IASME CYBER ASSURANCE

THE IASME CYBER ASSURANCE QUESTION SET BOOKLET

Version 12c

July 2022

Hartnell

INTRODUCTION

This booklet contains the question set for the IASME Cyber Assurance scheme (https://iasme.co.uk/iasme-cyber-assurance/)

The IASME Cyber Assurance standard

The Cyber Assurance standard is a formal information security methodology that is particularly accessible to SMEs but can be applied successfully to any organisation. It is sector agnostic and provides a working framework to assure information security against the background of contemporary threats.
The standard is designed to provide clear, simple to understand guidance to applicants and then to provide a high-quality, independent assessment of the level of maturity of an SME's information security.
Once assessed to the standard, applicants can use the certificate to assure customers/clients, supply chains and others that information stored and handled by the certified company is protected to a reasonable level for most practical purposes.

How to certify

In order to certify to IASME Cyber Assurance, you must first have certified your organisation to either Cyber Essentials (https://iasme.co.uk/cyber-essentials/) or IASME Cyber Baseline. You will need the certificate number when you apply.

The booklet is intended to help you to understand the IASME Cyber Assurance questions and take notes on the current setup in your organisation.

In order to complete the assessment, you must enter your answers via IASME's online assessment platform.

You must answer all questions in order to achieve certification.

Your answers must be approved by a Board level representative, business owner or the equivalent, otherwise certification cannot be awarded.

Need help?

If you need help with understanding the questions, get in contact with IASME on +44 (0)3300 882752 or email info@iasme.co.uk

Alternatively, IASME has a network of Certification Bodies who are skilled information assurance companies who can provide advice on the standards and who can help you make changes to your setup in order to achieve compliance. Visit the IASME website at www.iasme.co.uk to find your nearest Certification Body.

CERTIFYING TO IASME CYBER ASSURANCE

Thank you for choosing to certify to IASME Cyber Assurance.

IASME Cyber Assurance covers your whole organisation including all its technology and its risks, so this initial section asks you to provide some further context.

Further information on the IASME Cyber Assurance scope can be found in *Chapter 3* of the standard, available at https://iasme.co.uk/iasme-cyber-assurance/free-download-of-iasme-standard/

B1.1. Have you read 'The IASME Cyber Assurance standard' document, which details how the scheme operates and provides guidance on how to put the controls in place within your organisation?

The document provides guidance on the scheme and should be read before completing this question set and is available at https://iasme.co.uk/iasme-cyber-assurance/free-download-of-iasme-standard/

[Notes]

B1.2. Have you included all the devices that contain information within your organisation in the scope of this assessment?

The IASME Cyber Assurance scope requires you to include all devices that contain information within your organisation, including those that don't have an internet connection such as offline servers, air-gapped systems and production networks.

[Notes]

B1.3. Have you included any paper-based systems in the scope of this assessment?

The IASME Cyber Assurance scope requires you to apply information security controls to all information assets, including any non-electronic assets such as paper records and files.

[Notes]

B1.4. Does your organisation (or business unit) hold or process personal data subject to the EU or UK GDPR?

For most organisations in the UK and EU the answer to this question should be "Yes".

If you process personal data about residents of the European Economic Area (EEA) or the UK, you must comply with the EU/ UK GDPR wherever you are located in the world.

You can find details of the definition of personal data and legal requirements at your country's government data protection website (for example, in the UK, this is https://ico.org.uk/. In the Republic of Ireland this is https://www.dataprotection.ie/)

[Notes]

B1.5. Is this IASME Cyber Assurance application a renewal of an existing certification or is it the first time you have applied for certification for your organisation?

IASME Cyber Assurance certification requires annual renewal.

If you have previously achieved IASME Cyber Assurance, please select "Renewal". If you have not previously achieved IASME Cyber Assurance, please select "First Time Application".

[Notes]

B1.6. What is your main reason for applying for IASME Cyber Assurance certification?

Please let us know the main reason why you are applying for IASME Cyber Assurance certification.

If there are multiple reasons, please select the one that is most important to you. This helps us to understand how people are using our certifications.

[Notes]

B1.7. Do you already hold certification to Cyber Essentials or IASME Cyber Baseline that covers the scope of this assessment?

IASME Cyber Assurance certification requires you to achieve Cyber Essentials or IASME Cyber Baseline certification for your organisation to ensure you have basic technical cyber security in place.

[Notes]

B1.8. Please provide your certificate number for Cyber Essentials or IASME Cyber Baseline.

Your certification number will usually look like 'IASME-CE-xxxxxx' and can be found on your certificate or by searching on the IASME website https://iasme.co.uk/certified-organisations/

[Notes]

B1.9. Please state the organisation name shown on your certificate for Cyber Essentials or IASME Cyber Baseline.

Please provide the full name used when you applied for certification. This can be found on your certificate or by searching on the IASME website https://iasme.co.uk/certified-organisations/

[Notes]

ORGANISATION

In this section, we need you to tell us about how you manage security within your organisation. It is important that management is in control of security to achieve effective outcomes.

Please note, the standard is carefully designed to be applicable to small organisations, and as such, sole traders (one-person companies) and micro businesses must apply all the controls within the standard. For all questions below, involving staff and employees, there is a note in the guidance about how to apply the controls to a sole trader organisation.

In most cases, for a sole trader, the owner will take on all responsibilities, and will involve contractors or external providers, such to provide extra support and guidance on particular topics as needed.

B2.1. Please provide the name of the board member/director/partner/trustee who has accountability for information security and data protection?

This person must be a leader within your organisation who is fully accountable for information security and data protection. This person cannot be an employee of an outsourced IT provider. You can name multiple people if required.

For sole traders this will be the business owner.

[Notes]

B2.2. Is information security and data protection a standing agenda item for your board/director/partner/trustee meetings?

It is vital that the board/owners of the organisation are involved in information security and data protection. Security should be a standing agenda item at strategic and tactical meetings.

You must include a review of any recent incidents as part of the meetings.

Sole traders must set aside regular time to review security to meet this requirement.

[Notes]

B2.3. Please provide the name and role of the person who has overall responsibility for managing day-to-day security in your organisation.

This person must have day-to-day responsibility for operational security within your organisation. This person cannot be an employee of an outsourced IT provider. This may be the same person you provided for question B2.1 (particularly for micro businesses), but this will depend on who has the most appropriate technical skills in your organisation.

For sole traders this will be the business owner.

[Notes]

B2.4. Do you provide sufficient funding and a suitable number of appropriately skilled staff to ensure good information security and data protection? How do you achieve this?

To ensure that your organisation remains secure, you need to prioritise funding for security and data protection initiatives and ensure that you have suitable skills within the organisation.

For sole traders, provide details of how you have sufficient skills or if you use an external provider to help you with this.

[Notes]

B2.5. Do you have a person or group that has oversight of information security and data protection issues for your organisation?

Whilst the organisation's board/directors/partners/trustees maintain the overall responsibility for the risks surrounding information and data protection.

Smaller organisations and sole traders may only have an individual. For smaller organisations, this may be the same person you provided for question B2.3.

In larger organisations, you should delegate the day-to-day management of information security issues to a group of people from across departments.

[Notes]

SUPPLY CHAIN

Weaknesses in the security of your contractors, suppliers, partners, or customers may be exploited by cyber criminals, who are increasingly taking advantage of supplier relationships to reach valuable targets. Supply chains link many parties together and so security incidents can cascade from one organisation up or down the chain to others.

In this section, we need you to tell us about how your supply chain is structured and how you securely manage it.

Cloud Services

Many organisations use cloud services to store or share files between employees, contractors, suppliers, and customers. Cloud services include Office 365, Google Workspace, Dropbox, Slack, Salesforce, and Amazon Web Services (AWS).

B3.1. Do you use cloud providers to store company information (such as files, emails, data backups)? If so, please list all providers.

Most companies will use at least one cloud provider to store data which could include file storage such as Dropbox, emails using Office 365 or Google Workspace, and cloud backup providers. You should include all your cloud service providers in your list.

[Notes]

B3.2. Do you use cloud providers to share company information between employees or with customers (such as instant messaging or collaboration tools)? If so, please list all providers.

Cloud providers that you use to share information could include Slack, Yammer, Teams, Jira, Confluence and Basecamp.

[Notes]

B3.3. Where do your cloud providers store your data?

You should provide the geographical location or region (for example UK, USA, European Union, China) for all your cloud providers, using a list if needed.

[Notes]

B3.4. Please describe which provisions have been put in place to ensure that the requirements of your country's data protection legislation are met fully for the data held in your cloud services?

If you need to comply with UK/EU GDPR and your cloud provider stores your data outside of the European Economic Area (EEA) you will need to check that one of the following is in place:

- *An adequacy agreement which is recognised by your country's Supervisory Authority - information about this can usually be obtained from the cloud provider.*
- *You have implemented binding corporate rules where personal data is processed by another part of your organisation in a country outside of the EEA or one not covered by adequacy agreements.*
- *You have implemented the approved standard contract clauses between your company and another entity that is processing personal data outside of the EEA or a country covered by adequacy agreements.*

[Notes]

General

B3.5. Have you defined a set of security requirements that all your suppliers and contractors must meet, and have you ensured that your contracts with all your suppliers and contractors meet these requirements?
Please explain the requirements you have set and the reasons why you have chosen them.

The security requirements you define for your contractors and suppliers should be based on your risk assessment which will be influenced by your regulatory or business environment. For example, UK Ministry of Defence suppliers will be required to pass down certain security requirements to their supply chain. Contracts ensure there is a legal basis for your security requirements.

Overall, you should expect your contractors and suppliers to meet information security requirements that are at least equivalent to your own organisation for the data involved in that contract.

Certification is a good way to ensure your suppliers and contractors meet your requirements. You may wish to require suppliers to hold Cyber Essentials, IASME Cyber Assurance, ISO 27001, or another standard.

[Notes]

INFORMATION ASSET LIFECYCLE

Keeping your information safe relies on having a good understanding of your key information assets. The impact of any security incident will be most severe if it happens to the assets which keep the organisation going. Information assets need protecting throughout their lifecycle, from creation or acquisition through to safe disposal.

B4.1. Does your organisation have up-to-date asset registers, for both physical and information assets?

Your information assets may be physical, like a laptop, or intangible, such as a set of data you hold about your customers. You should include in your asset register any devices that hold your information, including those owned by staff if they are allowed to use them for business purposes.

For example, an information asset might be a set of data ("employee information") which will have a location attached to it ("the server in the HR department") and an owner (the "HR director") with a relative value ("confidential"). The server itself would also be recorded as an asset.

An asset register links closely to risk assessment by identifying the information assets that are to be protected.

IASME has a free information asset register template that can be used by applicants which can be found here : https://iasme.co.uk/iasme-cyber-assurance/helpful-templates/

[Notes]

B4.2. Do all assets have named owners?

Having a named owner for each asset ensures that someone is accountable for the activities required to keep it secure.

Asset owners will set the rules around data assets, such as classification, who can access them, and retention periods.

For sole traders, the business owner will be the owner of all assets.

[Notes]

B4.3. Does your asset register group assets into categories and also record the relative value for each asset?

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.

You need to know the relative value and impact of your information assets to your business so that you can apply adequate protection for them. For example, your customer contract details might be your most important asset and would cause the highest impact if lost or deleted.

[Notes]

B4.4. Is all sensitive information identified (e.g. by protective marking) and properly protected? Describe how this is done.

You must be able to identify all sensitive information within your company and make sure it is protected. One method to achieve this may be through protective marking, for example, where you use the relative values (such as public, confidential, secret) and mark this internally or externally on documents, emails, and spreadsheets. You don't have to use protective marking if you have other ways to keep sensitive information identified and protected.

[Notes]

B4.5. Is all personal data and special category data identified (e.g. by protective marking) and properly protected?

You need to be able to identify any personal data within your organisation to meet data protection requirements.

You should have a record of where all personal and special category data is held, the lawful purpose for holding that data, where the data is obtained from and any other organisations/individuals this data is shared with. You can record this in the data asset register.

This is important to ensure the rights of data subjects are upheld and will assist with meeting requirements such as Subject Access Requests.

[Notes]

B4.6. How does your asset register track the physical location of information assets?

You should be aware of where assets are located and if they are being moved around. If the asset is fixed (like a desktop computer), record the location. If the asset is mobile (like an iPad used in a van to track deliveries), record who uses it on a day-to-day basis and where it is typically used. It may also be possible to track portable assets through the use of mobile device management (MDM) software.

[Notes]

B4.7. How do you ensure all flows of personal and special category data are documented? This must include where data was obtained, where it is stored and all destinations of data.

You must be able to show how such data flows into and through your company. Using a diagram can be a useful way to achieve this requirement.

[Notes]

B4.8. Are all mobile assets (such as phones, tablets, and laptops) tracked in the asset register, pin/password protected and encrypted? Also, where available, have these devices been configured with a remote wipe capability? Please describe how you have achieved this for all criteria within this question.

This can be achieved using built-in tools (such as Find my iPhone, Find my Android) or additional mobile device management (MDM) software. Many mobile devices are encrypted by default (including iPhones and iPads).

Both inbuilt tools and MDM software usually have a 'remote wipe' feature that can allow you to delete data on the device in the event it is lost. You should enable this where it is available.

[Notes]

B4.9. Is all removable media tracked in the asset register and encrypted? Please describe how you achieve this.

Removable media includes USB sticks, USB hard drives, DVDs/CDs, and memory cards. It might also include backup tapes. You need a list of all removable media you use and need to manage, how it is used, where it is used and who uses it.

[Notes]

B4.10. Is your data encrypted before being passed between your systems and any cloud services you use (i.e. encrypted in transit)?

Your data should be encrypted when it is being sent between your devices and the cloud data centre, whether you are running your own cloud services or using a cloud service provider.

Most cloud services do this automatically by using the TLS protocol. For web-based services look for the https:// in the address bar and a padlock icon.

[Notes]

B4.11. Is your data encrypted whilst being stored on any cloud services you use (i.e. encrypted at rest)?

Your data should be encrypted when it is being stored in cloud services. It can be difficult to verify this just by looking at the cloud service - you will need to contact you cloud provider or view their security documentation to confirm this.

[Notes]

B4.12. Is all sensitive personal data encrypted?

Sensitive personal data can include, but is not restricted to, racial or ethnic origin, personal political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning a person's health, sex life, or sexual orientation.

[Notes]

B4.13. Do you review the data you hold on a regular basis 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 your risk assessment suggests, you may need to do more frequent reviews to ensure that the data you are collecting remains accurate.

Your retention policy should guide staff on how long each type of data should be kept.

[Notes]

B4.14. When assets are no longer required, is all data securely wiped or are the assets securely destroyed, and are they removed from the asset register? Describe how this is done.

Information assets may be physical devices such as laptops (including personal devices), servers, tablets, USB hard drives and USB sticks. Special software can be used to securely delete data or external companies can be used to provide a secure destruction service. Alternatively, you can physically destroy the device holding the data yourself. You must also consider how all versions of an asset are destroyed and whether they can still be restored from a backup copy.

[Notes]

LEGAL CONTEXT AND AWARENESS

Your organisation will have certain legally enforceable obligations associated with company registration, accounting, managing customers, use of technology, handling data, and other business processes. You will likely have other obligations that may be sector specific, or those relating to contractual or licensing agreements.

B5.1. List any business sector-specific regulations relating to risk treatment or information security which apply to your organisation.

Such regulations might include the Financial Conduct Authority rules for UK regulated businesses or the Network and Information Security (NIS) directive, if you are a European Operator of Essential Services.

More examples are provided in Theme 4 of the IASME Cyber Assurance standard document, which can be found here https://iasme.co.uk/iasme-cyber-assurance/free-download-of-iasme-standard/

[Notes]

B5.2. List any local or international laws relating to risk treatment or information security which apply to your organisation.

Such laws might include the UK Computer Misuse Act, data protection legislation, or local privacy laws.

More examples are provided in Theme 4 of the IASME Cyber Assurance standard document, which can be found here https://iasme.co.uk/iasme-cyber-assurance/free-download-of-iasme-standard/

[Notes]

RISK MANAGEMENT

You need to identify any threats to your organisation and assess the resulting risk. Your risk assessment helps you to choose the cyber security controls you will put into place. This will also be influenced by your organisation's risk appetite which will be guided by legal requirements and obligations to customers, partners, and other stakeholders such as data subjects.

B6.1. Do you have a current Risk Assessment covering information security risks to the information your organisation holds?

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.

You must include the risks presented to data subjects within your risk assessment, in line with data protection legislation.

IASME has a free risk assessment template that you can use available at https://iasme.co.uk/iasme-cyber-assurance/helpful-templates/

Appendix B of the IASME Cyber Assurance standard (which can be found here https://iasme.co.uk/iasme-cyber-assurance/free-download-of-iasme-standard/) provides examples of risks to consider.

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.

[Notes]

B6.2. Has your risk assessment been reviewed in the last 12 months? Who reviewed it?

You should ensure that sufficient knowledge of all areas of the organisation is included in the review. Involve a representative group of suitable people from across the organisation. In a micro business, the group will probably include the whole company.

You must also carry out a review following incidents, and in anticipation of changes.

For sole traders, the business owner will be the reviewer but may turn to an external provider or contractor for guidance.

[Notes]

B6.3. Does the risk assessment cover the scope of this assessment?

The risk assessment must cover the scope of your IASME Cyber Assurance assessment.

[Notes]

B6.4. Do you ensure that your organisation keeps up to date with emerging cyber threats and countermeasures, and feed this knowledge into your risk assessment process? Describe how this is done

Cyber threats and the things you can do to protect your organisation from them are constantly evolving. Many sources of information are available, ranging from free governmental guidance (the UK NCSC has useful guidance https://www.ncsc.gov.uk) to paid consultancy services. Anyone who has access to the data on your systems should be able to report vulnerabilities, incident, or make suggestions about how you may improve your security.

[Notes]

B6.5. Do you integrate your information security risk assessment with any other business risk assessments that you carry out? Describe how this is done

Some examples include environmental risk, operational risk, legal and regulatory risk, market risk, people risk, and health and safety risk.

[Notes]

B6.6. Does your risk assessment assign ownership of risks to a named owner?

Having a named owner for each risk ensures that someone is accountable for decisions relating to the risk. The responsibility for necessary actions such as those related to risk treatment can be delegated to other people as appropriate; the owner does not need to undertake all actions themselves, but they must approve any work completed by others.

For sole traders, the business owner will be the owner of all risks.

[Notes]

B6.7. Has your organisation set a level of acceptable risk (risk appetite)? Explain how you do this.

Understanding your risk appetite can help you decide whether you want to deal with each risk.

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 - this means you likely have a high-risk appetite and can accept many risks rather making changes to reduce them.

In some other industries, customers and investors may expect you to reduce all risks as much as possible and you will need to make many changes to the way you operate to reduce identified risks.

[Notes]

B6.8. Does your risk assessment identify the actions you will be taking for each risk (such as to reduce or accept) based on your organisation's risk appetite?

You need to make a decision for each risk you identify regarding what you intend to do about it.

You must take into account factors such as practicality of the actions taken and the corresponding policies which need to be implemented.

[Notes]

B6.9. Do you have an action plan to implement any actions identified in the risk assessment and does it include specific dates for delivery?

An action plan lets you prioritise the changes that are needed to manage the risks identified in your risk assessment and makes sure your organisation carries out any changes needed.

[Notes]

B6.10. Was the risk assessment and action plan approved at board/director/partner/trustee level?

Your risk assessment must be signed off and the person who signs off must agree to accept the risks that will remain after your action plan is implemented.

For sole traders, the business owner will sign off the assessment and action plan.

[Notes]

SECURITY POLICY

You must put into place information security policies which are aligned with your risk assessment.

Appendix C in the IASME Cyber Assurance standard lists the minimum set of security policies your organisation should have.

Micro businesses or sole traders are likely to have a much simpler and shorter set of policies than a larger organisation. There is no need to make policies overly long or complex.

Guidance on this is available in Theme 8 – Policy realisation in the Standard which can be downloaded from https://iasme.co.uk/iasme-cyber-assurance/free-download-of-iasme-standard/

IASME offers a suite of security templates including a basic security policy at https://iasme.co.uk/iasme-cyber-assurance/helpful-templates/ that can be adapted to the individual circumstances of most organisations.

B7.1. Do you have a policy or a set of policies that cover information security?

A security policy can be a stand-alone document, or it can be formed from a number of policies within your policy set, but it should set out your commitment and objectives for managing your security.

[Notes]

B7.2. Do your information security policies cover the scope of this assessment?

The policies must apply to the whole organisation covered by this assessment.

[Notes]

B7.3. Do your policies (whether documented or undocumented) cover all of the policy topics and areas within *Appendix C* of the IASME Cyber Assurance standard? If there are any policies that are not applicable to your organisation, please list them and briefly explain why.

The IASME Cyber Assurance standard is available here: https://iasme.co.uk/iasme-cyber-assurance/free-download-of-iasme-standard/

Your policies may group topics differently to the list to address the needs of your organisation, but you should cover all the policy topics unless there is a good reason why they are not applicable to your organisation.

[Notes]

B7.4. Have you documented all the policies marked as 'Explicit' within *Appendix C* of the IASME Cyber Assurance standard?

Documented policies can crucially support business continuity, provide assurance to suppliers, customers, and auditors, and additionally help to clarify any misunderstandings. As a minimum, you should document the policies marked as 'explicit' in the table included in Appendix C.

Micro businesses or sole traders are likely to have a much simpler and shorter set of policies than a larger organisation. There is no need to make policies overly long or complex, but you must document all policies required.

[Notes]

B7.5. Do your policies cover all of the topics in the following list?

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

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.

[Notes]

B7.6. Do your policies and procedures set clear responsibilities for implementation?

The people that the policies apply to should clearly understand their responsibilities. Include references to key roles such as the person in charge of security training or data protection. They will play a key part in making other people aware of their responsibilities.

[Notes]

B7.7. Are your information security and data protection policies distributed to all people responsible for implementing them, required to be followed in everyday practice and linked to disciplinary procedures? How do you achieve this?

People can only be expected to follow a policy if they have been made aware of it; this aligns with the necessity to provide adequate personnel training and 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.

For sole traders who use contractors, you will need to share policies with your contractors.

[Notes]

B7.8. Is there a documented policy review, consultation, and approval process?

Policies must be reviewed and if necessary updated at least annually. You should also review the policies if a security incident occurs, changes in the risk landscape emerge, or if monitoring reveals that the policy is no longer working for the business.

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. The approval process should consider the impacts to all areas of the organisations and any external stakeholders, such as contractors, customers, and suppliers, before signoff.

For sole traders, the business owner needs to review the policies and signoff.

[Notes]

B7.9. Do you keep a log of historical policies?

You should keep historical copies of policies so you have a record of what applied and when. This includes policies and terms and conditions provided to customers and data subjects, which form part of your business records.

[Notes]

B7.10. Have your policies been reviewed in the last 12 months?

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, if you have one.

For sole traders, you may wish to involve an external provider or contractor to help you with the review.

[Notes]

B7.11. Provide the name and role of the person who approved the policies?

This person must be a leader within your organisation. You can name multiple people if required.

For sole traders, this will be the business owner.

[Notes]

LEGAL COMPLIANCE

You will have legal obligations that are relevant to your business. These should be reflected in your policy design and implementation. This section highlights key compliance topics to verify that you have put the relevant steps in place, with particular reference to data protection legislation.

Payment systems

B8.1. Do you store credit card information?

Credit card information includes card numbers (PANs), expiry dates and personal details relating to cardholders

[Notes]

B8.2. If yes to above, are the systems that you use to store credit card information compliant to Payment Card Industry Data Standard (PCI-DSS)?

Most organisations that handle credit card information will be required to comply to PCI-DSS requirements (see https://www.pcisecuritystandards.org)

[Notes]

Privacy regulations

Your country will have a 'Supervisory Authority' (or other data protection authority) that will provide guidance on how to comply with your country's data protection. For example, in the UK, this is https://ico.org.uk/ ; in the Republic of Ireland, this is https://www.dataprotection.ie/ .

You may need to consult the guidance provided by your local authority when answering the following 'Privacy Regulations' compliance questions.

Privacy regulations - roles

B8.3. Do you fall into the category of requiring a Data Protection Officer?

Your country's Data Protection legislation may require you to appoint a data protection officer if you are a public authority or body, or if you carry out certain types of processing activities

[Notes]

B8.4. If you are required to appoint a Data Protection Officer, have you appointed one?

Your country's Data Protection legislation may require you to appoint a data protection officer if you are a public authority or body, or if you carry out certain types of processing activities.

[Notes]

B8.5. If you are not required to appoint a Data Protection Officer, have you recorded the decision?

If you are not required to appoint a Data Protection Officer, the reasons why should be recorded in company records.

[Notes]

B8.6. If you are not required to appoint a Data Protection Officer, have you appointed a suitably qualified person in the organisation to manage data protection matters on a day-to-day basis?

This does not have to be a full-time role, but the person appointed should have a level of knowledge of data protection law, and knowledge of the business to function appropriately.

For sole traders, this could be the business owner or a contractor.

[Notes]

B8.7. To whom does the Data Protection Officer or person managing data protection report in your organisation?

The Data Protection Officer or person managing data protection should report to the highest possible level within the business and their reporting lines should not present any conflicts of interest.

For sole traders, this must be to the business owner.

[Notes]

Privacy regulations - data collection

B8.8. For each piece of personal information and special category data you hold, do you record the justification for obtaining it? Where is this recorded?

Justifications for obtaining the information might include explicit consent, contract fulfilment, performing a public function, meeting a legal requirement, or another legitimate interest. Justifications for obtaining special category (or sensitive personal data) could include specific consent, use for employment purposes, or to meet a medical need. Ideally this would be recorded in the Asset Register.

[Notes]

B8.9. For each piece of personal information you hold, do you record whether your organisation is the data processor or the data controller?

The roles of data processor are different to those of data controller and carry different responsibilities. Controllers make the decisions, whether solely or jointly, about the purposes and means for processing data. Processors act on behalf of relevant controllers, according to instructions provided.

[Notes]

B8.10. Where you have decided to hold data under the lawful purpose of Legitimate Interest of the Controller or Third Party, have you completed the three-part Legitimate Interest test and kept a record of the results?

The test is used to verify that you can successfully use legitimate interest as a reason to hold data.

Whilst the three-part test may not be mandated, it is strongly recommended that it is done, and records retained.

[Notes]

Privacy regulations - privacy statement

B8.11. Do you have a privacy statement?

A data privacy statement is an important document that sets out the justifications for your use of personal data. It should be made available to data subjects, often by hosting it on a company website.

[Notes]

B8.12. In your privacy statement, do you clearly state what the data is being collected for, how it will be processed, and who will process it?

You must state why you are collecting personal data clearly at the point of collection.

[Notes]

B8.13. Do you make it clear in both your privacy statement and other customer facing information how customers contact your business to make complaints or exercise their rights as an individual?

Please provide the name and role of the person who is listed to customers as the point of contact.

Under data protection legislation, individuals have rights over the use of their data. It is important that the process that can be used to exercise these rights is clearly communicated to clients and other data subjects.

[Notes]

B8.14. Do you review your privacy statement regularly to ensure it remains relevant with your processing activities?

Like your other information security policies, your privacy statement must be reviewed, and if necessary updated, at least annually if a security incident occurs, changes in the risk landscape emerge, or if monitoring reveals that the policy is no longer working for the business and/ or a credible opportunity to improve your security posture is identified.

[Notes]

Privacy regulations - consent

B8.15. Where you are holding data based upon the consent of the data subject, how do you record details of the consent?

You must record consent clearly so that you can track it and can refer to it later as needed.

[Notes]

B8.16. Where you collect data from children, do you actively seek parental consent? How do you record this?

You must record consent clearly so that you can track it and can refer to it later as needed. The age of consent will be determined by your country's data protection legislation. For example, the definition of children in the UK is up to 14 years of age, in Belgium it is 13.

[Notes]

B8.17. How do you facilitate data subjects revoking their consent?

In order to respect the rights of data subjects, it is necessary to have clear mechanisms for revoking consent for data processing when a subject requests it.

[Notes]

B8.18. What are your processes for ensuring you meet the rights of the individual?

Under data protection legislation, individuals have a number of rights. You need to ensure that you have processes in place to manage the rights that are relevant to your business, including meeting any deadlines that are applicable.

[Notes]

Privacy regulations - supply chain

B8.19. Do you have Data Processing Agreements in place with all contractors and suppliers that process personal data on your behalf?

Such agreements set out the requirements for data security for a contractor or supplier and ensure that these requirements are clear.

[Notes]

B8.20. In each contract you hold with contractors, suppliers, and customers, involving the processing of personal data, do you confirm whether you are the data controller or data processor?

The roles of data processor are different to those of data controller and carry different responsibilities. Controllers make the decisions, whether solely or jointly, about the purposes and means for processing data. Processors act on behalf of relevant controllers, according to instructions provided. It is important that contractors, suppliers and customers understand your role in each relationship.

[Notes]

B8.21. Where you disclose personal data to a supplier/provider, does the contract explicitly impose the obligation to maintain appropriate technical and organisational measures, to protect personal data in line with relevant legislation?

It is important that contracts make clear your security expectations in relation to personal data.

[Notes]

B8.22. Where data is not stored in the UK, EEA, or a country not covered by an adequacy decision, have you ensured that there are protections in place to protect that data? How do you achieve this?

Such data may be covered by an adequacy agreement recognised by your country's supervisory authority, for example, in the UK this is the ICO. Alternatively, a business can use standard contract clauses for business-to-business transfers or binding corporate rules for intercompany transfers.

[Notes]

General legal compliance

B8.23. Do you ensure that all your business processes provide sufficient support to fulfil your legal obligations?

Your policies and processes should be supportive of all your business objectives, including meeting legal requirements.

[Notes]

B8.24. Do you monitor the performance of your business processes, identify any non-compliances, and make improvements where needed?

Monitoring these can allow you to correct non-conformances, or take opportunities to improve your security posture, beyond only reducing risk to the threshold you deem acceptable. This may be through collecting feedback from people involved with, or impacted by, your business processes, such as employees, customers, or data subjects. Using a questionnaire may be one way to achieve this but consider the responsibilities and risks for any data that you collect.

[Notes]

PEOPLE

People are your greatest allies in protecting your organisation's information. They can also present a risk because they have privileged access to information. It is important therefore to ensure you carefully review who you employ. It is essential that new employees are given a briefing on their security responsibilities upon employment. Employee contracts should also include security obligations and reminders should take place at regular intervals. Employees with special responsibility for security, or with privileged access to business systems should be adequately trained/qualified as appropriate. On termination of employment, access privileges should be withdrawn in time to prevent unauthorised usage and the employee de-briefed on their post-employment confidentiality responsibilities.

Sole traders do not have employees but may work with contractors who fall into scope of this section.

B9.1. Do you verify that anyone who has access to your data is suitable from a security viewpoint, before access is granted to systems, and on a regular basis thereafter? How do you achieve this?

You should carry out checks when employing staff or contractors to verify their identity and whether they are suitable for the role. Background checks including references and screening may be necessary for some roles. You should review suitability on an on-going basis.

Sole traders will not have employees but may have contractors with such access. Please provide details in your answer.

[Notes]

B9.2. Where criminal record checks are carried out, do you ensure that explicit consent has been obtained from employees and that such checks are carried out for the correct lawful purposes?

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

Sole traders can answer 'No' to this question.

[Notes]

B9.3. Do you spread responsibility for important processes across multiple people to reduce the risk of fraud?

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.

Sole traders will not have employees but may have contractors with such responsibilities.

[Notes]

B9.4. Do you ensure that people are only given access to the systems and data that they need in order to carry out their responsibilities? How do you achieve this?

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 equally important to ensure people are provided all resources they need.

In a micro business, it is common that staff will need access to almost all of the businesses information in order to carry out their responsibilities. This is acceptable but will need to change as the business grows larger and roles become more specialised.

Sole traders will not have employees but may have contractors with such access. Please provide details in your answer.

[Notes]

B9.5. Do staff and contractor contracts include security obligations (to comply with your security policies as a minimum) and are reminders given at regular intervals?

Contracts ensure there is a legal basis for your security requirements, such as complying with your security policies and leaving intellectual property with the business. If you use an appraisal system, security objectives and reminders should be included.

Sole traders will not have employees but may have contractors.

[Notes]

B9.6. Do you give new staff and contractors a briefing on their security responsibilities before, or immediately after employment? How do you achieve this?

You must brief staff and contractors on their security responsibilities, and you must provide a copy of relevant policies. By providing literature such as a copy of the relevant policies or a reference sheet, staff can remind themselves of your requirements at a later date.

Sole traders will not have employees but may have contractors. Please provide details in your answer.

[Notes]

B9.7. Are staff and contractors with specific responsibility for information security, or with privileged access to business systems, appropriately qualified and suitably trained? How do you achieve this?

It is important that those who hold security roles or have access to important data are skilled and trained so that they are less likely to make mistakes. Qualifications do not need to be formal and may be replaced by setting requirements on experience in a particular sector.

Sole traders will not have employees but may have contractors. Please provide details in your answer.

[Notes]

B9.8. Do all staff and contractors receive regular information security and data protection training (at least annually) and maintain awareness of current threats? Describe how this is done.

Appropriate training ensures all staff and contractors understand how to act securely when handling company data. Training could be in-person, online, or carried out remotely. Personnel should also be notified of any relevant changes and receive transition training if necessary.

You may need to train some contractors directly. For other suppliers, you will need to contractually require corresponding security requirements. Your risk assessment should guide you on how to manage training for everyone who has access to your information assets.

Sole traders will not have employees but may have contractors. Please provide details in your answer.

[Notes]

B9.9. Do you verify understanding for all training sessions and keep appropriate records to track that everyone has received the training necessary for their role?

It is good practice to keep a record of who is attending training. Keeping details of any test scores or other performance indicators, particularly for informal training sessions, will enable you to understand the effectiveness of your training and whether knowledge is improving. One performance indicator may be whether someone is able to give a short, clear description of a policy that they are responsible for implementing, though there are many others that may be relevant.

[Notes]

B9.10. Do you allow trainees to provide feedback on the training they receive?

Getting feedback from people receiving training can give insight into its effectiveness and identify areas for improvement.

[Notes]

B9.11. Provide the name and role of the person responsible for security and data protection training and awareness.

This person must have day-to-day responsibility for training within your organisation.

For sole traders, this person will be the business owner.

[Notes]

B9.12. On termination of contracts or when roles and responsibilities are changed, do you withdraw access privileges and brief departing staff on their confidentiality responsibilities? How do you do this?

It is important that you remove unnecessary access to systems when roles are changed or employment is terminated. Depending on the circumstances surrounding termination, you may choose to remove access immediately and not require employees to complete their notice period. Where relevant, your debriefing should include a reminder to leave any intellectual property with the business unless another explicit arrangement exists.

Sole traders will not have employees but may have contractors. Please provide details in your answer.

[Notes]

PHYSICAL AND ENVIRONMENTAL PROTECTION

Protection of your information and cyber security extends to the physical protection of information assets, to prevent theft, loss, or damage and their impact on the availability of your business information and associated resources. Usually this is no more than the common-sense approach to door locks, window bars, and video surveillance and so on, as dictated by the organisation's physical environment. However, in some cases, physical protection may be dictated by governmental or legal requirements. If your equipment requires any particular working conditions – such as heating, ventilation, or air conditioning (HVAC) – be careful to maintain these within the guidelines set out by the respective manufacturers.

B10.1. Do all business premises in scope have effective physical protection which has been determined by a risk assessment? How do you achieve this?

You should carry out a physical risk assessment which considers relevant factors, including any physical security requirements dictated by law or third parties. Risk treatments include locks, barriers, access control, surveillance, monitoring, and environmental controls such as heating and cooling. It could also include procedural controls such as locking away confidential information when it isn't in use, using privacy screens, and keeping confidential discussions to physically secure areas.

[Notes]

B10.2. Are only authorised personnel who have a justified and approved business case given access to restricted areas containing information systems or stored data? How do you achieve this?

You must ensure that access to systems is only provided to people who have a legitimate need to access these systems. This means you must restrict any other people from accessing such systems using locks, alarms, security cages, or any other form of physical access control.

[Notes]

B10.3. When you deploy wireless and wired networks, do you ensure that access is restricted only to authorised users?

If you use wireless networks, you must ensure that good wireless security (such as WPA2 AES or WPA3) is enabled so that only authorised devices are able to access your network. If you use a wired network, you must at a minimum, ensure that access to network sockets is only provided in locations you control or use network access control technology.

[Notes]

B10.4. Where indicated as necessary in your risk assessment, is the use of physical media on your systems controlled either by physical access restrictions or by a technical solution (such as by configuring devices to block USB storage)?

You can restrict access to USB devices and removable storage through Windows Group Policy or through third-party tools such as Sophos Cloud. For servers, you may choose to restrict access to the device, to only trusted individuals.

[Notes]

B10.5. Where indicated as necessary in your risk assessment, do you have dedicated machines to scan physical media for viruses and malware?

If your risk assessment identifies a particular risk from removable media, you may choose to dedicate computers to scanning incoming USB keys, drives and disks for viruses before allowing them to be used with your day-to-day systems.

[Notes]

B10.6. Are devices which require particular working conditions (such as heating and cooling) provided with a suitable environment within the guidelines set out by their respective manufacturers? How do you achieve this?

For example, servers and networking equipment may need air conditioning to ensure they keep to a reliable operating temperature. Your risk assessment will tell you what monitoring, and redundancy are expected from these measures.

[Notes]

B10.7. Do you ensure that relevant physical security controls are applied to people travelling and working from home? How do you achieve this?

You can achieve this by a combination of training, good policies, and practical processes to ensure the risks of home working and travelling are covered. Your policy should state what to do when other third-party 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.

For sole traders, consider how you apply controls to your own equipment and those of contractors when travelling.

[Notes]

PREVENTING INTRUSION

Devices containing your data are susceptible to in-person or remote unauthorised access. The security state of technology is dynamic and new ways to take advantage of vulnerabilities are frequently emerging. Therefore, detecting intrusion requires proactively identifying vulnerabilities and taking steps to address them. Staff negligence or mistakes can also expose your information systems to attack.

B11.1. Do you ensure that user accounts and devices do not remain signed-in indefinitely? How do you achieve this?

If devices or accounts remained signed-in whilst not in use, they are vulnerable to exploitation, as no authentication method, such as a password, is needed to access the system or data. Most devices, such as phones and computers, support automatic screen locking after a period of inactivity; many application/system accounts can be configured to do this. The maximum inactivity time allowed before automatic locking occurs should be based on your risk assessment.

[Notes]

Vulnerability Scanning

A vulnerability scan is a technical audit of the security status of your IT system. It can be performed by an expert or by automatic tools and can help you answer and provide evidence for some of the following questions. Some scanning tools are available for free to use via the internet. Common tools include Nessus, OpenVAS, Nmap, Qualys, Network Detective, SAINT, and Tripwire. A penetration test is a more in-depth test of the security of your systems where experts attempt to gain access by exploiting vulnerabilities.

B11.2. Do you carry out regular vulnerability scans on all your systems at least every 6 months, after incidents, after major changes, or more frequently based on your risk assessment? How do you achieve this?

You should carry out a regular vulnerability scan of your systems and network. Common tools which are free or low cost for SMEs including OpenVAS, Nessus, or Qualys can be used for this task. IASME Certification Bodies also offer this service.

[Notes]

B11.3. Where identified as necessary in your risk assessment, when was the last time you had a penetration test carried out on your critical business systems?

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 are often carried out after major system upgrades or changes.

[Notes]

B11.4. How did you act to improve the security of your system on the basis of the vulnerability scan (and penetration test) results?

It is important to address any issues identified as a result of the technical testing. You should make any changes in line with your usual change management processes and feed the learnings from the testing into your risk management process.

[Notes]

System segregation

B11.5. Do you set up your devices and software according to the principle of least privilege, where this capability is available? How do you achieve this?

Some operating systems have introduced free features to manage this requirement. Consider whether an application needs to access data in other applications on the device and peripherals such as cameras and sensors. For example, applications listed in mobile app stores will list the default permissions they have to access and modify other apps on your phone.

Other methods may include using a 'sandbox' – a virtual, isolated container on your device - can also be used to segregate and manage the access one application has to another. You may already use sandboxes to fulfil the Cyber Essentials malware requirements.

[Notes]

B11.6. Where identified as necessary in your risk assessment, have you segregated critical business systems and applied appropriate network security controls to them? Explain how this has been achieved.

If you run important business systems such as web servers containing client information, you may decide to segregate them from your main network in order to improve security. The decision to do this will be based on the risks you identified in your risk assessment process.

[Notes]

B11.7. Do you use firewalls or other technology to block and monitor access to malicious internet locations/domains at the boundary of your networks?

For example, to achieve this you could use a filtered DNS service such as (Quad9 or OpenDNS) or a firewall with rules blocking access to a list of suspicious URLs. Your risk assessment may recommend using additional intrusion detection technology to support this.

[Notes]

BACKUP AND RESTORE

Important information should be backed up regularly and kept in a secure location away from the working copy. Restores should be tested regularly in order to test the performance of the backup regime.

B12.1. Do you ensure all your information is backed up regularly (at least weekly and before any major changes), and do you test regularly whether you can successfully restore your information (at least monthly)?

Usage of a cloud system does not guarantee that there is a backup mechanism in place. Often cloud systems will replicate data loss or malware into the 'backup' copies. 'Replication' is a form of resilience offered by some providers that is useful but is not a backup. You must have a backup in addition to any replication. You should verify with your cloud-provider(s) that segregated off-site backups are available, or make provisions for an alternative backup solution that meets the requirements set out in this section.

You must ensure that a copy of all important data is made at least weekly and before any major changes - in line with your risk assessment. Some organisations will use a cloud backup, whereas others will rely on the use of encrypted USB drives or tape drives. You must also regularly try to access the copy of the data to ensure that it is valid and that you would be able to access it if needed. You don't need to restore the whole data set, just a selection of files to ensure accessibility - this process could be automated.

[Notes]

B12.2. Are each of your backups segregated and protected from being unintentionally overwritten or deleted? How do you achieve this?

Backups must be segregated from the main working copy, to prevent incidents spreading from your original system into the backup. Additionally, backups need protecting 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 affected by malware, the backup copy stored in the cloud is not also impacted.

This may be achieved by disconnecting cloud backups 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 the multiple backups are segregated and not all connected simultaneously to your main system.

[Notes]

B12.3. How do you ensure all backups are secured with an appropriate level of protection that reflects the classification of the data they hold?

Your backups contain your sensitive company data and must be protected with the same amount of effort as the main version of the data. This will be based on the relative value classification that you have assigned. Backups should be stored securely and if necessary, encrypted.

[Notes]

B12.4. Is a backup copy held in a different physical location to the original?

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.

[Notes]

MONITORING

Monitoring can help identify suspicious activity on your systems. Know which business systems and processes you need to track and monitor for acceptable activity – according to the information safety policies that you have set - and how you will identify any unacceptable aspects and/or where you can improve your security.

B13.1. Do you keep an eye on who is trying to access your information and where they are trying to access it from? Describe how you achieve this.

This should cover both authorised and unauthorised access.

You should maintain an audit trail of system access and/or data use by anyone who has access to your data for all relevant systems. You should review this on a regular basis (at least weekly).

Often your firewalls include features to assist you with detecting unauthorised activity. Your risk assessment may indicate that further necessary measures include implementing tools and appliances for intrusion detection, data loss prevention, and honey pots or traps to distract attackers.

You should also detect activity from internal sources such as staff accessing company data from personal devices without prior approval, personnel using accounts that should have been deactivated due to responsibility changes or termination, or attempts to access systems or segregated sections of networks holding data that is not required for that respective role. You can use an automated system to help you with this.

IASME's Certification Bodies can provide guidance on a suitable solution for your organisation.

[Notes]

B13.2. Do you make sure that staff and contractors are aware of any monitoring taking place?

You should make people aware of any monitoring you are conducting and also ensure that you comply with any relevant legal requirements.

For sole traders, this requirement is applicable to you and to any contractors that you might use.

[Notes]

B13.3. Do you ensure all your monitoring systems are calibrated correctly?

This can include making sure that devices have their time set accurately to ensure that logs and audit trails are in sync with each other. You can usually achieve this by changing the date/time preferences to enable automatic or internet time. System calibration can also include actions such as making sure that any CCTV cameras record adequate quality for playback and time analysis and are suitably positioned.

[Notes]

B13.4. Do you ensure that any event logs and audit trails are kept securely, retained for a suitable period, are forensically sound and do not expose sensitive information to unauthorised users?

You should aim 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 investigation. Ensure that any logs are stored in a safe location and are collected and managed appropriately so that they are deemed legally acceptable as evidence. Additionally, make sure that error messages do not return sensitive information to external or internal users. 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.

[Notes]

B13.5. Does your organisation review warnings and reports generated by your systems at least weekly, and take action to address any issues identified? How do you achieve this?

If you use an automated system to monitor events and flag up suspicious activity, then that is acceptable and you should answer 'yes' to the first part of this question, provided appropriate action is taken after alerts.

[Notes]

B13.6. Do you periodically review the security settings on all your systems to ensure they are adjusted for current threats?

This may include keeping your software up to date and adjusting firewall settings based on recognised or predicted threats, as recorded in your risk assessment.

[Notes]

CHANGE MANAGEMENT

Your organisation needs to ensure that management of computers, networks and devices is carried out in a controlled manner to ensure that changes to configuration are only implemented with authorisation. This ensures your security environment remains appropriate for the organisation.

B14.1. Do you ensure that all changes to information systems, applications, and networks are reviewed and approved, and that users are not allowed to make changes without approval? Describe the approval process.

Changes to systems should be approved by a suitable person with a decision-making role in the business. Users should not be able to make changes without approval, but they should be able to seek approval for changes easily. 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.

For sole traders, please provide details of how you apply this requirement to any contractors. If you don't have contractors, please note this in your answer.

[Notes]

B14.2. Do you ensure that all new and modified information systems, applications, and networks are correctly sized, comply with security requirements, are compatible with existing systems and are approved before they commence operation? Describe how you achieve this.

You must incorporate security provisions into your decision making about new and modified systems, including where personal devices (BYOD) are involved. You can achieve this by having a review process for all new and modified systems which involves both technical, security, and operational staff. The process should include consideration of the risks of decommissioning assets.

[Notes]

B14.3. Are all computers and servers provisioned only with approved software from a list of authorised applications that you maintain? Explain how you achieve this.

You should maintain a list of software that is used within the organisation and ensure that only software from this approved list is installed on your devices. You may not need a technical solution to achieve this, it could be based on good policy and procedure as well as regular training for staff.

[Notes]

B14.4. Do you ensure that a Data Protection Impact Assessment (DPIA) is carried out prior to the implementation of new systems and projects?

New systems and projects can present additional risks to the rights of data subjects. A DPIA can help highlight those risks and lead to an action plan for addressing them.

[Notes]

B14.5. If, after assessing all the risks in the DPIA, there is a high-level risk left, do you have processes for reporting this to your country's data protection office?

Any significant risks that remain after the DPIA should be notified to your country's data protection office (ICO in the UK, Data Protection Commission in the Republic of Ireland).

[Notes]

BUSINESS CONTINUITY

Plans for recovery and continuity should be drawn up and reviewed regularly. They should be tested in whole or in part so that participants in the plan understand their responsibilities. The aim is for the organisation to keep working through, and recover from, the effects of deliberate attack, accidental damage, and natural disasters.

B15.1. Do you ensure that business impact assessments, business continuity and disaster recovery plans are produced for your critical information assets, applications, and networks?

A business impact assessment assesses the risk of a critical function being disrupted and outlines the actions to be taken to restore the function.

Your business continuity and disaster recovery plan must cover:

- *Preserving any information which may be required from a legal standpoint or disciplinary action*
- *Relevant responsibilities for personnel and management*
- *Useful contact numbers for any internal and external services you may need to involve*
- *Copies (or references) to licence and Service Level Agreements*
- *Strategic priority for asset recovery and how this can be achieved*

IASME has a free template that you can use available at https://iasme.co.uk/iasme-cyber-assurance/helpful-templates/

[Notes]

B15.2. Do you review the business continuity and disaster recovery plans at least once per year? Who is involved in the review?

You should ensure that sufficient knowledge of all areas of the organisation is included in the review. Involve a proportionate and representative group of suitable people as necessary. Representation must be made from the board/director/partner/trustee level. For a micro business, you may need to involve all staff in the review.

For sole traders, the business owner must carry out the review involving external providers or contractors as needed to provide guidance.

[Notes]

B15.3. Do you test your business continuity and disaster recovery plans at least once per year by running a simulation exercise and ensure that the plans are kept up to date with any changes in the business?

You should test your plans by at least running a table-top exercise with a plausible scenario where you test how the plans would operate in an incident, for example, if a staff member accidentally emails data to a client.

The exercise does not need to be complex and could be run as part of a regular management meeting or away-day.

The UK's NCSC has produced a useful tool to help plan an exercise which is available here https://www.ncsc.gov.uk/information/exercise-in-a-box

You should make sure that your plans are kept up to date to reflect the current state of the business.

Your risk assessment may indicate that you need to carry out tests more often. You can also treat any real incident as a test of the process and feed any lessons learnt into the plan.

[Notes]

B15.4. Have your business continuity and disaster recovery plans been approved and signed off by someone who is authorised to make decisions for your organisation?

This may be a director, board member, partner, trustee.

This could be the person who has responsibility for information security that you provided in question B2.1.

For sole traders, this must be the business owner.

[Notes]

INCIDENT MANAGEMENT

You should have security incident management procedures to allow any incidents (such as loss of data, malware infections and phishing attacks) to be dealt with successfully. It is important that incidents are easy to report to a responsible entity without blame, and that the organisation learns the lessons from incidents.

B16.1. Are all information security incidents or suspected weaknesses reported and recorded, and do you provide a method for anyone to report security incidents without risk of recrimination?

You must provide a route for anyone who has access to your information systems to report any security weaknesses they encounter - including staff acting incorrectly and configuration issues. It is important that people can do this either anonymously or in a way that makes it clear there is no risk of negative consequences to them for highlighting an issue.

[Notes]

B16.2. Are users who install software or other active code on the organisation's systems without permission subject to disciplinary action?

Users who take risks and install software without permission must be subject to your disciplinary procedure.

For sole traders, this requirement should apply to any contractors that you use.

[Notes]

B16.3. Do you formally investigate information security incidents to establish their cause and their impact?

You should investigate incidents to identify the cause, repair the damage, and prevent the incident reoccurring. Investigate the incident and ensure the people involved have sufficient knowledge and skills. The aim of the investigation is always to reduce the impact of the incident and to prevent its reoccurrence.

Involve a proportionately sized group of people to achieve this, as necessary. You can use an external company to provide this service to you if needed. The aim of the investigation is always to reduce the impact of the incident and to prevent its reoccurrence.

[Notes]

B16.4. Do all staff, contractors, suppliers involved with incident management have clear roles and responsibilities and have they all received appropriate training?

It is important that people involved in investigating incidents have the knowledge and skills required so that their involvement assists and does not worsen the impact of any incidents.

You may need to train some contractors directly. For other suppliers, you will need to verify that they have the necessary competencies.

For sole traders, you will need to ensure that the business owner has sufficient training or involve an external provider as needed.

[Notes]

B16.5. If required as a result of an incident, is data isolated to facilitate forensic examination? How would you do this?

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.

[Notes]

B16.6. Do you report security incidents to external bodies as required, such as law enforcement for criminal activity and your country's data protection office?

You should report incidents to law enforcement for investigation where necessary. You may also be required to report personal data breaches to your country's data protection office.

[Notes]

B16.7. Do you keep a record during all security incidents to ensure lessons are learned from each event?

You should keep a record of what happened whilst handling the incident. The result of any investigations should also be recorded to aid future investigations and so that trends can be identified over time to help improve your incident prevention and handling processes.

[Notes]

MAINTAINING AND IMPROVING SECURITY

Your security controls should be embedded into regular day-to-day practice. Opportunities for improvement should be identified, evaluated, and implemented in line with your organisation's change management procedure. Striving to continuously improve is a key component of an Information Security Management System compliant with The IASME Cyber Assurance standard.

B17.1. Do you ensure that all of your security controls are maintained and improved as needed as part of your business-as-usual activities?

You should embed security into your regular day-to-day practices to ensure that your controls are maintained and where appropriate, improved upon. Some areas you should pay particular attention to include, making sure:

- *Your asset register remains up to date and asset usage reflects your acceptable usage policy*
- *The controls from a prerequisite scheme are maintained such as checking that software remains supported and up to date*
- *Encryption is used in accordance with the requirements defined in Theme 3 - Assets and your risk treatment plan*
- *Policies are created, reviewed, implemented, and updated in line with the requirements set out in Theme 8 - Policy realisation*
- *Your technology settings remain up to date in line with Theme 10 - Technical intrusion requirements*
- *Staff, contractors, and suppliers remain suitable for their role and have access to all the resources needed for their role but no more*

[Notes]