THE IASME CYBER ASSURANCE STANDARD V7.0

Micro Organisation (3 – 9 people)

(Formerly known as IASME Governance)

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
7.0	May 2025	Detailed revision, restructure, update of the standard and the introduction of Themes and Requirements by organisational size in separate documents. This document contains the Standard Themes and Mandatory Requirements for an organisation size of Micro.

TABLE OF CONTENTS

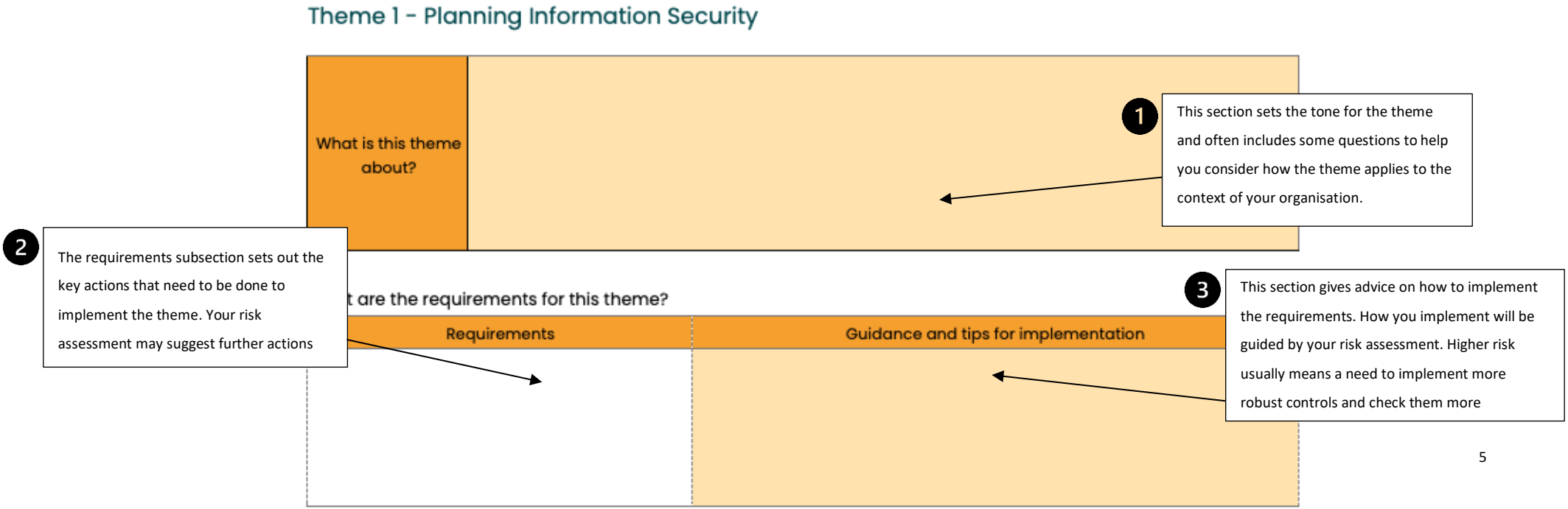
THE FOURTEEN THEMES: REQUIREMENTS AND GUIDANCE

The IASME Cyber Assurance standard comprises of activities which are divided into Fourteen 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 Fourteen 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

Mandatory Requirements

The mandatory requirements for your organisation size are highlighted in green. They are based on the minimum controls that IASME would expect a Sole Trader / Two Person Partnership to implement. They are based on the following being fully implemented:

1. Security Policy
2. Risk Assessment
3. Business Impact Analysis / Business Continuity plan

IASME can provide templates for each of the above that should be tailored to your organisation. IASME CBs can provide guidance on all areas of the standard if required.

Requirements highlighted in grey are not mandatory, however, your organisation may need to implement some of these controls based on your risk assessment. If your risk assessment highlights that your organisation requires any of the non-mandatory controls those should be implemented in line with the requirements in the standard.

Theme 1 - Planning Information Security

What is this theme about?	Planning is about making decisions in advance. Some planning relates to your day-to-day activities, such as serving customers or manufacturing a product. Other planning might be focused on a particular project to ensure that you have considered its security impact. You also need to plan how to react to certain events such a cyber-attack or an error made by a member of staff or contractor. As part of this theme, you should consider: • How do you build right-sized security into all your business activities? • How do you consider the security impact of change on your staff, customers, and other stakeholders, your working practices, hardware and software?

What are the requirements for this theme?

Requirements	Guidance and tips for implementation
1. Make provisions for information security as part of your business planning. a. Plans should be achievable with specific dates for delivery.	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. Planning recurs throughout the themes and is fundamental to good information security, see especially

	Theme 11 – Change Management *Theme 12 - Secure business operations: monitoring and review* The next themes in the standard will help you organise and formulate your plans.

Theme 2 - Organisation

What is this theme about?	A clear structure within your organisation is the foundation for effective and successful security. Consider: • 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
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. a. Review information security activities with board members/directors/partners/trustees so that they can understand and take responsibility for security risks.	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. 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. 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.
2. Appoint a suitably skilled leader with the authority to coordinate and act on information security activities. a. Define the responsibility of directors to make clear their direct involvement in setting levels of acceptable risk.	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. 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.

	 *Important:* 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. 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. a. This will depend on the decisions you have made for *Requirement 2* on who is most appropriate to hold the authority to coordinate and act on information security activities.
3. Form a group – or a network of people – from across the organisation to coordinate and implement information security activities. a. Make responsibilities clear. If you have a system of staff appraisal, include the information security work within objectives.	Micro organisations, with only a few members, can implement this informally; larger organisations need more formal structures to preserve the group communication channels. Your group's activities can include: • 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

	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. However, ensure that people can handle their responsibilities and workload and consider the appropriate segregation of roles. 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 identify any changes needed to roles and responsibilities and identify any relevant training or additional support needed for the role. *(Further direction on securely managing personnel, including segregation of roles, will be provided in Theme 7 - People)*
4. Define Service Level Agreements (SLAs), or other contracts, that set expectations for service provision and responsibilities with your partners and supply chain.	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. 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:

	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 Conducting and maintaining your risk assessment will help you to understand the information security requirements you need to put in your agreements. *(Further direction will be provided in Theme 5 – Assessing and treating risks)* 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 obligations. Examples as above: Ensure that your agreements and risk assessment are amended as necessary so that they continue to support your organisation's objectives.

Theme 3 - Assets

What is this theme about?	It is important to understand what you have and how to protect it. Consider: • 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?

Requirements	*Guidance and tips for implementation*
1. Keep an up-to-date register of *all* your information assets. a. Your asset register must include any personal devices (BYOD) if your security policies allow staff to use them for business purposes.	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. 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.

	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. 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. *(Further direction on change management will be provided in Theme 11 – Change Management and Theme 12 - Secure business operations: monitoring and review)*  *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	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

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	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]. 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.

	(Further direction on resilience will be provided in Theme 13 – Backup and restore and Theme 14 – Resilience: business continuity, incident management, and disaster recovery) 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.
3. Sensitive assets must be clearly identifiable.	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. 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. Consider that marking a document with a 'Confidential' or 'Secret" marking may draw more attention to it. This can have positive and negative impacts. You don't have to use protective marking if you have other ways to keep sensitive information identified and protected. *(Further direction on access controls will be provided in Theme 9 – Managing access and Theme 6 – Physical and environmental protection)*

4. Encrypt by default: a. Sensitive personal data b. Removable media (if allowed by your security policies) c. Portable devices *i.* Configure a remote wipe capability on portable devices where practicably possible d. Data stored on, and in transit to and from, the cloud	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. 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. 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.
5. Review the data you hold at least annually to ensure it is still relevant and accurate.	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.
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	*Guidance and tips for implementation*
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	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 See **Table 1** below for a sample of information-related legislation which may be relevant to businesses operating in the UK.
2. Ensure that you have the support in your business processes to fulfil any legal obligations.	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 *all* your business objectives, including meeting legal requirements. (Further direction on policy creation and management will be provided in *Theme 8 – Policy realisation*)

3. Monitor compliance and do what needs to be done to counter deviations or to improve your business processes.	Your day-to-day activities should align with your processes and policies. If these are not being met – why not? Has the necessary training and resource been provided? Do your policies and processes need amending? Is your last resort – disciplinary action – needed? 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. Further direction on these topics will be provided in *Theme 7 – People* and *Theme 12 – Secure business operations: monitoring and review*
4. Ensure that your business records are protected from loss, destruction, or falsification in accordance with your obligations.	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. 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.

Important:

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

Table 1: 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

What is this theme about?	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. The security controls you apply to your organisation should be influenced by your risk assessment and your risk appetite. 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.

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*
1. Gain vigilant oversight of the risks in your business by creating and maintaining an up-to-date information risk assessment. a) This must be reviewed: a. At least annually b. In anticipation of changes	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.  *Template available:*

c. Following any incidents	IASME can provide a *risk assessment and treatment plan* template that can be adapted for most organisations. Additionally, the ISAME ICA Risk Assessment Guidance document compiles some of the topics and areas of risk referenced in the IASME Cyber Assurance standard's fourteen themes. It offers a starting point for conducting your own comprehensive review of information risk. 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 11 –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.

Important:

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. *Further guidance on incidents will be provided in Theme 14 – Resilience: business continuity, incident management, and disaster recovery*
2. Extend the risk assessment to customers, partners, contractors and suppliers.	Consider: 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 suppliers – 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 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*.
3. Be aware of other business risks being addressed and integrate these with your information risk assessment.	Other business risks may include:  Environmental risk  Operational risk  Legal and regulatory risk  Market risk  People risk  Health and safety risk  Political risk

4. Keep up to date with emerging cyber threats and feed these into your risk assessment process. a. Maintain knowledge of emerging threats and countermeasures using expert advice.	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. 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.
5. Agree your organisations level of acceptable risk (or risk appetite).	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. 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*.

6. Assign the ownership of each risk and its treatment to a named owner	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! 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.
7. 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 - BYOD  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 for most organisations. *Note: further direction on this topic will be* provided in *Theme 7 - People* and in *Theme 8 - Policy realisation*.
8. 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 5). 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 11 - Change management*. Remember that responsibility for actions can be delegated to other people but the relevant risk owner must approve any work (see Requirement 6).

9. 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 *Theme 2 - Organisation.* 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

What is this theme about?	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: • 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.	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. 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. The measures you take – such as smoke and fire detection and suppression, intruder alarms – 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).
3. Consider which physical access controls are needed to protect your regular office environment a. For people internal to your organisation b. For people external to your organisation who may wish to access your premises	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.  *Template available:* IASME can provide a *keyholder tracker* template that can be adapted for most organisations.

	a. Refer to the roles assigned to personnel in line with the direction set out in *Theme 2 - Organisation* and *Theme 7 - People*. 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.
4. Restrict access to wired and wireless networks to authorised users.	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.
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.	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.
6. Extend physical and environmental protection to cover information assets taken outside your regular premises.	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

a. Ensure your policies can cope with rules that potentially conflict with those determined by parties in control of the external environment.	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

What is this theme about?	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: • 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
1. Clearly assign specific roles and responsibilities relating to information governance to named individuals. a. Segregate work – and access to the resources needed – to match these responsibilities, according to the associated risks.	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. Remember that one person may have multiple roles but ensure that people can

b. If you have a system of staff, supplier, or contractor appraisal, include the information security work within objectives.	handle their responsibilities and workload, and consider the appropriate segregation of roles - 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. Further direction on access controls to support role segregation will be provided in *Theme 9 – Managing access* and *Theme 6 - Physical and environmental protection*) 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.
2. Establish explicit rules for the acceptable use of your company assets. These must include at minimum: a. Whether personal use is allowed, and if relevant, what level of personal use is permissible	Use your risk assessment, legal responsibilities, and asset register which define relative asset values to guide you. 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*).

b. What can or can't be said about your business and the people involved in it on internet platforms	 *Template available:* IASME can provide a suite of security policy templates, which cover acceptable usage and access control, that can be adapted for mostorganisations. Note: that further direction on policies will be provided in *Theme 8 - Policy realisation*. 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. *(Further information will be provided on this in Theme 14 – Resilience : Business continuity, Incident management, and Disaster recovery).*
3. Ensure that everyone who has access to the data in your information systems: a. Is suitable from a security viewpoint before and during employment b. Is contractually obligated:	This includes permanent and temporary staff, whether full or part time, on contract, paid or unpaid. a. Refer to your list of legal obligations 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 a have a legal basis for carrying them out.

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	Ensure that suitability remains – do visas have an expiration? Is the person susceptable 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 and review*)
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	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.
d. Is aware of current threats	
e. Is able to report vulnerabilities and incidents without receiving blame and make suggestions	c. Responsibilities include: how to use assets, reporting discovered vulnerabilities or incidents immediately. If you have a system of staff, supplier, or contractor

on how your security may be improved 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	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 to be informed about? The direction set out in *Requirement 3c* can help you keep on top of this.

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.

Whilst implementing this policy, it is important to ensure people are provided

	all 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.*
4. Upon people moving role or termination, ensure that: a. Access privileges are revised/revoked in time to prevent unauthorised usage b. Leaving employees are debriefed on their post-employment confidentiality responsibilities	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 (*see Requirement 3bii*).

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	Guidance and tips for implementation
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	1. Policies need not each be in a separate document. A policy may cover multiple topics. 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 Requirement 6*), will depend on the practical actions you take to match your risk assessment. The IASME ICA Policies document provides a list of information security policies. Your risk assessment may suggest additional policies are relevant to your organisation that are not listed – the policies provided are offered as a baseline only.

	 *Template available:* IASME has a security template document, covering many of the topics in the ICA Policies document, that can be adapted for most organisations.
2. Policies must cover: 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 f. What happens if the policy is breached	This applies to each policy whether it covers only one, or multiple, areas. 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 *Theme 7 - People*. 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 Requirements 3 and 7 that cover how you should handle policy reviews. 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. f. Security incidents are inevitable. Be prepared with a business continuity element for every policy (further direction on this will be provided in *Theme 14 – Resilience: business continuity, incident management, and disaster recovery*). 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.
3. Each policy must be approved by someone in your organisation with the appropriate competency and authority. a. Document your policy review and approval process.	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. 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 (*see Requirement 1a)*.
4. Ensure your security policies can cope with potentially conflicting rules set by other relevant parties.	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.

	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 owner.
5. Policies must be distributed to all people responsible for implementing them.	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 training and this is particularly relevant where policies may not have been documented. 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.
6. Policy understanding. a. Policies must be supported with a suitable level of documentation which can be easily understood by the people who need to implement them.	a. 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. 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

b. 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.	provided all necessary content is covered with suitable clarity. The IASME ICA Policies document sets out which policies should be documented as a minimum. b. This is a strong initial indicator of whether policy is being followed and whether the person has been adequately trained to implement the policy.
7. Each policy must be reviewed and updated (if necessary): a. At least annually b. If a security incident occurs c. Changes in the risk landscape emerge 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	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.  *Important:* 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 plethora of nuances in which risk may realise. Policies should be based on your risk assessment and the practicalities of implementing corresponding countermeasures. 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 when.

	a. Your risk assessment may dictate more frequent reviews are required. Bring review dates forward as necessary. b. Did the policy support you as intended before, during, and after the incident? c. Does the policy still support the new context? 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. (*Further direction on changes will be provided in Theme 11 – Change Management and Theme 12 - Secure business operations: monitoring and review*)

Theme 9 - Managing Access

What is this theme about?	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: • 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
1. Provide people access to all the resources and data necessary for their roles, but no more. This applies to: a. Data stored on computer equipment b. Physical access to equipment and premises	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.

Whilst implementing this policy, it is equally important to ensure people are provided all resources they need. This allows them to fulfil their (security) responsibilities.

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:


Customer information


Databases


Information about staff, contractors, and suppliers


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. 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.
3. 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.
4. 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.

Theme 10 - Technical Intrusion

What is this theme about?	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: – 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 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?

What are the requirements for this theme?

Requirements	Guidance and tips for implementation

1. Detect unauthorised activity. Deploy technical tools including intrusion detection and prevention methods. Things to consider (based on business size) to appropriately detect unauthorised activities (in addition to physical security controls): • IPS / IDS in firewall technologies • Anti-malware • 2FA on cloud accounts (link with secure business ops) • M365 / Google / Amazon monitoring • EDR • SIEM / SOC Solutions	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. Note: detecting unauthorised activity also includes internal sources. Examples include • Staff accessing company data from personal devices without prior approval (see *Theme 3 - Assets*). • 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. (Further direction on monitoring and change management will be provided in *Theme 11 - Change management* and *Theme 12 – Secure Business Operations: Monitoring and Review*).
2. Review the security settings on all your technology periodically to ensure that they are adjusted for current threats.	This may include keeping your software up to date or adjusting firewall settings based on recognised or predicted threats, according to your risk assessment.

Theme 11 – Change Management

What is this theme about?	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.

What are the requirements for this theme?

Requirements	Guidance and tips for implementation
1. Set out a documented procedure for changes to working practices and technology. 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. i. Make sure that where personal devices (BYOD) are used for business, that suitable	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*. 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, updated.

protective measures are in place. b. Consider and manage the risks when decommissioning assets. 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. d. Ensure that your 'allow list' of approved applications that may be installed on your devices remains up to date.	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. 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: • *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 • *Theme 13 - Backup and restore* - 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 *Theme 14 – Resilience: business continuity, incident management, and disaster recovery*.

	b. As per *Theme 3 - Assets*, safe disposal methods may include secure erasure and shredding. c. 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 *Theme 10 – Technical intrusion* . d. As determined in *Theme 10 - Technical intrusion*, 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.

Theme 12 - Secure Business Operations: Monitoring and Review

What is this theme about?	Secure business operations means the carrying out of security activities in a 'business-as-usual' way. Consider: • 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?

What are the requirements for this theme?

Requirements	Guidance and tips for implementation
1. 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. a. Ensure that your monitoring systems are calibrated correctly.	Your policies should provide a strong indication of what needs monitoring, and how deviations or opportunities for improvement can be identified. 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*.

b. Make sure that personnel are aware of any monitoring that may take place.

c. Keep information which is forensically sound from a legal perspective.

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).

a. 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.

b.

Important:

Consider relevant legal requirements to inform personnel and the public of any monitoring taking place. Refer to, and update as necessary, your list 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.

f. Consider this alongside the access controls and role segregations defined in *Theme 7 - People* and *Theme 2 - Organisation*.

	 *Template available*: IASME can provide *keyholder tracker* and *administrator privilege tracker* templates that can be adapted for most organisations.
2. Protect access to your monitoring systems and preserve the records they produce according to a suitable retention schedule. 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.	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 investigations. 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. 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.
3. Scan your systems and network for vulnerabilities: a. At least every six months b. After introducing major changes	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

c. Following incidents where a vulnerability may have been exploited or created	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. a. Note that your risk assessment may dictate that more frequent reviews are required. b. Changing your systems or network configuration may introduce vulnerabilities. (*Further direction on change management will be given in Theme 11 - Change management*). 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. (*Further direction on incident response will be provided in Theme 14 – Resilience: Business continuity, incident management and disaster recovery*).
4. Extend your system and network scans to include penetration testing if deemed necessary by your risk assessment.	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.
5. Pay attention to warnings and reports from your monitoring, malware and technical intrusion controls, including vulnerability scans and any penetration testing,	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.

and take action. Review event logs (including errors and alerts) at least weekly.	(Further direction on monitoring will be provided in *Theme 12 - Secure business operations: monitoring and review*). 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. (Further direction on responding to incidents will be provided in *Theme 14 – Resilience: business continuity, incident management, and disaster recovery*). 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. 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 14 – Resilience: business continuity, incident management, and disaster recovery*.

Theme 13 - Backup and Restore

What is this theme about?	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. • 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
1. Make sure you have a backup of all information and an easy way to restore it to your systems if a problem occurs and 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.	You should keep three copies of your information: 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 – see Requirement 3) 3) A local back up for easy retrieval - but all tuned by the expectations of your risk assessment

a. Back up as necessary before implementing significant changes.	Consider whether any data is primarily paper-based and the respective capabilities to recover this if damaged or lost.  Important: 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 same level of resilience as a backup against cyber attacks such as ransomware. 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. 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 as a minimum.

	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.
2. 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. 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.
3. 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 assets.

4. 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 14 - Resilience: Business Continuity, Incident Management, and Disaster Recovery

What is this theme about?	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: • 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
1. Ensure breaches of confidentiality, integrity, or availability of your data are detected, recorded, and dealt with.	This includes either partial or total loss of key information assets. Following the direction set out in *Theme 12 - Secure business operations: monitoring and review* will assist you to detect incidents. 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

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. i. Make sure it's clear who is responsible for disclosing details of a data breach.	knowledge and skills. The aim of the investigation is always to reduce the impact of the incident and to prevent its reoccurrence. 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. a. You may have created this already whilst following the direction set out in *Theme 12 - Secure business operations: monitoring and review*. 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*.
2. Set out a communication policy which clearly defines: 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	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. 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

c. Who is – and is not – allowed to talk about incidents outside the business	people involved in it on relevant platforms.
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: a. Preserving any information which may be required from a legal standpoint or disciplinary action b. Relevant responsibilities for personnel and management c. Useful contact numbers for any internal and external services or authorities you may need to involve i. Include copies (or references) to licence and Service Level Agreements	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. 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.  *Template available*: IASME can provide a *Business Impact Assessment and Business Continuity and Disaster Recovery Plan* template that can be adapted for most organisations.

d. Strategic priority for asset recovery and how this can be achieved	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. b. This includes reporting and communication responsibilities. 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. 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. 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 register to guide your prioritisation. In addition to utilising the backups of your data created in line with *Theme 13 - Backup and restore*, 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.

4. 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.	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.
5. Exercise your plan at least annually and keep it up to date to account for changes to your business.	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.  *Important*: 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. 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.

6. Analyse your records for: a. Recurring incidents b. Your effectiveness in dealing with an incident c. The effectiveness of your risk assessment and business impact assessment	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?
7. Learn the lessons from the event(s) a. Use the information gathered to review and update your risk assessment, and your risk treatment plan. i. Review incidents with top-level management at strategic and tactical meetings. b. Review your information security policies accordingly.	View incidents as learning experiences. Use them to educate yourself and your staff, offering support through training where necessary. 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. 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.