Intr

Cyber Essentials and IS
info@nethostlegisl

NetHost Legislation is providing this free Cyber Essent
Security polices templates towards

Policy Templates
Access Control Policy
Anti Malware Policy
BYOD Hand-Held Device Policy
Clear Desk and Screen Policy
Electronic Mail Policy
Firewall and Router Policy
Information Security Policy
Information System Risk Management Policy
Internet Usage Policy
Mobile Device Policy
Secure File Transfer Policy
Password Policy
Remote Access Policy
Security Awareness Policy
System Configuration Policy
Wireless Access Policy

Cyber Essentials aims to help organisations i
their customers that they take cyber securit
available at two levels:

• **Cyber Essentials (£300 + vat)** - an indeper
five basic security controls and a qualified as
• **Cyber Essentials PLUS (£1000 per day)** – a
the same five controls, testing that they wo
£1500 from the UK goverment towards cer

The five basic controls within Cyber Essentia
protect against unskilled internet-based atta
internet.

Organisations that undertake Cyber Essentia
progress their security.
Since 1 October 2014, Cyber Essentials beca
(https://www.gov.uk/government/publicati

For further information please see www.cyb

NetHost Legislation
SO Management System Certification Company
lation.co.uk, www.nethostlegislation.co.uk

tials toolkit support SMEs complaince with the standard. This toolkit includes 16 Cyber
; and 9 free tools to validate/anwer Cyber Essentials requirements,

implement basic levels of protection against cyber attack, demonstrating to
y seriously. The scheme is

ndently verified self assessment. Organisations assess themselves against
ssessor verifies the information provided.
a higher level of assurance. A qualified and independent assessor examines
rk in practice by simulating basic hacking and phishing attacks. ***Claim back***
tifiying against Cyber Essentials

als were chosen because, when properly implemented, they will help to
ackers using commodity capabilities – which are freely available on the

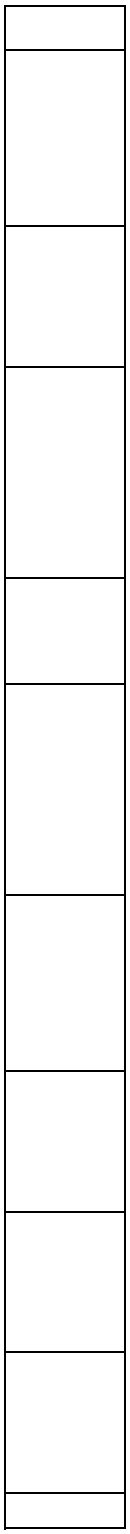
als are encouraged to recertify at least once a year and, where appropriate,

me a minimum requirement for bidding for some government contracts
ons/procurement-policy-note-0914-cyber-essentials-scheme-certification

berstreetwise.com\cyberessentials

Free tools to support Cyber Essentials Compliance

Index	Tool Name	Tool Describtion
1	**Password Meter** - http://www.passwordmeter.com/	*This application is designed to assess the strength of password strings. The instantaneous visual feedback provides the user a means to improve the strength of their passwords, with a hard focus on breaking the typical bad habits of faulty password formulation.*
2	**Is your email account compromised-** https://haveibeenpwned.com/	*A free resource for anyone to quickly assess if they may have been put at risk due to an online account of theirs having been compromised or "pwned" in a data breach*
3	**Microsoft Baseline Security Analyzer 2.3-** https://www.microsoft.com/en-gb/download/details.aspx?id=7558	*The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations*
4	**VeraCrypt-** https://veracrypt.codeplex.com/	*VeraCrypt is an open-source utility used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition.*
5	**Kali**- https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/	*A free security assessment tool used for penetration testing, vulnerability scans and others*
6	**Online Port Scanner** - https://hidemy.name/en/ports/	*Online Port scanner shows which ports are open on your (or someone else's) computer and what they are accountable for. Verification is performed via the scanner nmap, and shows the extend to which your PC is open to the outside world*
7	**nmap**- https://nmap.org/	*Nmap is a tool that can be used to discover services running on Internet connected systems. Nmap is related to vulnerability assessment tools, which test for common vulnerabilities in open ports*
8	**Router Checker**- https://campaigns.f-secure.com/router-checker/en_global/	*Router Checker is a free, web-based tool that checks your router's connection settings. If your router isn't configured to use an authorized DNS server, it might mean someone has modified it in order to hijack your Internet connection*
9	**IoTSeeker-** https://information.rapid7.com/iotseeker	*With this tool you can find out if you have connected "Things" which are using the default factory password leaving them potentially vulnerable to a hostile takeover*



Cyber Essentials Question

NetHost Legslation	Sub-Category	Question Number
	Your Organisation	
		1
		2
		3
		4
		5
		6
		7
	Scope of Assessment	

		8
		9
		10
		11
		12
		13
	Office firewalls and internet gateways.	

			14
			15
			16
			17
			18
			19
			20

		21
		22
		23
	Software firewalls	24
		25
	Secure configuration	

		26
		27
		28
		29
		30
		31
		32
		33
		34
		35

Patches and Updates	
	36
	37
	38
	39
	40
	41
User Accounts	

		42
		43
		44
		45
	Administrative Accounts	
		46
		47
		48
		49
		50
		51

		52
	Malware protection	
		53
		54
		55

		56
		57
		58
	Insurance	
		59

		60
		61
		62
		63
		64

naire Guide

Question or Description	Answer Guide
Please tell us a little about how your organisation is set up so we can ask you the most appropriate questions.	
What is your organisation's name (for companies: as registered with Companies House)	<< As you would like it displayed on your certificate>>
What is your organisation's registration number.	<< check company house-- >>https://beta.companieshouse.gov.uk/
What is your organisation's address (for companies: as registered with Companies House)	<<Full detail address including post code>> https://beta.companieshouse.gov.uk
What is your main business?	<< e.g. Provide financial software development for banks in UK>>
What is your website address?	<< main website site address>>
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*	Micro or Small or Medium or Large
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*	<< permanent home workers>>
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"	<< the scope should include areas of your network that actually process sensitive data. In most cases the scope is the entire network unless segmentation is applied>>

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.	**Acceptable answer is Yes** << in most cases the whole organisation is the scope>>
If it is not the whole organisation, then what is the scope description you would like to appear on your certificate and website?	<< e.g. the software development and supporting infrastructure that reside at …>>
Please describe the geographical locations of your business which are in the scope of this assessment	<< a detail address>>
Please describe 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***	<< include equipment type, purpose and department >>
Please describe the networks that will be in the scope for this assessment (such as office network, home offices and firewalls)	<<if you do not have segmentation in place, then it is just 1 corporate network>>
Who is responsible for managing the information systems in the scope of this assessment?	< name and title>
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**	**FREE Tools to support** 1-Password Meter - http://www.passwordmeter.com/ 2-Is your email account compromised- https://haveibeenpwned.com/ 3-Microsoft Baseline Security Analyzer 2.3- https://www.microsoft.com/en--gb/download/details.aspx?id=7558 4-VeraCrypt- https://veracrypt.codeplex.com/ 5-IoTSeeker- https://information.rapid7.com/iotseeker 6-Kali- https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/ 7-Online Port Scanner - https: //hidemy.name/en/ports/ 8-nmap- https://nmap.org/ 9-Router Checker- https://campaigns.f-secure.com/router-checker/en_global/

Do you have firewalls at the boundary 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.*	**Acceptable answer is Yes-** << Your ISP router will include a firewall and also your laptops/workstations could also have firewall installed, logging in and check>>
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?	**Acceptable answer is Yes-**<< You can check by logging into the router and changing the password. Alternatievly speak to your ISP for advise>
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"*	**Acceptable answer is Yes-**<<You can check by loggin into the firewall or device and changing the password>>
Do you change the password when you believe it may have been compromised?	**Acceptable answer is Yes-**<< You should, and at regular intervals - 90 days>> Free Cyber Essentials password policy template covers this issue
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*	**Acceptable answer could be Yes (we have approved business case or No, we have not opened any ports.**<<The business case can be in email format justifying why the firewall service is opened>> If you have not enable any service the answer is no, but you to explain this in the note section.
If yes to above, do you have a process to ensure they are disabled in a timely manner when they are no longer required?	**Acceptable answer is Yes** << Check the firewall or router enabled services and disable services not in use>> All business cases should have a time limit specified to disable firewall opened service ports
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*	**Acceptable answer is Yes-**<< use the free nmap tool to check>> Free Cyber Essentials firewall and router policy template cover this issue.

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.*	**Acceptable answer is N0, thus you do not allow remote connection or you use VPN** << log into the firewall and check>>
If yes, is there a documented business requirement for this access?	**Acceptable answer is Yes** << Free Cyber Essentials Information Security policies template provided covers this risk>>
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?	**Acceptable answer is Yes** << logging in and check>>
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"*	**Acceptable answer is Yes** << logging in and check>>
If no, is this because software firewalls are not commonly available for the operating system you are using?	**Accpetable answer is Yes,** << confirm a risk assessment was carried out and approved>>
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**	Free tools to support 1-Password Meter - http://www.passwordmeter.com/ 2-Is your email account compromised- https://haveibeenpwned.com/ 3-Microsoft Baseline Security Analyzer 2.3- https://www.microsoft.com/en--gb/download/details.aspx?id=7558 4-VeraCrypt- https://veracrypt.codeplex.com/ 5-IoTSeeker- https://information.rapid7.com/iotseeker 6-Kali- https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/ 7-Online Port Scanner - https: //hidemy.name/en/ports/ 8-nmap- https://nmap.org/ 9-Router Checker- https://campaigns.f-secure.com/router-checker/en_global/

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? *This includes applications, system utilities and network services*	**Acceptable answer is Yes.** << use the free tools to check>>
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?	**Acceptable answer is Yes.** << use the free tools to check>>
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?	**Acceptable answer is Yes.** << use the free tools to check>>
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.*	**Acceptable answer is Yes.** << use the free tools to check>>
Do you run software that provides sensitive or critical information (that shouldn't be made public) to internet-based users?	**Acceptable answer could either be Yes or No**, depending on your business process
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?	**Acceptable answer is Yes.** << use the free tools to check>>
If yes, you ensure that you change passwords if you believe that they have been compromised?	**Acceptable answer is Yes.** << Fee Cyber Essentails Password and Access Acount policies template cover this issues >>
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?	**Acceptable answer is Yes.** << Free Cyber Essentials Password and Access Account policies template cover this issues >>
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.*	**Acceptable answer is Yes.** << Free Cyber Essentials Password and Access Acount policies template cover this issues >>
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*	**Acceptable answer is Yes.** << Use the free tools to check>>

To protect your organisation, you should ensure that your software is always up-to-date with the latest software 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**	Free tools to support 1-Password Meter - http://www.passwordmeter.com/ 2-Is your email account compromised- https://haveibeenpwned.com/ 3-Microsoft Baseline Security Analyzer 2.3- https://www.microsoft.com/en--gb/download/details.aspx?id=7558 4-VeraCrypt- https://veracrypt.codeplex.com/ 5-IoTSeeker- https://information.rapid7.com/iotseeker 6-Kali- https://www.kali.org/penetration-testing/openvas-vulnerability-scanning/ 7-Online Port Scanner - https: //hidemy.name/en/ports/ 8-nmap- https://nmap.org/ 9-Router Checker- https://campaigns.f-secure.com/router-checker/en_global/
Are all **operating systems** and **firmware** on your devices supported by a supplier that produces regular fixes for any security problems?	**Acceptable answer is Yes.** << Free Cyber Essential policies template cover this issues and free tools can be used to checked operating system and firmware >>
Are all **applications** on your devices supported by a supplier that produces regular fixes for any security problems?	**Acceptable answer is Yes.** << Free Cyber Essential policies template cover this issues and free tools can be use to checked operating system and firmware >>
Is all software licensed in accordance with the publisher's recommendations?	**Acceptable answer is Yes.** << Free Cyber Essential policies template cover this issues >>
Are all high-risk or critical security updates for operating systems and firmware installed within 14 days of release?	**Acceptable answer is Yes.** << Cyber Essential policies template cover this issues >>
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?	**Acceptable answer is Yes.** << Cyber Essential policies template cover this issues >>
Do you have any applications on any of your devices that are no longer supported and no longer received regular fixes for security problems?	**Acceptable answer is Yes.** << Cyber Essential policies template cover this issues and the free tools provided can be use to check >>
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**	<<Free Cyber Essentials policies template provided will cover this section>>

Are users only provided with user accounts after a process has been followed to approve their creation?	**Acceptable answer is Yes.** <<Free Cyber Essentials Information Security policy template covers this issue>>
Can you only access laptops, computers and servers in your organisation (and the applications they contain) by entering a unique user name and password?	**Acceptable answer is Yes.** <<Free Cyber Essentials Information Security policy template covers this issue>>
Have you 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.*	**Acceptable answer is Yes.** <<Free Cyber Essentials Information Security policy template covers this issue>>
Do you ensure that staff only have the privileges that they need to do their current job? *When a staff member changes job role you may also need to change their access privileges*	**Acceptable answer is Yes.** <<Free Cyber Essentials Information Security policy template covers this issue>>
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**	<<Free Cyber Essentials policies template provided will cover this section>>
Do you have a formal process for giving someone access to systems at an "administrator" level?	**Acceptable answer is Yes.** <<Free Cyber Essentials Access Control policy template covers this issue>>
Do you ensure that staff only use administrator accounts to carry out administrative activities (such as installing software or making configuration changes)?	**Acceptable answer is Yes.** <<Free Cyber Essentials Access Control policy template covers this issue>>
Do you ensure that administrator accounts are not used for accessing email or web browsing?	**Acceptable answer is Yes.** <<Free Cyber Essentials Access Control policy template covers this issue>>
Do you formally track which users have administrator accounts in your organisation?	**Acceptable answer is Yes.** <<Free Cyber Essentials Access Control policy template covers this issue>>
Do you review who should have administrative access on a regular basis?	**Acceptable answer is Yes.** <<Free Cyber Essentials Access Control policy template covers this issue>>
Have you enabled two-factor authentication for access to all administrative accounts?	**Acceptable answer is Yes.** <<Free Cyber Essentials Access Control policy template covers this issue>>

If no, is this because two-factor authentication is not available for some or all of your devices or systems?	**Acceptable answer is Yes.** <<Free Cyber Essentials Access Control policy template covers this issue>>
Malware (such as computer viruses) are 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**	<<Free Cyber Essentials policies template provided will cover this section>>
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)? *Its usually easiest to protect computers and laptops from malware by using A - Anti-Malware software. Tablets and mobile phones are usually protected using B - App Store / Application Whitelisting. Application sandboxing (option C) is a way of running an application in a secure manner that blocks the application from accessing many of the usual functions of the computer, such as its data, its peripherals and the network.*	**Acceptable answer is Yes.** <<Free Cyber Essentials Anti-Malware policy template covers this issue>>
(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.	**Acceptable answer is Yes.** <<Free Cyber Essentials Anti-Malware policy template covers this issue>>
(A) Where you have anti-malware software installed, is it set to scan web pages you visit and warn you about accessing malicious websites?	**Acceptable answer is Yes.** <<Free Cyber Essentials Anti-Malware policy template covers this issue>>

(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*	**Acceptable answer is Yes.** <<Free Cyber Essentials Anti-Malware policy template covers this issue>>
(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?	**Acceptable answer is Yes.** <<Free Cyber Essentials Anti-Malware policy template covers this issue>>
(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? I*f you are using a virtual machine to sandbox applications, you can usually set these settings within the configuration options of the virtual machine software.*	**Acceptable answer is Yes.** <<Free Cyber Essentials Anti-Malware policy template covers this issue>>
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.	The cover, underwritten by AIG; and the policy provides the following: **Event Management** - Legal, IT Forensics, Data Restoration, Reputational Protection, Notification Costs and Credit and ID Monitoring services following an actual or suspected breach of personal or corporate information, an IT security or system failure **Data Protection Obligations** - Insurers will pay Defence Costs in respect of a Regulatory Investigation, and any lawfully insurable Data Protection Fines that the Company is legally liable to pay in respect of such Regulatory Investigation with regards to a breach of Data Protection Legislation **Liability -** Damages and Defence Costs arising from: An actual or alleged breach of data, an actual or alleged security failure, the failure to notify a Data Subject and/or any Regulator of a breach of personal information in accordance with the requirements of Data Protection Legislation, an actual or alleged breach of duty by the Information Holder in respect of the processing information (for which the Company is responsible) on behalf of the Company
Is your head office domiciled in the UK and is your gross annual turnover less than £20m?	<< Accpetable answer is Yes to to be eligible for the insurance cover>>

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/cyber essentialsprofile/automatic-insurance-cover.*	<< Yes or No>>
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*	<< To be eligible for the defualt insurance cover your turnover should be less than 20 Million GBP>>
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*	<< check the FCA website- https://www.fca.org.uk>>
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*	<< Yes or No>>
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.*	<<email address>>