IASME Governance
Self-Assessment Preparation Booklet
includes assessment against
Cyber Essentials and GDPR

Version 11

February 2019

Introduction

This booklet contains the question set for the IASME Governance information assurance standard:

IASME Governance

Based on international best practice, IASME Governance is risk based and includes key aspects of security such as incident response, staff training, planning and operations.

IASME Governance incorporates Cyber Essentials assessment and an assessment against the General Data Protection Regulation (GDPR).

More information about the IAMSE Governance standard can be found at

https://www.iasme.co.uk

IASME Consortium ®

The IASME Governance standard incorporates our Cyber Essentials question set. If you achieve certification to IASME Governance you will also be awarded certification to Cyber Essentials.

Cyber Essentials

Cyber Essentials is a government-backed scheme focussing on the five important technical security controls.

Further guidance on the Cyber Essentials scheme can be found at

https://www.cyberessentials.ncsc.gov.uk

CYBER ESSENTIALS

Answering the questions

The booklet is intended to help you to understand the questions and take notes on the current setup in your organisation. In order to complete assessment, you must enter your answers via IASME's online assessment platform.

- Questions which apply only to the **IASME Governance** standard are in red
- Questions which apply to the **Cyber Essentials** requirements are in black.

In order to achieve IASME Governance certification, most companies will need to answer the black, and red questions.

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 you nearest Certification Body.

Your Company

In this section we need to know a little about how your organisation is set up so we can ask you the most appropriate questions.

A1.1. What is your organisation's name (for companies: as registered with Companies House)?
Please provide the full name for the company being certified. If you are certifying the local entity of a multinational company, provide the name of the local entity.

[Notes]

A1.2. What is your organisation's registration number (if you have one)?
If you are a UK limited company, your registration number will be provided by Companies House, in the Republic of Ireland, this will be provided by Companies Registration Office. Charities, partnerships and other organisations should provide their registration number if applicable.

[Notes]

A1.3. What is your organisation's address (for companies: as registered with Companies House)?
Please provide the legal registered address for your organisation, if different from the main operating location.

[Notes]

A1.4. What is your main business?
Please summarise the main occupation of your organisation

Agriculture, Forestry and Fishing

Mining and Quarrying

Manufacturing

Electricity, Gas, Steam and Air-conditioning Supply

Water supply, Sewerage, Waste management and Remediation

Construction

Wholesale and Retail trade

Repair of motorcars and motorcycles

Transport and storage

Accommodation and food services

Information and communication

Financial and insurance

Real estate

Professional, scientific and technical

Administration and support services

Public administration and defence

Compulsory social security

Education

Human Health and Social Work

Arts Entertainment and Recreation

Other service activities

Activities of households as employers; undifferentiated goods and services producing for households for own use

Activities of extraterritorial organisations and bodies

[Notes]

A1.5. What is your website address?

Please provide your website address (if you have one). This can be a Facebook/LinkedIn page if you prefer.

[Notes]

A1.6. What is the size of your organisation?

Based on the EU definitions of Micro (<10 employees, < €2m turnover), Small (<50 employees, < €10m turnover) , Medium (<250 employees, < €50m turnover) or Large.

[Notes]

A1.7. How many staff are home workers?

Home workers are staff whose main work location is their home address and who work there for the majority of their time. This does not include office workers who occasionally work at home or when travelling.

[Notes]

Scope of Assessment

In this section, we need you to describe the elements of your organisation which you want to certify to this accreditation. The scope should be either the whole organisation or an organisational sub-unit (for example, the UK operation of a multinational company). All computers, laptops, servers, mobile phones, tablets and firewalls/routers that can access the internet and are used by this organisation or sub-unit to access business information should be considered "in-scope". All locations that are owned or operated by this organisation or sub-unit, whether in the UK or internationally should be considered "in-scope".

A2.1. Does the scope of this assessment cover your whole organisation?

Please note: Your organisation is only eligible for free Cyber Insurance if your assessment covers your whole company, if you answer "No" to this question you will not be invited to apply for insurance.
Your whole organisation would include all divisions and all people and devices that use business data.

[Notes]

A2.2. If it is not the whole organisation, then what scope description would you like to appear on your certificate and website?

Your scope description should provide details of any areas of your business that have internet access and have been excluded from the assessment (for example, "whole company excluding development network").

[Notes]

A2.3. Does your organisation hold or process personal data (as defined by your country's data protection legislation)?

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

[Notes]

A2.4. Is your usage of personal data subject to the EU GDPR?

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

[Notes]

A2.5. Please describe the geographical locations of your business which are in the scope of this assessment.

You should provide either a broad description (i.e. All UK offices) or simply list the locations in scope (i.e. Manchester and Glasgow retail stores).

[Notes]

A2.6. Please list the quantities of laptops, computers and servers within the scope of this assessment. You must include the model and operating systems versions for all devices.

All laptops, computers, and servers that are used for accessing business data and have access to the internet must be included in the scope of the assessment. You do not need to provide serial numbers, mac addresses or other technical information.

[Notes]

A2.7. Please list the quantities of tablets and mobile devices within the scope of this assessment. You must include model and operating system versions for all devices.

All tablets and mobile devices that are used for accessing business data and have access to the internet must be included in the scope of the assessment. You do not need to provide serial numbers, mac addresses or other technical information.

[Notes]

A2.8. Please provide a list of the networks that will be in the scope for this assessment.

You should include details of each network used in your organisation including its name, location and its purpose (i.e. Main Network at Head Office for administrative use, Development Network at Malvern Office for testing software). You do not need to provide IP addresses or other technical information.

[Notes]

A2.9. Please provide a list of network equipment that will be in scope for this assessment (including firewalls and routers).

You should include all equipment that controls the flow of data such as routers and firewalls. You do not need to include switches or wireless access points that do not contain a firewall or do not route internet traffic.

[Notes]

A2.10. Please provide the name and role of the person who is responsible for managing the information systems in the scope of this assessment?

This should be the person who influences and makes decisions about the computers, laptops, servers, tablets, mobile phones and network equipment within your organisation. This person must be a member of your organisation and cannot be a person employed by your outsourced IT provider.

[Notes]

Insurance

All organisations with a head office domiciled in the UK and a turnover of less than £20 million get automatic cyber insurance if they achieve Cyber Essentials certification. The cost of this is included in the assessment package but you can opt out of the insurance element if you choose. This will not change the price of the assessment package. If you want the insurance then we do need to ask some additional questions and these answers will be forwarded to the broker. The answers to these questions will not affect the result of your Cyber Essentials assessment.

A3.1. Is your head office domiciled in the UK and is your gross annual turnover less than £20m?

This question relates to the eligibility of your company for the included cyber insurance.

[Notes]

A3.2. If you have answered "yes" to the last question then your company is eligible for the included cyber insurance if you gain certification. If you do not want this insurance element please opt out here.

The cost of this is included in the assessment package and you can see more about it at https://www.iasme.co.uk/index.php/cyberessentials profile/automatic-insurance-cover.

[Notes]

A3.3. What is your total gross revenue? You only need to answer this question if you are taking the insurance.

The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

A3.4. Is the company or its subsidiaries any of the following: medical, call centre, telemarketing, data processing (outsourcers), internet service provider, telecommunications or an organisation regulated by the FCA? You only need to answer this question if you are taking the insurance.

The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

A3.5. Does the company have any domiciled operation or derived revenue from the territory or jurisdiction of Canada and / or USA?

You only need to answer this question if you are taking the insurance. The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

A3.6. What is the organisation email contact for the insurance documents? You only need to answer this question if you are taking the insurance.

The answer to this question will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification and they will use this to contact you with your insurance documents and renewal information.

[Notes]

Managing Security

In this section, we need you to tell us about how you manage security within your organisation.

B1.1. Please provide the name of the board member / director / partner / trustee identified as responsible for information security and data protection?

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

[Notes]

B1.2. Is information security and data protection (including a review of any recent incidents) 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.

[Notes]

B1.3. Please provide the name and role of the person who has overall responsibility for security in your organisation?

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

[Notes]

B1.4. How do you ensure that you provide sufficient funding and a suitable number of appropriately skilled staff to develop and maintain good information security and data protection?

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

[Notes]

Information Assets

Risk assessment and recovery from information and cyber security incidents both rely on having a good understanding of your key information assets. Only then can you appreciate your attack surface and what you've got to lose. The impact of any security incident will be most severe if it happens to the assets which keep the organisation going.

B2.1. Does your organisation have up to date information and physical asset registers?

An asset register should track all categories of information and provide an owner for each one. It links closely to risk assessment by identifying the information assets that are to be protected. IASME has an information asset register template that can be used by applicants and is available on request.

[Notes]

B2.2. How does your asset register track information assets (i.e. categories of information)?

An information asset might be a set of data (for example "employee information") which will have a location attached to it (for example "the server in the HR department") and an owner (for example the "HR director").

[Notes]

B2.3. Do all assets (both physical and information assets) have named owners?

Having a named owner ensures that someone is taking responsibility for each asset.

[Notes]

B2.4. 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 and DVDs/CDs. 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 by whom.

[Notes]

B2.5. Are all mobile phones, tablets and laptops tracked in the asset register, pin/password protected and encrypted? Please describe how you have achieved this for all criteria within this question.

This can be achieved using built-in tools (such as iCloud/Find my iPhone, Find my Android or additional mobile device management (MDM) software.

[Notes]

B2.6. Is all personal data and special category data identified (e.g. by protective marking) and properly protected? Describe how this is done.

You need to be able to identify any such data within your organisation. This is important to ensure the rights of data subjects are upheld and will assist with meeting requirements such as Subject Access Requests.

[Notes]

B2.7. How do you ensure all flows of personal and special category data are documented, including 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]

B2.8. Is all sensitive information identified (e.g. by protective marking) and properly protected?

You must be able to identify all sensitive information within your company and make sure it is protected from cyber threats and errors/staff mistakes. You can do this by using protective marking where you assign categories (public, confidential, secret) and mark these categories 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]

B2.9. When assets are no longer required, is all data securely wiped from them or are the assets securely destroyed? Describe how this is done.

"Assets" include laptops, 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. You can alternatively physically destroy the assets yourself, although this is not always effective.

[Notes]

Cloud Services

Some organisations use public cloud services to store or share files between employees, suppliers and customers. Cloud services include Office 365, G Suite (Google Apps), Dropbox, Slack, Salesforce and Amazon Web Services (AWS).

B2.10. 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 Office365 or Gsuite, and cloud backup providers

[Notes]

B2.11. 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 your use to share information could include Slack, Yammer, Teams, Gsuite, Jira, Confluence and Basecamp.

[Notes]

B2.12. Where do your cloud providers store your data?

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

[Notes]

B2.13. Please describe which provisions have been put in place to ensure that the requirements of the GDPR are met fully for the data held in your cloud services?

If your cloud providers store your data outside of the European Economic Area (EEA) you will need to check that they have signed up to rules or agreements that ensure they offer equivalent protection to your data as would be found within the EEA.

[Notes]

B2.14. Which security accreditations are held by the cloud providers used by your organisation?

Your cloud providers should hold suitable security accreditations, particularly if you store sensitive data with them. Examples of security accreditations include ISO27001 and G-cloud.

[Notes]

B2.15. Is your data encrypted before being passed between your site and the public cloud provider(s) (i.e. encrypted in transit)?

Your cloud provider must encrypt your data when it is being sent between your computers and the cloud provider. This is usually achieved by using TLS encryption. For web-based services look for the https:// in the address bar and a padlock icon.

[Notes]

B2.16. Is your data encrypted whilst being stored by your cloud provider(s) (i.e. encrypted at rest)?

Your data should be encrypted by your cloud provider when it is being stored on their systems. It is difficult to confirm 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]

Risk Management

It is important to identify the threats to the organisation and assess the resulting risk. The applicability of the controls to your business is determined partly by a risk assessment and partly by your risk appetite. IASME knows that too few SMEs have a formal information risk assessment, nor a business risk assessment of any kind. However, they do have a keen sense of the risks and frailty of their business at board level. The organisation should create and regularly review Risk Assessments.

B3.1. Do you have a current Risk Assessment which includes information security risks and includes risks to data subjects for the information you hold?

You must ensure that your risk assessment covers risks to data from events such as malware infection, criminal activity and staff making mistakes. 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. A template is available from IASME .

[Notes]

B3.2. Has your risk assessment been reviewed in the last 12 months? Who reviewed it?

The assessment must be reviewed by a suitable group of people who between them have knowledge of all areas of the organisation.

[Notes]

B3.3. Does the risk assessment cover the scope of this assessment?

The risk assessment should cover the scope of your IASME Governance assessment.

[Notes]

B3.4. Does the risk assessment identify which actions you will be taking for each risk (such as reduce or accept)?

You need to make a decision for each risk you identify what you intend to do about it. Usually you will choose to decide the risk by making changes to your systems or processes.

[Notes]

B3.5. Do you have an action plan to implement any actions identified in the risk assessment?

An action plan lets you prioritise the changes that are needed to reduce the risks identified in your risk assessment.

[Notes]

B3.6. Was the risk assessment 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.

[Notes]

Data Protection

The organisation should have a policy to manage personal data as defined by your country's data protection legislation. The Information Commissioner's Office (ICO) website provides more information on this topic in the UK. Organisations that offer goods and services to EU member states must comply with the EU General Data Protection Regulations (GDPR).

B4.1. Have you put policies and procedures in place to mitigate risks to personal data?

To effectively manage risks to personal data you need a set of policies that set out your expectations and requirements around handling personal data.

[Notes]

B4.2. Are these policies and procedures provided to all employees, required to be followed in everyday practice and linked to disciplinary procedures? How do you achieve this?

It is important that the policies and procedures are followed by all employees in all situations.

[Notes]

B4.3. Is Data Protection referred to in employee contracts of employment?

Employee contracts of employment should outline responsibilities for the handling of the personal data of customers and employees.

[Notes]

B4.4. Do policies and procedures set clear responsibilities for handling of personal data, including where appropriate reference to responsibilities held by your Data Protection Officer?

It should be the responsibilities for managing personal data within the business.

[Notes]

B4.5. If you fall into the category of requiring a Data Protection Officer have you appointed one?

The GDPR introduces a duty for 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]

B4.6. When your organisation collects personal data from a subject do you clearly state what it is being collected for, how it will be processed and who will process it and does the data subject have to provide consent for this?

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

[Notes]

B4.7. 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.

[Notes]

B4.8. What is your process for dealing with Subject Access or Data Portability requests with 30 days? Do you have processes in place to maintain the rights of the individual, within the time limits laid down by the Regulation?

Under data protection legislation, individuals have a right to obtain a copy of the information you hold about them. This could include requests for subject access or data portability.

[Notes]

B4.9. Do you make it clear to data subjects how they should contact your organisation to exercise their rights and to raise complaints?

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]

B4.10. Do you have documented data retention periods and do these cover contractual and legal requirements?

You should decide how long you need to keep each type of data once the justification for keeping it has expired (such as when a customer stops using your product). Retention period will be influenced by legal requirements and your business needs.

[Notes]

B4.11. Do you have documented data classification criteria?

Data classification allows you to prioritise your efforts in protecting data by clearly identifying the most sensitive data to your organisation. Classification categories might include "public", "confidential", "sensitive" or "secret".

[Notes]

B4.12. Do you have a data privacy statement compliant with the requirements of GDPR and does the statement provide a point of contact for data protection issues? Who is the point of contact?

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

[Notes]

B4.13. 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]

B4.14. Do you have mechanisms in place which make it as easy for the data subject to remove consent for the data processing under the consent lawful purpose?

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]

B4.15. 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.

[Notes]

B4.16. 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.

[Notes]

B4.17. In each contract you hold with 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. It is important that suppliers and customers understand your role in each relationship.

[Notes]

B4.18. 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.

[Notes]

B4.19. 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]

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 that you know as much about them as possible before you employ them. This is usually done by taking up references, and in certain cases through formal vetting procedures.
It is essential that new employees are given a briefing on their corporate and security responsibilities before, or immediately after 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, user access privileges should be immediately withdrawn and the employee de-briefed on their post-employment confidentiality responsibilities.

B5.1. Do you take up references or confirm employment history (or carry out any other pre-employment checks to meet regulatory requirements) when employing new staff? How do you do this?

You should carry out checks when employing staff to verify their identity.

[Notes]

B5.2. 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 lawful purposes?

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

[Notes]

B5.3. 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.

[Notes]

B5.4. Do all staff and contractors receive regular information security and data protection training (at least annually)? 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.

[Notes]

B5.5. Do you give new employees a briefing on their corporate and security responsibilities before, or immediately after employment, preferably reinforced by reference literature? How do you do this?

You must brief staff on their security responsibilities. By providing literature such as a copy of the security policy or reference sheet staff can remind themselves of your requirements at a later date.

[Notes]

B5.6. Do employee contracts include security obligations (such as an obligation to comply with the security policy) and are reminders given at regular intervals?

Contracts ensure there is a legal basis for your security requirements.

[Notes]

B5.7. Are employees with responsibility for information security, or with privileged access to business systems, appropriately qualified and suitably trained?

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

[Notes]

B5.8. On termination of employment, are user access privileges immediately withdrawn and the employee de-briefed on their post-employment confidentiality responsibilities? How do you do this?

It is important that you remove access to systems when terminating employment - depending on the circumstances surrounding termination, you may choose to remove access immediately and not require employees to complete their notice period.

[Notes]

Security Policy

The organisation must have an implemented security policy to match its risk profile. This is usually the ultimate responsibility of the CIO/Director.
IASME provides a model template policy which can be adapted to the individual circumstances of most organisations.
Dates for achieving objectives can be set within the policy, which should be reviewed by the Board at regular intervals or when security incidents occur or changes in the risk landscape emerge.

B6.1. Do you have a policy or set of policies that cover information security?

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

[Notes]

B6.2. Has your Policy been reviewed in the last 12 months?

Your security policies must be reviewed by a suitable group of people who between them have knowledge of all areas of the organisation.

[Notes]

B6.3. Do your information security policies cover the scope of this assessment?

The policies must apply to all business units covered by this assessment.

[Notes]

B6.4. 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.

[Notes]

B6.5. Is there a policy review and consultation process?

Policies must be regularly reviewed and updated to ensure they stay current and reflect business requirements.

[Notes]

B6.6. Do your policies refer to Intellectual Property Rights and legal requirements?

Your policies should meet any legal requirements that apply to your organisation.

[Notes]

B6.7. Do your policies refer to personnel security?

Your policies should cover how you ensure that staff and contractors identities are verified and any other personnel security checks such as vetting are carried out.

[Notes]

B6.8. Do your policies refer to asset management (including removable media)?

Your policies should define how you manage physical and information assets including procedures when new assets are acquired and when assets are no longer required.

[Notes]

B6.9. Do your policies refer to user authentication and access management?

Your policies should detail how users are authenticated onto your systems and how you ensure access to systems is restricted to only authorised people

[Notes]

B6.10. Do your policies refer to physical and environmental security?

Your policies should cover your requirements on physical access to locations and systems, as well as any environmental requirements such as heating and cooling of equipment.

[Notes]

B6.11. Do your policies refer to computer and network security?

Your policies should cover security of systems and networks.

[Notes]

B6.12. Do your policies refer to monitoring and acceptable usage of systems/data?

Your policies should detail how your company carried out monitoring of data and system access and usage. They should also detail what usage is acceptable so that staff understand for which purposes they may use systems.

[Notes]

B6.13. Do your policies refer to security from malware and intrusion?

Your policies should set requirements around how systems are to be kept safe from malware attacks and attempts by hackers to gain access to systems and data through network intrusion.

[Notes]

B6.14. Do your policies refer to security incident management?

Your policies should detail how your company will deal with security incidents.

[Notes]

B6.15. Do your policies refer to business continuity measures?

Your policies should detail how your company will deal with incidents that threaten the viability and operation of the business through invoking business continuity measures.

[Notes]

B6.16. Do your polices refer to home and mobile working?

Your policies should set expectations around how staff should act when working at home or in other locations such as client sites or when travelling.

[Notes]

B6.17. Do your policies refer to handling personal data (and, where appropriate, reference your data protection policy)?

Your policies should set requirements around handling of personal data. This may be contained within a data protection policy.

[Notes]

B6.18. Are your information security policies distributed to all employees?

You must distribute a copy of your information security policy set (containing all the topics listed in the previous questions) to all employees. This could be a physical copy or via email/instant messaging. You cannot just place the policy in a shared area, unless employees also receive an email/instant message with a link to the shared area and a request to click the link and view the policies

[Notes]

B6.19. Are your information security policies part of all employees' contractual obligations?

Staff must be contractually obligated to follow the requirements defined within your policies

[Notes]

B6.20. Do the contracts with all your suppliers ensure that they meet a set of security requirements that you have defined around handling data and keeping information secure? Please explain the requirements you have set and the reasons why you have chosen them.

The security requirements you define for your suppliers may be determined by your regulatory or business environment. For example, MoD suppliers will be required to flow-down certain security requirements to their supply chain.

[Notes]

B6.21. List any business sector-specific regulations relating to risk treatment or information security which apply to your business.

Such regulations might include the Financial Conduct Authority rules for regulated businesses.

[Notes]

B6.22. List any local or international laws relating to risk treatment or information security which apply to your business.

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

[Notes]

B6.23. Do you store credit card information?

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

[Notes]

B6.24. If yes to above, are the systems that you use to store credit card information compliant to PCI-DSS regulation?

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

[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 etc, 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.

B7.1. 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 access any other people from accessing such systems using locks, alarms, security cages or any other form of physical access control.

[Notes]

B7.2. 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 blocking USB storage devices)?

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]

B7.3. 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]

B7.4. 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?

Servers and networking equipment may need air conditioning to ensure they keep to a reliable operating temperature.

[Notes]

B7.5. Do all business premises have effective physical protection and, if indicated by a risk assessment, surveillance and monitoring?

You should carry out a physical risk assessment to determine if any areas of your premises are at risk of being accessed by unauthorised people. If you find risks, you should install locks, access control, video monitoring, additional staff or other controls to reduce the risk.

[Notes]

Office Firewalls and Internet Gateways

Firewall is the generic name for software or hardware which provides technical protection between your systems and the outside world. There will be a firewall within your internet router. Common internet routers are BT Home Hub, Virgin Media Hub or Sky Hub.

Your organisation may also have set up a separate hardware firewall device between your network and the internet. Firewalls are powerful devices and need to be configured correctly to provide effective security.

Questions in this section apply to: Hardware Firewall devices, Routers, Computers and Laptops only.

A4.1. Do you have firewalls at the boundaries between your organisation's internal networks and the internet?

You must have firewalls in place between your office network and the internet. You should also have firewalls in place for home-based workers, if those users are not using a Virtual Private Network (VPN) connected to your office network.

[Notes]

A4.2. When you first receive an internet router or hardware firewall device it will have had a default password on it. Has this initial password been changed on all such devices? How do you achieve this?

The default password must be changed on all routers and firewalls, including those that come with a unique password pre-configured (i.e. BT Hub) You can change the default password by logging into the web interface for the device (often located at 192.168.1.1 or 192.168.1.254).

[Notes]

A4.3. Is the new password on all your internet routers or hardware firewall devices at least 8 characters in length and difficult to guess?

A password that is difficult to guess will be unique and not be made up of common or predictable words such as "password" or "admin", or include predictable number sequences such as "12345".

[Notes]

A4.4. Do you change the password when you believe it may have been compromised? How do you achieve this?

Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should be aware of this and know how to change the password if this occurs.

[Notes]

A4.5. Do you have any services enabled that are accessible externally from your internet routers or hardware firewall devices for which you do not have a documented business case?

At times your firewall may be configured to allow a system on the inside to become accessible from the internet (such as a VPN server, a mail server or a service that is accessed by your customers). This is sometimes referred to as "opening a port". You need to show a business case for doing this because it can present security risks. If you have not enabled any services, answer "No". By default, most firewalls block all services. The business case should be documented and recorded.

[Notes]

A4.6. If you do have services enabled on your firewall, do you have a process to ensure they are disabled in a timely manner when they are no longer required? Describe the process.

If you no longer need a service to be enabled on your firewall, you must remove it to reduce the risk of compromise. You should have a process that you follow to do this (i.e. when are services reviewed, who decides to remove the services, who checks that it has been done).

[Notes]

A4.7. Have you configured your internet routers or hardware firewall devices so that they block all other services from being advertised to the internet?

By default, most firewalls block all services from inside the network from being accessed from the internet, but you need to check your firewall settings.

[Notes]

A4.8. Are your internet routers or hardware firewalls configured to allow access to their configuration settings over the internet?

Sometimes organisations configure their firewall to allow other people (such as an IT support company) to change the settings via the internet. If you have not set up your firewalls to be accessible to people outside your organisations or your device configuration settings are only accessible via a VPN connection, then answer "no" to this question.

[Notes]

A4.9. If yes, is there a documented business requirement for this access?

You must have made a decision in the business that you need to provide external access to your routers and firewalls. This decision must be documented (i.e. written down).

[Notes]

A4.10. If yes, is the access to the settings protected by either two-factor authentication or by only allowing trusted IP addresses to access the settings? List which option is used.

If you allow direct access to configuration settings via your router or firewall's external interface, this must be protected by one of the two options.

[Notes]

A4.11. Do you have software firewalls enabled on all of your computers and laptops?

You can check this setting on Macs in the Security & Privacy section of System Preferences. On Windows laptops you can check this by going to Settings and searching for "windows firewall". On Linux try "ufw status". You can also use the firewall that may be provided by your anti-virus software.

[Notes]

A4.12. If no, is this because software firewalls are not commonly available for the operating system you are using? Please list the operating systems.

Only very few operating systems do not have software firewalls available. Examples might include embedded Linux systems or bespoke servers. For the avoidance of doubt, all versions of Windows, macOS and all common Linux distributions such as Ubuntu do have software firewalls available.

[Notes]

Secure Configuration

Computers are often not secure upon default installation. An 'out-of-the-box' set-up can often include an administrative account with a standard, publicly known default password, one or more unnecessary user accounts enabled (sometimes with special access privileges) and pre-installed but unnecessary applications or services. All of these present security risks.
Questions in this section apply operating systems and applications running on: Servers, Computers, Laptops, Tablets and Mobile Phones.

A5.1. Where you are able to do so, have you removed or disabled all the software that you do not use on your laptops, computers, servers, tablets and mobile phones? Describe how you achieve this.

To view your installed applications on Windows look in Start Menu, on macOS open Finder -> Applications and on Linux open your software package manager (apt, rpm, yum). You must remove or disable all applications, system utilities and network services that are not needed in day-to-day use.

[Notes]

A5.2. Have you ensured that all your laptops, computers, servers, tablets and mobile devices only contain necessary user accounts that are regularly used in the course of your business?

You must remove or disable any user accounts that are no needed in day-to-day use on all devices. You can view your user accounts on Windows by righting-click on Start -> Computer Management -> Users, on macOS in System Preferences -> Users & Groups, and on Linux using "cat /etc/passwd"

[Notes]

A5.3. Have you changed the default password for all user and administrator accounts on all your laptops, computers, servers, tablets and smartphones to a non-guessable password of 8 characters or more?

A password that is difficult to guess will be unique and not be made up of common or predictable words such as "password" or "admin", or include predictable number sequences such as "12345".

[Notes]

A5.4. Do all your users and administrators use passwords of at least 8 characters?

The longer a password, the more difficult it is for cyber criminals to guess (or brute-force) it.

[Notes]

A5.5. Do you run software that provides sensitive or critical information (that shouldn't be made public) to external users across the internet?

Your business might run software that allows people outside the company on the internet to access information within your business via an external service. This could be a VPN server, a mail server, or an internet application that you provide to your customers as a product. In all cases these applications provide information that is confidential to your business and your customers and that you would not want to be publicly accessible. This question does not apply to cloud services such as Google Drive, Office365 or Dropbox. If you only use such services and do not run your own service you should answer no to this question.

[Notes]

A5.6. If yes, do you ensure all users of these services use a password of at least 8 characters and that your systems do not restrict the length of the password?

The longer a password, the more difficult it is for cyber criminals to guess (or brute-force) it.

[Notes]

A5.7. If yes, do you ensure that you change passwords if you believe that they have been compromised?

Passwords may be compromised if there has been a virus on your system or if the manufacturer notifies you of a security weakness in their product. You should be aware of this and know how to change the password if this occurs.

[Notes]

A5.8. If yes, are your systems set to lockout after ten or fewer unsuccessful login attempts, or limit the number of login attempts to no more than ten within five minutes?

The external service that you provide must be set to slow down to stop attempts to log in if the wrong username and password have been tried a number of times. This reduces the opportunity for cyber criminals to keep trying different passwords (brute-forcing) in the hope of gaining access.

[Notes]

A5.9. If yes, do you have a password policy that guides all your users?

The password policy must include: guidance on how to choose non-guessable passwords, not to use the same password for multiple accounts, which passwords may be written down and where they can be stored, and if they may use a password manager.

[Notes]

A5.10. Is "auto-run" or "auto-play" disabled on all of your systems?

This is a setting which automatically runs software on a DVD or memory stick. You can disable "auto-run" or "auto-play" on Windows through Settings, on macOS through System Preferences and on Linux through the settings app for your distribution.

It is acceptable to choose the option where a user is prompted to make a choice about what action will occur each time they insert a memory stick. If you have chosen this option you can answer yes to this question.

[Notes]

Software Patching

To protect your organisation, you should ensure that your software is always up-to-date with the latest patches. If, on any of your in-scope devices, you are using an operating system which is no longer supported, (e.g. Microsoft Windows XP/Vista/2003 or macOS El Capitan, Ubuntu 17.10), and you are not being provided with updates from another reliable source, then you will not be awarded certification. Mobile phones and tablets are in-scope and must also use an operating system that is still supported by the manufacturer.

Questions in this section apply to: Servers, Computers, Laptops, Tablets, Mobile Phones, Routers and Firewalls.

A6.1. Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems?

Please list the operating systems you use so that the assessor can understand your setup and verify that all your operating systems are still in support. Older operating systems that are out of support include Windows XP/Vista/2003, mac OS El Capitan and Ubuntu Linux 17.10.

[Notes]

A6.2. Are all applications on your devices supported by a supplier that produces regular fixes for any security problems?

Please summarise the applications you use so the assessor can understand your setup and confirm that all applications are supported. This includes frameworks and plugins such as Java, Flash, Adobe Reader and .NET

[Notes]

A6.3. Is all software licensed in accordance with the publisher's recommendations?

All software must be licensed. It is acceptable to use free and open source software as long as you comply with any licensing requirements.

[Notes]

A6.4. Are all high-risk or critical security updates for operating systems and firmware installed within 14 days of release? Describe how do you achieve this.

You must install any such updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates.

[Notes]

A6.5. Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Adobe Flash) installed within 14 days of release? Describe how you achieve this.

You must install any such updates within 14 days in all circumstances. If you cannot achieve this requirement at all times, you will not achieve compliance to this question. You are not required to install feature updates or optional updates in order to meet this requirement, just high-risk or critical security updates.

[Notes]

A6.6. Have you removed any applications on your devices that are no longer supported and no longer received regular fixes for security problems?

You must remove older applications from your devices when they are no longer supported by the manufacturer. Such applications might include older versions of web browsers, frameworks such as Java and Flash, and all application software.

[Notes]

Operations and 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.

B8.1. Is management of computers and networks controlled using documented procedures that have been authorised? Describe how you achieve this.

Changes to systems must be made following clear procedures that have been defined by the organisation.

[Notes]

B8.2. Does the organisation ensure that all new and modified information systems, applications and networks include security provisions, 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 systems. You can achieve this by having a review process for all new and modified systems which involves both technical, security and operational staff.

[Notes]

B8.3. 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]

B8.4. Are changes to information systems, applications or networks reviewed and approved, and users disallowed from making 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. 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]

B8.5. Where identified as necessary in your risk assessment, have you identified and 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 provide security.

[Notes]

B8.6. 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 wireless security (such as WPA2) 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]

B8.7. Do you use firewalls or other technology to block and monitor access to malicious internet locations/domains at the boundary of your networks?

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 to achieve this.

[Notes]

B8.8. Do you ensure that a Data Protection Impact Assessment (DPIA) is carried out for 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]

B8.9. 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]

B8.10. How do you ensure that all your suppliers (including cloud providers and sub-contractors) follow information security procedures that are certified to be the same as, or more comprehensive than, the information security procedures followed by your own organisation for the data involved in that contract?

An example of such certification would be an independent audit of the whole business to ISO27001, the IASME Governance standard or Cyber Essentials. Bear in mind that a contract involving purely public data (such as hosting a simple website) may require a lower standard of information security that one involving more sensitive information (such as customer personal data).

[Notes]

B8.11. Do you have Data Processing Agreements in place with all suppliers that process personal data on your behalf?

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

[Notes]

User Accounts

It is important to only give users access to the resources and data necessary for their roles, and no more. All users need to have unique accounts and should not be carrying out day-to-day tasks such as invoicing or dealing with e-mail whilst logged on as a user with administrator privileges which allow significant changes to the way your computer systems work.

Questions in this section apply to: Servers, Computers, Laptops, Tablets and Mobile Phones.

A7.1. Are users only provided with user accounts after a process has been followed to approve their creation? Describe the process.

You must ensure that user accounts (such as logins to laptops and accounts on servers) are only provided after they have been approved by a person with a leadership role in the business.

[Notes]

A7.2. Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique user name and password?

You must ensure that no devices can be accessed without entering a username and password. Users cannot share accounts.

[Notes]

A7.3. How do you ensure you have deleted, or disabled, any accounts for staff who are no longer with your organisation?

When an individual leaves your organisation you need to stop them accessing any of your systems.

[Notes]

A7.4. Do you ensure that staff only have the privileges that they need to do their current job? How do you do this?

When a staff member changes job role you may also need to change their access privileges to systems and data.

[Notes]

Administrative Accounts

User accounts with special access privileges (e.g. administrative accounts) typically have the greatest level of access to information, applications and computers. When these privileged accounts are accessed by attackers they can cause the most amount of damage because they can usually perform actions such as install malicious software and make changes. Special access includes privileges over and above those of normal users.

It is not acceptable to work on day-to-day basis in a privileged "administrator" mode.

Questions in this section apply to: Servers, Computers, Laptops, Tablets and Mobile Phones.

A7.5. Do you have a formal process for giving someone access to systems at an "administrator" level? Describe the process.

You must have a formal, written-down process that you follow when deciding to give someone access to systems at administrator level. This process might include approval by a person who is an owner/director/trustee/partner of the organisation.

[Notes]

A7.6. How do you ensure that staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)?

You must ensure that administrator accounts are only used when absolutely necessary, such as when installing software. Using administrator accounts all-day-long exposes the device to compromise by malware.

[Notes]

A7.7. How do you ensure that administrator accounts are not used for accessing email or web browsing?

You must ensure that administrator accounts are not used to access websites or download email. Using such accounts in this way exposes the device to compromise by malware. 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]

A7.8. Do you formally track which users have administrator accounts in your organisation?

You must track by means of list or formal record all people that have been granted administrator accounts.

[Notes]

A7.9. Do you review who should have administrative access on a regular basis?

You must review the list of people with administrator access regularly. Depending on your business, this might be monthly, quarterly or annually. Any users who no longer need administrative access to carry out their role should have it removed.

[Notes]

A7.10. Have you enabled two-factor authentication for access to all administrative accounts?

If your systems support two factor authentication (where you receive a text message, a one-time code, use a finger-print reader or facial recognition in addition to a password), then you must enable this for administrator accounts.

[Notes]

A7.11. If no, is this because two-factor authentication is not available for some or all of your devices or systems? List the devices or systems that do not allow two-factor authentication.

You are not required to purchase any additional hardware or install additional software in order to meet this requirement. Most standard laptops do not have two-factor authentication available. It your systems do not have two-factor authentication available answer yes to this question.

[Notes]

Malware protection

Malware (such as computer viruses) is generally used to steal or damage information. Malware are often used in conjunction with other kinds of attack such as 'phishing' (obtaining information by confidence trickery) and social network sites (which can be mined for information useful to a hacker) to provide a focussed attack on an organisation. Anti-malware solutions (including anti-virus) are available from commercial suppliers, some free, but usually as complete software and support packages.

Malware are continually evolving, so it is important that the supplier includes both malware signatures and heuristic detection facilities which are updated as frequently as possible. Anti-malware products can also help confirm whether websites you visit are malicious.

Questions in this section apply to: Computers, Laptops, Tablets and Mobile Phones.

A8.1. Are all of your computers, laptops, tablets and mobile phones protected from malware by either

A - having anti-malware software installed,

B - limiting installation of applications to an approved set (i.e. using an App Store and a list of approved applications) or

C - application sandboxing (i.e. by using a virtual machine)?

Please select all the options that are in use in your organisation across all your devices. Most organisations that use smartphones and standard laptops will need to select both option A and B.

[Notes]

A8.2. If Option A: Where you have anti-malware software installed, is it set to update daily and scan files automatically upon access?

This is usually the default setting for anti-malware software. You can check these settings in the configuration screen for your anti-virus software. You can use any commonly used anti-virus product, whether free or paid-for as long as it can meet the requirements in this question. For the avoidance of doubt, Windows Defender is suitable for this purpose.

[Notes]

A8.3. If Option A: Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?

Your anti-virus software should have a plugin for your internet browser or for the operating system itself that prevents access to known malicious websites. On Windows 10, SmartScreen can provide this functionality.

[Notes]

A8.4. If Option B: Where you use an app-store or application signing, are users restricted from installing unsigned applications?

By default, most mobile phones and tablets restrict you from installing unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications.

[Notes]

A8.5. If Option B: Where you use an app-store or application signing, do you ensure that users only install applications that have been approved by your organisation and do you document this list of approved applications?

You must create a list of approved applications and ensure users only install these applications on their devices. This includes employee-owned devices. You may use Mobile Device Management (MDM) software to meet this requirement but you are not required to use MDM software if you can meet the requirements using good policy, process and training of staff.

[Notes]

A8.6. If Option C: Where you use application sandboxing, do you ensure that applications within the sandbox are unable to access data stores, sensitive peripherals and your local network? Describe how you achieve this.

If you are using a virtual machine to sandbox applications, you can usually set these settings within the configuration options of the virtual machine software.

[Notes]

Vulnerability Scanning

A vulnerability scan is a technical examination of the security status of your IT system. It can be performed by an expert or by some automatic tools and can help you answer and provide evidence for some of the following questions.

Some scanning tools are even 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.

B9.1. When was the last time you had a vulnerability scan on your system?

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

[Notes]

B9.2. 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]

B9.3. How did you act to improve the security of your system on the basis of the scan results?

[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.

B10.1. Does the organisation regularly review event logs (including alerts and errors) at least weekly?

If you use an automated system to monitor events and flag up suspicious activity, then that is acceptable and you should answer yes to this question.

[Notes]

B10.2. Is an audit trail of system access and/or data use by staff maintained in a central location for all relevant systems and reviewed on a regular basis? Describe how you achieve this.

You should ensure that logs of system access and use are pulled to a central location. This could be using a cloud-based solution or a local server.

[Notes]

B10.3. Do you ensure that all your devices have their time set accurately to ensure logs and audit trails are in sync with each other?

You can make sure your devices are synchronised by changing the date/time preferences to enable automatic or internet time.

[Notes]

B10.4. Do you ensure that any event logs and audit trails are kept secure and do not expose sensitive information to unauthorised users?

You should endure that any logs are stored in a safe location and that error messages do not return sensitive information to external or internal users.

[Notes]

Backup and Restore

Key information should be backed up regularly and the backups preferably kept in a secure location away from the business premises. Restores should be tested regularly in order to test the performance of the backup regime.

B11.1. Are data stored on the business premises backed up regularly (at least weekly) and restores tested at appropriate intervals (at least monthly)?

You must ensure a copy of all important data is made regularly and stored in a location other than your main place of business. 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]

B11.2. How do you ensure all backups are secured with an appropriate level of protection for the type of data they contain?

Your backups contain your sensitive company data and must be protected with the same amount of effort as the main location of the data. Backups should be stored securely and encrypted.

[Notes]

B11.3. Is a backup copy held in a different physical location?

You must keep at least one backup copy in a different physical location from your main office. If the main office was destroyed by fire, you would still be able to access the backup copy if it is in a different location.

[Notes]

Incident Management

All organisations 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.

B12.1. Are all information security incidents or suspected weaknesses reported and recorded, and do you provide a method for all employees and contractors to report security incidents without risk of recrimination (or anonymously)?

You must provide a route for staff and contractors to report any security weaknesses they encounter - including staff acting incorrectly and configuration issues. It is important that staff 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]

B12.2. 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.

[Notes]

B12.3. Do you formally investigate information security incidents to establish their cause and their impact with a view to avoiding similar event?

You must investigate incidents using a team of knowledgeable and appropriately skilled people to ensure that changes are made to prevent the incident reoccurring. You can use an external company to provide this service to you if needed.

[Notes]

B12.4. If required as a result of an incident, is data isolated to facilitate forensic examination? How is this done?

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]

B12.5. Do you report incidents to external bodies as required, such as law enforcement for criminal activity and the relevant authorities (such as the UK ICO) for personal data breaches?

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

[Notes]

B12.6. Is a record kept of the outcome of all security incident investigations to ensure all lessons have been learned from each event?

The result of any investigations should be recorded so that trends can be identified over time and to aid future investigations.

[Notes]

B12.7. Do all staff involved with incident management have clear roles and responsibilities and have they received appropriate training?

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

[Notes]

B12.8. Do you test your incident response process at least once per year?

You should carry out a table-top exercise where you create a plausible scenario (such as a staff member accidentally emailing 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.

[Notes]

Business Continuity

Plans for recovery and continuity should be drawn up, reviewed regularly, and 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.

B13.1. Do you ensure that business impact assessment, business continuity and disaster recovery plans are produced for your critical information, applications, systems 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.

[Notes]

B13.2. Do you review the business continuity and disaster recovery plans at least once per year? Who is involved in the review?

You should involve a group of people from across the organisation to review the plans including representation from the board/director/partner/trustee level.

[Notes]

B13.3. Do you test the business continuity and disaster recovery plans at least once per year by running a simulation exercise that includes cyber incidents?

You should test your plans by at least running a table-top exercise each year where you test how the plans would operate in major incident. Your risk assessment may indicate that you need to carry out such tests more often.

[Notes]

Achieving compliance with the Cyber Essentials profile or the IASME governance standard indicates that your organisation has taken the steps set out in the HMG Cyber Essentials Scheme documents or the broader IASME Governance standard. It does not amount to an assurance that the organisation is free from cyber vulnerabilities and neither IASME Consortium Limited (as Accreditation Body) nor the Certification Body accepts any liability to certified organisations or any other person or body in relation to any reliance they might place on the certificate.

A "pass" under the GDPR assessment does not mean that you are assessed as being legally compliant. It indicates only that your organisation is starting on the pathway to compliance and is committed to ensuring 'privacy by design'.

You should ensure that your organisation obtains specialist legal advice on the GDPR as on any other data protection issue. This GDPR assessment is not legal advice and must not be relied upon as such and IASME accepts no liability for loss or damage suffered as a result of reliance on views expressed here.

The full extent of the GDPR regime and its application post Brexit (for example) is not yet fully known but the assessment addresses what we consider to be key elements and to help organisations demonstrate progress towards meeting the policy objectives that underpins the GDPR.

If you are awarded a certificate you will also be sent a badge to use in correspondence and publicity. You must accept the conditions of use.