | Areas covered | Key requirements and guidance | Must be documented? |
|--------------|---------------------------------|--|--|---|
| | Acceptable use of computers | Covering topics such as personal use (including personal social media accounts), BYOD, and removeable media usage. | <ul style="list-style-type: none"> • Theme 5 - Assessing and treating risks • Theme 7 - People • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| | Data sharing and communications | Regulate which information can be shared and how, covering regular day-to-day business operations, and during and after incidents. Include responsibilities for reporting incidents as required by law and decency to customers and the respective external authorities, and responsibilities for handling any marketing or public relations implications. | <ul style="list-style-type: none"> • Theme 7 - People • Theme 9 – Managing access • Theme 13 – Resilience: business continuity, incident management, and disaster recovery | |
| | Social media | Who and what may be posted on social media, forums, and websites. Consider what may cause offence or attract unwanted attention (religion, politics, libel, customer details, journeys, locations) especially where several pieces of information may come together to disclose information. | <ul style="list-style-type: none"> • Theme 7 - People • Theme 9 – Managing access • Theme 13 – Resilience: business continuity, incident management, and disaster recovery |  |
| | Remote working | Covering how staff should act when working remotely/teleworking, including from home, client sites, or when travelling | <ul style="list-style-type: none"> • Theme 6 - Physical and environmental protection • Theme 7 - People |  |

| Policy group | Policy topic | Areas covered | Key requirements and guidance | Must be documented? |
|---------------------|------------------------|---|--|---------------------|
| | | | <ul style="list-style-type: none"> • Theme 9 – Managing access | |
| | Training and awareness | How training commensurate with roles and responsibilities and end-user guidance to security issues is provided. | <ul style="list-style-type: none"> • Theme 7 - People • Theme 12 - Secure business operations: monitoring, review, and change management • Theme 13 – Resilience: business continuity, incident management, and disaster recovery | |
| Managing technology | Architecture | How systems such as internal servers, data centres, cloud (both private and public) are managed and securely deployed so that they support the work done with adequate flexibility. | <ul style="list-style-type: none"> • Theme 3 - Assets • Theme 5 - Assessing and treating risks • Theme 10 - Technical intrusion | |
| | Internet connection | Topics relating to internet access, permitted protocols (including wireless and VOIP), content filtering, firewall, internet facing services, demilitarised zone (DMZ), routers and switches. | <ul style="list-style-type: none"> • Theme 6 - Physical and environmental protection • Theme 9 – Managing access • Theme 10 - Technical intrusion • Theme 12 - Secure business operations: monitoring, review, and change management | |
| | Remote access | Criteria for allowing remote access, such as utilising Virtual Private Networks (VPN). | <ul style="list-style-type: none"> • Theme 9 – Managing access • Theme 10 - Technical intrusion | |

| Policy group | Policy topic | Areas covered | Key requirements and guidance | Must be documented? |
|--------------|--|---|---|---|
| | Encryption | Management of cryptographic communications, devices, and stored data. | <ul style="list-style-type: none"> • Theme 3 - Assets • Theme 5 - Assessing and treating risks |  |
| | Authentication, passwords and key management | How authorised users only are authenticated onto systems and management of cryptographic keys and passwords that provide access to information. | <ul style="list-style-type: none"> • Theme 5 - Assessing and treating risks • Theme 9 – Managing access • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| | Testing | How the Demonstration/Testing/ Sandbox Facility is to be setup and configured. | <ul style="list-style-type: none"> • Theme 9 – Managing access • Theme 12 - Secure business operations: monitoring, review, and change management | |
| | Change Management | New Installations and Change Management Procedures including data quality and integrity, backup and storage. | <ul style="list-style-type: none"> • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| | Configuration management | How to keep configuration of systems secure including vulnerability management/ patching. | <ul style="list-style-type: none"> • Theme 10 - Technical intrusion • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| | Protection against malicious software | How the company protects against viruses, Trojans, worms, adware and spyware. | <ul style="list-style-type: none"> • Theme 10 - Technical intrusion • Theme 12 - Secure business operations: monitoring, review, and change management |  |

| Policy group | Policy topic | Areas covered | Key requirements and guidance | Must be documented? |
|-------------------------------------|--------------------------|---|--|---|
| Backup | Backup | How the business backs up its information, including how often backups are made, how backups are kept secure, and testing to ensure backups can be restored. | <ul style="list-style-type: none"> • Theme 11 - Backup and restore |  |
| Monitoring, review, and improvement | Monitoring | Topics such as Intrusion detection/prevention (both technically and physically), tracking system access and usage, non-repudiation and log management. | <ul style="list-style-type: none"> • Theme 6 - Physical and environmental protection • Theme 10 - Technical intrusion • Theme 12 - Secure business operations: monitoring, review, and change management |  |
| | Assessment | Auditing of the company (including internal and external) and realising opportunities to improve information security. | <ul style="list-style-type: none"> • Theme 2 - Organisation • Theme 4 - Legal and regulatory landscape • Theme 7 - People • Theme 8 - Policy realisation • Theme 12 - Secure business operations: monitoring, review, and change management | |
| Resilience | Vulnerability disclosure | Covering contact information for the reporting of issues, and information on timelines for the initial acknowledgement of receipt and for status updates until the resolution of the reported issues. | <ul style="list-style-type: none"> • Theme 7 - People • Theme 12 - Secure business operations: monitoring, review, and change management • Theme 13 – Resilience: business continuity, incident management, and disaster recovery |  |

| Policy group | Policy topic | Areas covered | Key requirements and guidance | Must be documented? |
|--------------|---|---|--|---|
| | Incident management and business continuity | How the business prepares for, and manages, incidents including business continuity and disaster recovery planning, points of escalation, and incident logging. | <ul style="list-style-type: none"> • Theme 7 - People • Theme 10 - Technical intrusion • Theme 12 - Secure business operations: monitoring, review, and change management • Theme 13 – Resilience: business continuity, incident management, and disaster recovery |  |

Appendix D – Glossary

| Term | Definition |
|---------------------|--|
| Accountable | Having to face up to the impact of decisions made. An individual who takes sole ownership for a particular item, process, or task and the respective decisions relating to these. This includes decisions made directly by the accountable person or where approval was granted for a decision made by a <i>responsible</i> party. |
| Access control | The practical measures that you put in place to protect your information assets from the risks of unauthorised access. (This is a specific kind of <i>Control</i>). |
| Availability | The state of ensuring that information assets are available to those who are authorised to access or use them. |
| 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 | 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. |
| Confidentiality | The state of keeping <i>information assets</i> protected from those who are <u>not authorised</u> to access or use them. |

| Term | Definition |
|-----------------------|--|
| Contractor | Contractors are often taken on to carry out a specific task for your organisation. This Standard uses the term contractor 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 “contractor” and “supplier” are closely related and have become increasingly blurred. <i>See supplier.</i> |
| Control | The practical measures that you put in place to protect your information assets from risks. |
| Cyber Essentials | Cyber Essentials is a Government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks. This is also the name of the basic level of certification that can be awarded under this scheme. |
| Cyber Essentials Plus | Cyber Essentials is a Government-backed, industry-supported scheme to help organisations protect themselves against common cyber attacks. Cyber Essentials Plus is a higher level of assurance through the internal and external testing of the organisation’s systems for certain vulnerabilities. |
| Cyber security | The assurance of <i>confidentiality, integrity, and availability</i> of information stored and processed on electronic devices that are usually interconnected. |
| Data Breach | An incident that leads to a compromise of the <i>confidentiality, integrity, or availability</i> 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. |
| 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 <i>confidentiality, integrity, of availability</i> of your <i>information assets</i> . |
| DMZ | Demilitarised zone. A network location between trusted resources and untrusted resources (usually the internet) where servers and other externally facing equipment may be located. |
| Footprint | The physical or virtual areas where your organisation has a presence. |
| HVAC | Heating, ventilation, air conditioning. |

| Term | Definition |
|----------------------------------|--|
| 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 <i>confidentiality, integrity, and availability</i> . |
| Information security | A state of <i>confidentiality, integrity, and availability</i> commensurate with the value of the information under scrutiny. |
| Integrity | The state of information being accurate, consistent, and untampered with. |
| MDM software | Mobile Device Management software. A program used to administer portable devices which often including tools such as, encryption, update management, location tracking, remote wipe, and secure isolated containers (sandbox) for using sensitive data or applications. |
| Micro enterprise or organisation | Comprises less than 10 staff and a turnover or balance sheet of \leq €2 m respectively. (Source: EU recommendation 2003/361, Official Journal of the European Union EN 20.5.2003) |
| Medium-sized organisation | Comprises between 51 and 250 staff, a turnover of \leq €50m or a balance sheet total of \leq €43m. (Source: EU recommendation 2003/361, Official Journal of the European Union EN 20.5.2003) |
| NCSC | The National Cyber Security Centre is the national technical authority for information assurance within the UK, providing the definitive voice on the technical aspects of information security across the most critical organisations in the UK, the wider public sector, industry, and SMEs. It was formed from CESG (Communications-Electronics Security Group), the Centre for Cyber Assessment, CERT-UK, and the Centre for Protection of National Infrastructure (CPNI). |
| 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 <i>'Business'</i> . |
| Personal data | Any information relating to an identified or identifiable natural person – a <i>'data subject'</i> . (Source: EU Regulation 2016/679, Official Journal of the European Union EN 4.5.2016) |

| Term | Definition |
|-------------------|--|
| 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 <i>control</i> 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 <i>accountable</i> 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. |
| Risk appetite | A threshold that defines how much risk can be accepted. This is usually decided by the respective <i>risk owner(s)</i> but should be in collaboration to process the overall risk appetite of the organisation. |
| Risk owner | The person accountable for decisions relating to a risk. <i>See accountable.</i> |
| Risk treatment | The response taken to an identified risk such as prevention, reduction, outsource/transfer of treatment, or acceptance. |
| Role | A defined set of responsibilities. One person may hold multiple roles, or sometimes a single role may be shared between a team. <i>See responsible.</i> |
| Security | A state of grace wherein the assets under scrutiny are adequately protected from the realisation of risks to them. |
| Security breach | <i>See security incident.</i> |
| 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 <i>confidentiality, integrity, or availability</i> of information assets. |

| Term | Definition |
|----------------------------------|---|
| Sensitive personal data | A subset of <i>personal data</i> which has greater ramifications if involved in a <i>security incident</i> . 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. |
| Small enterprise or organisation | Comprises between 11 and 49 staff, and a turnover or balance sheet of ≤ €10 m respectively. (Source: EU recommendation 2003/361, Official Journal of the European Union EN 20.5.2003.) |
| SME | Comprises less than 250 staff and a turnover or balance sheet of ≤ €50m or €43m respectively. (Source: EU recommendation 2003/361, Official Journal of the European Union EN 20.5.2003.) |
| 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 “contractor” and “supplier” are closely related and have become increasingly blurred. <i>See contractor.</i> |
| 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 E – The IASME family of practical information and cyber security certifications

The IASME Cyber Assurance 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 Assurance.

| Scheme | Description | Level 1 Verified self- 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) | ✓ | ✓ |
| CAA Assure | Complete set of cyber security controls for civil aviation | | ✓ |