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

Amwell Information Security Ltd

Contact: info@amwellsolutions.co.uk

Version 10.8

May 2018

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.
- The questions in blue only need to be completed if you hold or process personal data about EU citizens

In order to achieve IASME Governance certification, most companies will need to answer the black, red and blue questions. If your company does not hold or process personal data about EU citizens, you can ignore the blue questions and still 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 you nearest Certification Body.

Your Company

Please tell us a little about how your company is set up

1. What is your organisation's name (for companies: as registered with Companies House)?

[Notes]

2. What is your organisation's registration number (if you have one)?

[Notes]

3. What is your organisation's address (for companies: as registered with Companies House)?

[Notes]

4. What is your main business?

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]

5. What is your website address?

[Notes]

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]

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

Please briefly 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".

8. 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.

[Notes]

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

[Notes]

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

[Notes]

11. Have you completed a Data Protection Impact Assessment, or Privacy Impact Assessment in the last 12 months?

[Notes]

12. Is your usage of personal data subject to the EU GDPR? If you hold and process personal data about EU citizens, you must comply with the EU GDPR wherever you are located in the world).

[Notes]

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

[Notes]

14. Please list all equipment which is included in the scope of this assessment (please include details of laptops, computers, servers, mobile phones and tablets).

All laptops, computers, servers and mobile devices that can access business data and have access to the internet must be included in the scope of the assessment.

[Notes]

15. Please provide details of the networks that will be in the scope for this assessment (such as office network, home offices and firewalls).

[Notes]

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

[Notes]

Managing Security

Please tell us about how you manage security within your organisation.

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

[Notes]

18. Is information security and data protection a standing agenda item for your Board Meetings?

[Notes]

19. Please provide the name and role of the person who has overall responsibility for security in your organisation? This should be a named board member or director.

[Notes]

20. Please provide the name and role of the person who has overall responsibility for data protection in your organisation? This should be a named board member or director.

[Notes]

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

[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.

22. Does your organisation have up to date asset registers?

[Notes]

23. How does your asset management system track your own and other company's intellectual property within your organisation?

[Notes]

24. How does your asset register track information assets (ie 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]

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

[Notes]

26. How is removable media recorded and managed?

[Notes]

27. Confirm and describe how all mobile phones and tablets are tracked in the asset register, pin or password protected, encrypted and remotely wipeable. Please describe all criteria within this question.

This can be achieved using built-in tools or additional mobile device management software.

[Notes]

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

[Notes]

29. How do you ensure all flows of personal and special category data are documented including where data was obtained and all destinations of data?

[Notes]

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

[Notes]

31. Describe how your processes allow data subjects to request changes to incorrect data or deletion of data?

[Notes]

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

Special software can be used to securely wipe data and external companies can be used to provide a secure destruction service.

[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, Salesforce and Amazon Web Services (AWS).

33. Do you use a public cloud provider to store or share files and information between employees? If so, please list all providers.

[Notes]

34. Where is the data that is sent to a public cloud provider stored?

[Notes]

35. If you store personal data with your cloud provider, do you store any of that data outside of the European Economic Area (EEA)?

[Notes]

36. If yes to the above, have you obtained explicit consent from data subjects to transfer their data outside of the European Economic Area (EEA)?

[Notes]

37. If yes to the above, does your provider certify to an agreement such as EU-UK Privacy Shield or to other binding corporate rules that confirm the level of protection given to that data?

[Notes]

38. Do the public cloud providers that your organisation uses hold any recognised security accreditations?

[Notes]

39. Is your data encrypted before being passed between your site and the public cloud provider (ie encrypted in transit)?

[Notes]

40. Is your data encrypted whilst being stored or processed by the public cloud provider (ie encrypted at rest)?

[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.

41. Do you have a current Risk Assessment?

[Notes]

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

[Notes]

43. Does the risk assessment cover the scope of this assessment?

[Notes]

44. Was the risk assessment approved at Board Level?

[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. Based on current government guidance and policy it is likely that any organisation proposing to offer goods and services to EU members states will need to comply with the EU General Data Protection Regulation (GDPR) from May 2018.

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

[Notes]

46. 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?

[Notes]

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

[Notes]

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

[Notes]

49. 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?

[Notes]

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

[Notes]

51. Does your risk assessment cover the management of personal data or special category data?

[Notes]

52. What is your process for dealing with Subject Access or Data Portability requests within 30 days?

Under data protection legislation, individuals have a right to obtain a copy of the information you hold about them.

[Notes]

53. What is your process for correcting inaccurate records, deleting records or suspending the processing of records?

Under data protection legislation, individuals have the right to have inaccuracies corrected and may have the right to have information about them deleted from systems.

[Notes]

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

[Notes]

55. Do you have documented data classification criteria?

[Notes]

56. Do you have a data protection or data privacy statement compliant with the requirements of the General Data Protection Regulation (GDPR) and does the statement provide a point of contact for data protection issues? Who is the point of contact?

[Notes]

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

[Notes]

58. Do you have mechanisms in place which make it as easy for the data subject to remove consent for data processing and do you ensure it is as easy to remove consent as it was for them to give it?

[Notes]

59. For each piece of personal information you hold, do you record the purpose for which it was obtained? Where is this recorded?

[Notes]

60. For each piece of personal information 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.

[Notes]

61. For each piece of special category data you hold, do you record the justification for obtaining it? Where is this recorded?

Justifications for obtaining special category (or sensitive personal data) could include specific consent, use for employment purposes or to meet a medical need.

[Notes]

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

[Notes]

63. 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?

[Notes]

64. 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?

[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.

65. Do you take up references and/or confirm employment history when employing new staff? How do you do this?

[Notes]

66. 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?

[Notes]

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

[Notes]

68. Do all staff and contractors receive regular information security and data protection training (at least annually)? Describe how this is done.

[Notes]

69. 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?

[Notes]

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

[Notes]

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

[Notes]

72. 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?

[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 with in the policy, which should be reviewed by the Board at regular intervals or when security incidents occur or changes in the risk the landscape emerge.

73. Do you have a current Security Policy?

A Security Policy can be stand-alone or incorporated into other policy, but it should set out your objectives for managing your security.

[Notes]

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

[Notes]

75. Does the Policy cover the scope of this assessment?

[Notes]

76. Provide the name and role of the person who approved the policy?

[Notes]

77. Is there a policy review and consultation process?

[Notes]

78. Does the policy refer to Intellectual Property Rights and legal requirements?

[Notes]

79. Does the policy refer to personnel security?

[Notes]

80. Does the policy refer to asset management?

[Notes]

81. Does the policy refer to access management?

[Notes]

82. Does the policy refer to physical and environmental security?

[Notes]

83. Does the policy refer to computer and network security?

[Notes]

84. Does the policy refer to security from malware and intrusion?

[Notes]

85. Does the policy refer to security incident management?

[Notes]

86. Does the policy refer to business continuity measures?

[Notes]

87. Does the policy refer to handling personal data (and, where appropriate, reference your data protection policy)?

[Notes]

88. Is the policy distributed to all employees?

[Notes]

89. Is the security policy part of all employees' contractual obligations?

[Notes]

90. Do the contracts with all your suppliers ensure that they meet the requirements of your security policy around handling data and keeping information secure?

[Notes]

91. List any business sector-specific laws/regulations relating to risk treatment or information security which apply to your business.

[Notes]

92. List any UK or EU laws/ regulations relating to risk treatment or information security which apply to your business.

[Notes]

93. List any other International legislation/regulations relating to risk treatment or information security which apply to your business.

[Notes]

94. Do you store credit card information?

[Notes]

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

[Notes]

96. Is your business part of a public global organisation that is required to have external financial reporting?

[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.

97. 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?

[Notes]

98. 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?

[Notes]

99. Do all business premises have effective physical protection and, if indicated by a risk assessment, surveillance and monitoring? How do you achieve this?

[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

100. Do you have firewalls at the boundaries between your organisations internal networks and the internet?

You should 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. Remember most internet-routers contain a firewall.

[Notes]

101. 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?

[Notes]

102. 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 not be made up of common or predictable words such as "password" or "admin", or include predictable number sequences such as "12345".

[Notes]

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

[Notes]

104. 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 server or a video conferencing unit). 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".

[Notes]

105. 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.

[Notes]

106. 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]

107. 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]

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

[Notes]

109. 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.

[Notes]

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

You can check this setting on Mac laptops in the Security & Privacy section of System Preferences. On Windows laptops you can check this by going to Settings or Control Panel and searching for "windows firewall".

[Notes]

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

[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 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.

112. 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. This includes applications, system utilities and network services.

[Notes]

113. 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?

[Notes]

114. 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?

[Notes]

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

A strong password typically is a mixture of at least 8 characters, numbers and symbols, the longer the better.

[Notes]

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

[Notes]

117. 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?

[Notes]

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

[Notes]

119. 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?

[Notes]

120. 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]

121. 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" through control panel / system preferences.

[Notes]

Software Patching

To protect your organisation, you should ensure that your software is always up-to-date with the latest updates or "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 or mac OS Mountain Lion, 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.

122. Are all operating systems and firmware on your devices supported by a supplier that produces regular fixes for any security problems? Please list any operating systems that are not supported.

[Notes]

123. Are all applications on your devices supported by a supplier that produces regular fixes for any security problems? Please list any applications that are note supported.

[Notes]

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

[Notes]

125. 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.

[Notes]

126. 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.

[Notes]

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

[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.

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

[Notes]

129. 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.

[Notes]

130. Where personal data is in use, do you ensure that a privacy impact assessment is carried out for new systems and projects?

[Notes]

131. Are changes to information systems, applications or networks reviewed and approved? Describe the approval process.

[Notes]

132. 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.

[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.

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

[Notes]

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

[Notes]

135. 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]

136. 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.

[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.

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

[Notes]

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

[Notes]

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

[Notes]

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

[Notes]

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

[Notes]

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

[Notes]

143. 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.

[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.

144. 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 (ie using an App Store or application whitelisting) or

C - application sandboxing (ie by using a virtual machine)?

[Notes]

145. 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.

[Notes]

146. 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?

[Notes]

147. 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 do not allow you to install unsigned applications. Usually you have to "root" or "jailbreak" a device to allow unsigned applications.

[Notes]

148. 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?

[Notes]

149. 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 to download for free from the internet. You can also use a continuous vulnerability scanning tool to monitor your ongoing vulnerabilities. Please note that we do not endorse any particular product.

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

[Notes]

151. 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 the information safety policies that you have set - and how you will identify any unacceptable aspects.

152. Does the organisation regularly review event logs?

[Notes]

153. Is an audit trail of system access and/or data use by staff maintained and reviewed on a regular basis? Describe how you achieve this.

[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.

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

[Notes]

155. Are all backups secured with an appropriate level of protection for the type of data they contain?

[Notes]

156. Is a backup copy held in a different physical 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.

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

[Notes]

158. 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)?

[Notes]

159. What is your process for reporting losses of personal data to the Information Commissioner (or your national data protection authority) and the data subjects?

[Notes]

160. Are information security incidents investigated to establish their cause and impacts with a view to avoiding similar events?

[Notes]

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

[Notes]

162. Is a record kept of the outcome of all security incident investigations?

[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.

163. Does the organisation ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks?

[Notes]

164. Does the organisation review the business continuity and disaster recovery plans at least once per year and who is involved in the review?

[Notes]

165. Does the organisation exercise the business continuity and disaster recovery plans at least once per year?

[Notes]

Insurance

All organisations with a head office domiciled in the UK that have the whole company in scope and a turnover of < £20m 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.

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

The answer to this question is just for information and, if you are eligible for the insurance and opt in, will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

If you have answered "yes" to the last question, then your company is eligible for the included cyber insurance if you gain certification. The cost of the insurance is included in the cost of the assessment

167. Do you want to accept this cyber insurance?

The answer to this question is just for information and, if you are eligible for the insurance and opt in, will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

168. What is your total gross revenue?

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

[Notes]

169. 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 is just for information and will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

170. 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 is just for information and will be passed to the Insurance Broker in association with the Cyber Insurance you will receive at certification.

[Notes]

171. 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]

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.