

July 2022

Report for the National Cyber Security Centre (NCSC) on
'Cyber Essentials: Requirements for IT Infrastructure' (v3)

A cyber crime against clarity: why the NCSC should revise its confusing guidance

by **Martin Cutts**

Director, Plain Language Commission

Author, 'Oxford Guide to Plain English'

Summary

The Cyber Essentials 'requirements' booklet is so unclear that it should be completely rewritten and redesigned using the principles of plain language and good typography.

The booklet is a masterpiece of jargon-strewn incoherence that seems to become more complex the more effort readers make to grasp what it means.

Confusion caused by the booklet is likely to have cost small firms about £40million in wasted time trying to gain Cyber Essentials certification this year.

After rewriting the booklet, the NCSC should conduct a genuine consumer-testing exercise and learn from the results to improve it further.

This report is addressed directly to the NCSC, a government body that is part of GCHQ (<https://www.ncsc.gov.uk>). It has not been commissioned by the NCSC.

PLAIN
LANGUAGE
COMMISSION

Plain Language Commission

The Castle, 29 Stoneheads

Whaley Bridge

Derbyshire SK23 7BB

Tel: +44 (0) 1663 733177

Web: www.clearest.co.uk

Plain Language Commission is a business, independent of government

Introduction

In March 2022, I sought your Cyber Essentials certification for my company. I'd been through a similar process in each of the last two years, but this year you had considerably increased your requirements and their complexity. It was thus hard to obtain certification without spending disproportionate time and effort.

Last year, the process took me two hours or so. This year, it took me at least 30 hours. I was impeded by the tortuous documents you had created for applicants to use. First, there was an application form where several of the questions were barely comprehensible. Then there was a guidance booklet that was badly written and poorly designed. Like a lot of muddled and jargon-infested English, it became more baffling the harder I tried to understand it. The booklet, called **Cyber Essentials: Requirements for IT Infrastructure** (version 3, Nov 2021), is the user's main source of help on completing the form. The certifying body I used was your contractor, IASME.

This report explains how the documents, particularly the booklet, offend against many of the principles of writing clear English which have become widely accepted in the UK's public services during the last 40 years. Plenty of good sources describe these principles, including my own 'Oxford Guide to Plain English' (v5, OUP, 2020).

This report says you should get the booklet rewritten, restructured and redesigned so that non-specialists may have a reasonable chance of understanding it without excessive effort.

You have not asked for or commissioned this report; I offer it in a friendly spirit as a gift.

Why the NCSC has a duty to be clear

Cyber Essentials certification is often demanded by government agencies and outsourcing companies like Capita, otherwise firms like mine cannot get government contracts and – even worse – are likely to lose the contracts they already have. Thus, firms are held to ransom: they must pay £300 to get certified, and they must undergo whatever process you choose to impose. Not being certified can easily cost tens of thousands of pounds in lost business, so a lot rides on our ability to convince the certifying body that we are compliant. This means we need to fully understand what we are being asked to do, otherwise we will fail the assessment and, if a re-submission also fails,

we must restart the process from scratch and pay another £300 fee.

As a government body, you have a duty to make your procedures and the related documents clear and easy for typical users. This duty has been well established since the Thatcher era. You have implicitly acknowledged it by publishing many excellent documents about cyber security on your website, eg the Cyber Security Small Business Guide (Oct 2020). Several of the documents you issue to schools seeking Cyber Essentials also make good efforts to explain your requirements. So, you can be clear when you try.

Your website says the NCSC 'understands cyber security, and distils this knowledge into practical guidance that we make available to all'. However, for it to be truly practical, the guidance must be as clear as possible to the vast majority of its intended readers.

IASME says that last year there were about 26,500 Cyber Essentials certifications, roughly two-thirds achieved by micro and small businesses. Let's make the reasonable assumption that the low quality of your Cyber Essentials documents this year will lead 26,500 firms to take an average of 15 extra hours each, at (say) £100/hour for a senior manager's time. This amounts to an extra cost of nearly £40million to such businesses, which seems an unacceptable level of futility and waste. You should aim to reduce this figure to almost zero.

Anguish, misery, rage and despair, however, fall outside any mere monetary calculation, and many small firms have felt all these emotions as they sought certification this year. Several have told me so. Lacking specialist help, they have often been flying blind.

I ended up trying to negotiate your contractor's uncomprehending and complacent complaints procedure – IASME seemed to think the documents were just fine. But there was little else I could do except use it, while burning ever more hours trying to construe the guidance and discern what precise tests of compliance IASME was applying.

Detailed comments on the guidance

To keep my comments brief and easy to use, I have shown many of them as annotations on the offending booklet that I attach as an appendix to this report. I hope you will find them fair and reasonable.

I have written the notes below in a direct style because, having spent so long trying to meet your requirements, I do not want to waste time

sugar-coating them. If you need more information, though, just ask.

These are the headline points for you to consider:

- 1** You need to use more **active-voice verbs**, so that in most sentences you put an identifiable agent (or 'doer') before the verb it governs. Comprehension research (and common sense) shows this helps readers a lot.
- 2** You need to use more **personal pronouns**, such as 'we', 'our', 'you' and 'your'. It is verbose to keep using terms like 'the applicant organisation' and 'the applicant' when you could use 'you'; it also militates against readability. Again, this is borne out by research. The document should not read like some old-fashioned scientific report, straining to sound lofty and detached by overusing passive voice without pronouns. Users want to know who is speaking and what they are saying. So use a simple writing style that is aimed directly at us from you.
- 3** You need to put yourself in the typical user's shoes, which means you need to **explain technical stuff properly and pre-test the text with typical users**. By typical users, I do not mean experts in digital and cyber technology. I mean a range of small-business users including plenty who are not digital natives or millennials. Most small firms cannot afford to outsource certification to an IT consultant. And outsourcing may also, perversely, harm their security. As the poet said: 'Quis custodiet ipsos custodes?'

A good way of conducting proper consumer testing is for you to ask users to answer questions based on your documents and see (a) how long it takes them to locate the answers, and (b) how often they get the answers right. Another way is to get them to underline anything they don't understand. This can be painful and humbling to witness but can yield priceless insights.

- 4** You need to organize the booklet properly, so that you create a **clear access structure and an obvious hierarchy of headings**. The current contents page does not even have page numbers. There are no section numbers or paragraph numbers either, so if I wanted to talk to other people about points in the text, I first had to ask them to number the booklet pages by hand, then refer to a heading by name, and then quote them a line number or a particular sentence. This typographical obscurity also means that a question on the form cannot concisely refer users to the parts of

the booklet where they might find help to get the answer.

- 5 Your sentences need to be as short as they can sensibly be. Full stops are the reader's friend because they help you give us the facts in small, easily digestible doses. We are reading your booklet not to take pleasure in its literary merit but because we want to find the answers to the form's questions. So an average sentence length of 15–20 words would be best. Readers may be bemused by a 39-word sentence in technical language like this from the guidance:

'Where the cloud provider implements a control, the applicant must satisfy themselves that this has been done by the cloud provider committing to implementation within contractual clauses or documents referenced by contract, such as security statements or privacy statements.'

We won't be offended or patronized by simplicity, and nobody will ever complain that your booklet is just too clear. Those who already know what you are talking about will skip the easiest bits anyway.

- 6 **Don't allow experts to write your guidance unchallenged.** All experts suffer from the curse of knowledge. They find it hard to imagine what the uninitiated will have difficulty understanding. If you do have to use technical experts as authors, make sure they are overseen by good writers and usability specialists who know how to edit, check and user-test what they produce. That way, you are far less likely to produce a jargon-infested document. Remember that undergoing certification is unlikely to be the highlight of our lives. We want to do it once a year, forget about it, then spend the other 364 days sipping the nectar of life.

- 7 Here is an example of **appalling text** from the application form:

'The use of a PIN with a length of at least six characters can only be used where the credentials are used solely to unlock a device and does not provide access to organisational data and services without further authentication.'

I pointed out to IASME that this made no sense. It is ungrammatical (what is the subject of the verb 'does not provide'?). It overuses truncated passive-voice verbs (ie, no doers), making it opaque. If you start a sentence with 'The use of a PIN... can only be used', everyone knows it will be a disaster because it is tautologous.

I asked IASME to explain what the sentence meant. IASME was unwilling or unable to do so, perhaps realizing it was gibberish. I asked IASME to ask you, the authors, what it meant. IASME chose not to do so and suggested I engage an IT professional to make

sense of your form and booklet and help me through the process. This was an impractical suggestion given the likely expense, the difficulty of finding a competent person, and the haste I needed to employ (firms normally have two days for their re-submission after failing the first assessment).

IASME opined that the text must be clear because the NCSC had decreed it so. It was 'easy to understand', IASME implied:

'Wording of Cyber Essentials is approved by the National Cyber Security Centre. As such we are unable to rewrite text... The document referred to is an NCSC owned document and is written and approved by the relevant Subject Matter Experts prior to being sent through [to] the NCSC's technical writer to make sure it is correctly worded and easy to understand.'

When I asked IASME to explain in writing a section in the guidance about 'Device unlocking credentials', IASME would not do so. Eventually, after I'd complained to its chief executive, I was put on to a very helpful IASME specialist. He explained that the relevant requirement I was so concerned about (arising from question A5.11 on the form) had now been dropped. This meant I had spent several hours trying to disentangle a requirement that the NCSC had already consigned to the dustbin.

This episode highlights the need for you to ensure that, from the outset, your requirements are practical and not unduly onerous.

- 8** You need to ensure there is a connection between every question on the form and a clearly identified place in the booklet (or other source) where the user can get more information. In other words, **the form and booklet need to dovetail as one document.**

Recommendations

- 1** As you are asking firms to meet high standards, you need to ensure that your own standards are beyond reproach. So your Cyber Essentials documents should be as lucid as you can make them.
- 2** You should not waste money consumer-testing the current form and booklet, because they are obviously very poor.
- 3** You should overhaul the form and booklet using a team that understands the principles of plain language and good typography.
- 4** You should thoroughly pre-test the new draft form and guidance, adjusting it in light of the results (specialist testing firms can help).

Appendix

The following pages show my detailed notes on the booklet 'Cyber Essentials: Requirements for IT Infrastructure'. The points are not meant to be exhaustive.



Cyber Essentials: Requirements for IT infrastructure

[The NCSC regularly addresses the reader as 'the applicant' or 'the applicant organisation' instead of 'you'. This makes the whole document clumsy and more difficult than it needs to be. Using personal pronouns like 'you', 'your', 'we' and 'our' also leads to other good writing habits, particularly the use of more active-voice verbs.

You could even use these ideas to rephrase the title, eg as 'Our requirements for your IT infrastructure' because this makes the title more specific. The requirements belong to NCSC, and the IT infrastructure belongs to the intended readers.]

Contents

What's new.....	4
Definitions.....	5
Scope.....	6
Overview of the scope.....	6
Bring your own device (BYOD).....	7
Home working.....	8
Wireless devices.....	8
Externally managed services – cloud.....	8
Externally managed services – other.....	10
Web applications.....	10
Requirements, by technical control theme.....	10
Firewalls.....	10
Objective.....	10
Introduction.....	10
Requirements under this technical control theme.....	11
Secure configuration.....	12
Objective.....	12
Introduction.....	12
Requirements under this technical control theme.....	13
User access control.....	14
Objective.....	14
Introduction.....	14
Requirements under this technical control theme.....	15
Malware protection.....	17
Objective.....	18
Introduction.....	18
Requirements under this technical control theme.....	18
Security Update management.....	19
Objective.....	20

[The contents list gives page numbers but the pages don't actually have page numbers. There are no section or paragraph numbers either. These would help users to discuss the topics easily among colleagues or refer to sections easily. Ease of use and ease of reading are twin essentials.]



Security Update management
Objective

[Why is the 'u' capped here? Why is the 'g' capped on the next page? Readers need to feel they are in the hands of competent authors who take care with wording and typography. After all, this is a certification process.]



Introduction.....20

Requirements under this technical control theme.....20

Further Guidance.....22

Back up your data.....22

[Why no heading here? Why isn't the document organized under these five control themes? After all, the reader is urged to 'proceed' by using these themes – see the 'Proceed as follows' note 2 below. A heading would enable this little section to appear in the Contents list]

We specify the requirements under five technical control themes:

- firewalls
- secure configuration
- user access control
- malware protection
- security update management

[starting on page x]

[Use of 'you'. So why is it so little used elsewhere in this doc?]

As a Cyber Essentials scheme applicant, you must ensure that your organisation meets all the requirements. You may also be required to supply various forms of evidence before your chosen Certification Body can award certification at the level you seek.

Proceed as follows:

1. Establish the **boundary of scope** for your organisation and **determine what is in scope within this boundary.**
2. Review each of the five **technical control themes** and the **controls they embody as requirements.**
3. Take steps as necessary to **ensure that your organisation meets every requirement**, throughout the scope you have determined.

[It's so much simpler if you use the words 'we' and 'you' to immediately identify the actors in the sentences]

[Who are the 'doers' in this sentence? Double passive voice.]

What's new

- Added a home working requirement and information on how this is to be included in the scope of certifications.
- All cloud services are now in scope, added definitions and a shared responsibility table to assist with this.
- Extended the multi-factor authentication requirement in relation to cloud services.
- Updated the password-based authentication requirement and added a new section on multi-factor authentication. This requirement has also been moved to the 'user access' control.
- Thin clients are now in scope and added to the 'devices' definition.
- Added a new device unlocking requirement to the 'secure configuration' control.

[Not explained hereabouts, yet crucial.]

[Multi-word prepositions are usually poor style. Use 'on'.]

[Why avoid stating the doer here? It's so much harder to read sentences that lack doers]

[Why not use 'our' not 'the'? Easier to grasp!]

[Most of these statements would be simpler to construe if they began with 'We'. This is a basic technical-writing idea.]

[This means 'We have added'. Readers have to add their own words to make sense of it, meaning they have to stop and re-read]

[This and bullet 5 break the parallel structure by being full sentences, though this bullet is poorly constructed. What is the grammatical subject of 'added definitions and a shared responsibility table'?]

[What are 'thin clients'? Not listed among the definitions overleaf.]

[Why put the participle 'added' so late when most of the other participles are ranged in parallel structure at the front?

[What does this really mean? It is too compressed to be understandable at first reading. Does it mean, eg, 'We have made clear that you must always treat 'end user devices' [unexplained term] as in scope.'?

- Added a new statement clarifying the inclusion of end user devices in the scope of certifications.
- Further information on unsupported applications added to the 'security update management' control.
- Removed specific 'email, web, and application servers' from control definitions and replaced with 'servers'.
- Updated the bring your own device (BYOD) section.
- Updated the wireless devices section.
- Added a new 'servers' definition.
- Added a new 'sub-set' definition and information on its impact on the scope.
- Added a new 'licensed and supported' definition.

[This 'what's new' section is a long list of points that isn't organized in any coherent way. Could the authors have grouped like with like, perhaps under subheads? The section assumes a lot of prior knowledge. Many users are unlikely to remember much of what they did in last year's certification, so will find it hard to associate these points with anything in their knowledge bank. The section is so long that it more or less means 'we've changed almost all the sections in some way, so you'll have to read them all thoroughly.']

[Insert 'you,']

Definitions

- **Software** includes operating systems, commercial off-the-shelf applications, plug-ins, interpreters, scripts, libraries, network software and firmware.
- **Devices** includes all types of hosts, networking equipment, servers, networks, and end user devices such as desktop computers, laptop computers, thin clients, tablets and mobile phones (smartphones) – whether physical or virtual.
- **Applicant** means the organisation seeking certification, or sometimes the individual acting as the main point of contact, depending on context.
- A **corporate VPN** is a Virtual Private Network solution that connects back to the applicants office location or to a virtual/cloud firewall. This must be administered by the applicant organisation so that the firewall controls can be applied.
- **Organisational data** includes any electronic data belonging to the applicant organisation. For example, emails, office documents, database data, financial data.

[By using the word 'your', the authors would avoid apostrophe mistakes like this, which are regrettably common in NCSC documents.]

[This sentence is a classic case where the authors should use the word 'you', eg 'You must administer the VPN so that you can apply the firewall controls.'

[Here, you give an initial cap to Cloud but earlier you don't do this. Different capping often implies different meanings. Quality control?]

[Insert 'that you own or subscribe to'. Why do the authors insist on using the wordy phrase 'applicant organisation' when they have already gone to the trouble of saying that 'applicant' means 'you'?]

- **Organisational service** includes any software applications, Cloud applications, Cloud services, User Interactive desktops and Mobile Device management solutions owned or subscribed to by the applicant organisation. For example: Web applications, Microsoft Office 365, Google Workspace, Mobile Device Management containers, Citrix Desktop, virtual desktop solutions, IP telephony.
- A **sub-set** is defined as a part of the organisation whose network is segregated from the rest of the organisation by a firewall or VLAN.
- **Servers** are specific devices that provide organisational data or services to other devices as part of the business of the applicant.
- **Licensed and supported software** is software that you have a legal right to use and that a vendor has committed to support by providing regular updates (patches). The vendor must provide the future date when they will stop providing updates. The vendor does not have to be the original creator of the software, but they must have the ability to modify the original software to create updates.

[English enables people to write 'applicant's business' or 'your business', instead of this kind of wordy phrase.]

[This is a definitions section, so just say 'means']

'software's original creator']

Overview of the scope

Assessment and certification should cover the whole of the IT infrastructure used to perform the business of the applicant, or if necessary, a well-defined and separately managed sub-set. Either way, the boundary of the scope must be clearly defined in terms of the business unit managing it, the network boundary and physical location. The scope must be agreed between the applicant and the Certification Body before assessment begins.

[Desperate need for the active voice here and throughout, eg: 'you must define...']

A sub-set can be used to define what is **in scope** or what is **out of scope** for Cyber Essentials.

[The authors regularly use this dreadful phrase 'boundary of the scope'. Yet they also use 'scope' on its own, which is adequate because 'scope' includes the idea of 'boundary'. This kind of tautology should have been weeded out during a quality check. But did the NCSC do a quality check?]

Information Organisations that choose a scope that includes the whole IT infrastructure achieve the best protection and increase customer confidence.

[What is the mechanism for agreeing this in advance as decreed here? Or is it nonsense, because we just state the scope on the application form?]

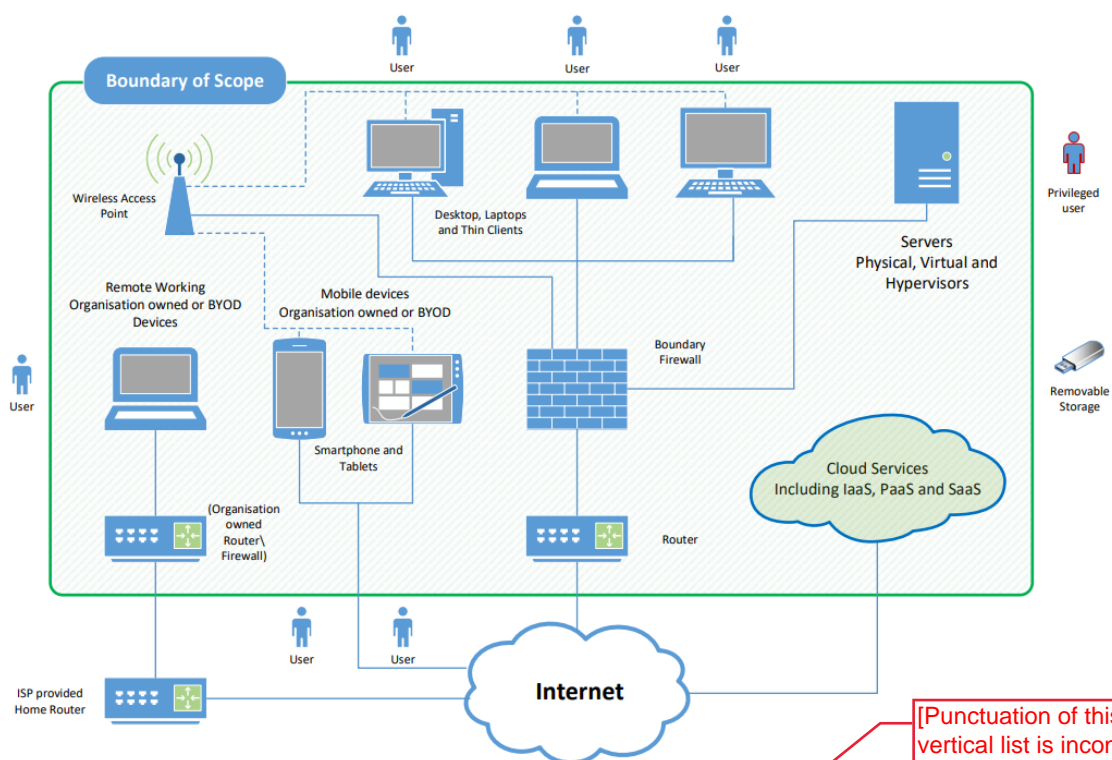
The requirements apply to all the devices and software that are within the boundary of the scope and that meet the any of these conditions:

[typo]

- can accept incoming network connections from untrusted internet-connected hosts; or
- can establish user-initiated outbound connections to devices via the internet; or
- control the flow of data between any of the above devices and the internet.

A scope that does not include end user devices is not acceptable.

Figure 1: Scope of the requirements for IT infrastructure -



Bring your own device (BYOD)

In addition to mobile or remote devices owned by the organisation, user-owned devices which access organisational data or services (as defined above) are in **scope**. However, all mobile or remote devices used **only** for the purpose of:

- native voice applications
- native text applications
- multi-factor authentication applications

are **out of scope**.

[Punctuation of this vertical list is inconsistent with the previous one. Quality control?]

[Do users know what 'native voice' and 'native text' mean? No explanation.]

[Hard to understand what readers are supposed to do with this information. The 'so what?' is missing here and in many other places, perhaps because the authors presume that the readers know. But they may well not know.]

Traditionally, user devices were managed through centralised administration, ensuring consistency across the organisation. In such cases, certification of the security controls is straightforward as there will be a standard build or reference to assess.

BYOD complicates matters, as users are given more freedom to 'customise' their experience making consistent implementation of the controls more challenging. Using the organisational data and services definitions to enforce strong access policies should remove some of this ambiguity.

Home working

[Use 'Our' or 'Your' so that the readers know immediately who owns this so-called 'default approach'.]

The default approach is that all corporate or BYOD home working devices used for applicant business purposes within the home location are **in scope** for Cyber Essentials.

Internet Service Provider (ISP) routers and user provided routers are **out of scope** which means that the Cyber Essentials firewall controls need to be applied on the user devices (e.g. a software firewall).

If a router is supplied to the home worker by the applicant organisation, then that router will be **in scope**.

[This is a dire noun string. Use 'your purposes'.]

If the home worker is using a corporate VPN, their internet boundary is on the company firewall or virtual/cloud firewall.

[Use active voice, eg 'you need to apply'.]

Devices

Wireless devices (including wireless access points) are:

[English offers the admirably brief alternative 'at home'.]

- **in scope** if they can communicate with other devices via the internet
- **not in scope** if it is not possible for an attacker to attack directly from the internet (the Cyber Essentials scheme is not concerned with attacks that can only be launched from within the signal range of the wireless device)
- **not in scope** if they are part of an ISP router within the home location

Externally managed services – cloud

If the applicant's data or services are hosted on cloud services, then these services must be **in scope**.

[In English, people say 'If you give the home worker a router, it will be in scope.' (13 words not 20.)]

In cloud services **the applicant is always responsible** for ensuring all the controls are implemented, but some of the controls can be implemented by the cloud service provider. Who implements which control depends on the type of cloud service. We consider three different types of cloud service:

[Have users realistically any way of ensuring that cloud service providers do what they say they'll do?]

[This sentence seems deliberately Delphic. Does it mean: 'Even if your cloud service provider implements some controls, you are still responsible for ensuring that all the necessary controls are implemented.'?]

[Three uses of 'applicant' in this line of type. Use 'you'!]

- **Infrastructure as a Service (IaaS)** – the cloud provider delivers virtual servers and network equipment that are configured and managed by the applicant, much like physical equipment would be. Examples of IaaS include Rackspace, Google Compute Engine, or Amazon EC2.
- **Platform as a Service (PaaS)** – the cloud provider delivers and manages the underlying infrastructure, and the applicant provides and manages the applications. Examples of PaaS include Azure Web Apps and Amazon Web Services Lambda.
- **Software as a Service (SaaS)** – the cloud provider delivers applications to the applicant, and the applicant configures the services. The applicant must still take time to ensure the service is configured securely. Examples of SaaS include Microsoft 365, Dropbox, Gmail.

[In brief English, say 'but the table explains'.]

Who implements the controls will vary depending on the design of the cloud service used, but the table below is presented as a guide to who would typically be expected to implement each control:

Requirement	IaaS	PaaS	SaaS
firewalls	both applicant and cloud provider	cloud provider and sometimes also the applicant	cloud provider
secure configuration	both applicant and cloud provider	both applicant and cloud provider	both applicant and cloud provider
user access control	applicant	applicant	applicant
malware protection	both applicant and cloud provider	cloud provider and sometimes also the applicant	cloud provider
security update management	both applicant and cloud provider	both applicant and cloud provider	cloud provider

[Use 'you' throughout the table]

Where the cloud provider implements a control, the applicant must satisfy themselves that this has been done by the cloud provider committing to implementation within contractual clauses or documents referenced by contract, such as security statements or privacy statements. Cloud providers will often explain how they implement security in documents published in their trust centres, which will include reference to a 'shared responsibility model'.

[Dreadfully obscure sentence.]

[How much time does the NCSC think users will have to waste mulling the implications of this obscure requirement?]

Externally managed services – other

Where the applicant is using other externally managed services (such as remote administration) it may not be possible for the applicant to meet all the requirements directly. The applicant may **choose** whether or not to include these services within the boundary of scope, according to feasibility.

If included, then the applicant must be able to attest that the requirements that are outside of the applicant's control are being adequately met by the service provider. Existing evidence may be considered (such as that provided through PCI certification of a cloud service, and ISO 27001 certifications that cover an appropriate scope).

[It is obvious that 'you' and 'your' should be used throughout this section to remove some of the wordiness.]

Web applications

Commercial web applications created by development companies (rather than in-house developers) and which are publicly accessible from the internet are **in scope** by default. Bespoke and custom components of web applications are **not in scope**. The primary mitigation against vulnerabilities in such applications is robust development and testing in line with commercial best practices, such as the Open Web Application Security Project (OWASP) standards.

Requirements, by technical control theme

Firewalls

[Poor typography. This is meant to be a theme heading but looks inferior to the bold black of, eg, 'Applies to' and 'Objective'. Action needed: NCSC should re-assess heading values throughout]

Applies to: boundary firewalls, desktop computers, laptop computers, routers, servers, IaaS, PaaS, SaaS.

Objective

Ensure that only safe and necessary network services can be accessed from the internet.

Introduction

[Why is this sitting on its own, separated from the text beneath? Poor typography. Lack of quality control by NCSC.]

All devices run network services, which create some form of communication with other devices and services. By restricting access to these services, you reduce your exposure to attacks. This can be achieved using firewalls and equivalent network devices, or data flow policies in cloud services.

[You can do this by...]

A boundary firewall is a network device which can restrict the inbound and outbound network traffic to services on its network of computers and mobile devices. It can help protect against cyber attacks by implementing restrictions, known as 'firewall rules', which can allow or block traffic according to its source, destination and type of communication protocol.

Alternatively, where an organisation does not control the network a device is connected to, a software firewall must be configured on a device. This works in the same way as a boundary firewall but only protects the single device on which it is configured. This approach can provide for more tailored rules and means that the rules apply to the device wherever it is used. However, this increases the administrative overhead of managing firewall rules.

[you must configure]

[if you do not control]

Information Most desktop and laptop operating systems now come with a software firewall pre-installed, we advise that these are turned on in preference to a third-party firewall application.

Requirements under this technical control theme

[Bad punctuation: this comma is not adequate to hold a sentence break. Use a semicolon or full stop, and restart with 'y/You should switch it on...']

Every device that is in scope must be protected by a correctly configured firewall (or equivalent network device).

[You must protect every in-scope device...]

For all firewalls (or equivalent network devices), the applicant organisation must routinely:

- change any default administrative password to an alternative that is difficult to guess (see password-based authentication) – or disable remote administrative access entirely
- prevent access to the administrative interface (used to manage firewall configuration) from the internet, unless there is a clear and documented business need and the interface is protected by one of the following controls:
 - multi-factor authentication (see MFA details below)

[you]

- an IP allow list that limits access to a small range of trusted addresses combined with a properly managed password authentication approach
- block unauthenticated inbound connections by default
- ensure inbound firewall rules are approved and documented by an authorised individual; the business need must be included in the documentation
- remove or disable unnecessary firewall rules quickly, when they are no longer needed
- use a software firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots.

Secure configuration

Applies to: servers, desktop computers, laptop computers, tablets, mobile phones, thin clients, IaaS, PaaS, SaaS.

Objective

Ensure that computers and network devices are properly configured to:

- reduce the level of inherent vulnerabilities
- provide only the services required to fulfil their role

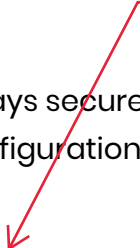
Introduction

Computers and network devices are not always secure in their default configurations. Standard, out-of-the-box configurations often include one or more weak points such as:

- an administrative account with a predetermined, publicly known default password or without multi-factor authentication enabled
- pre-enabled but unnecessary user accounts (sometimes with special access privileges)
- pre-installed but unnecessary applications or services

Default installations of computers and network devices can provide cyber attackers with a variety of opportunities to gain unauthorised access to an organisation's sensitive information – often with ease.

[Use the simpler word 'pre-set'.]



[This section is long and extraordinarily complex for non-specialists to disentangle and interpret. IASME repeatedly referred me to it as providing the explanation of a badly written question (A5.11) on the application form. Perhaps because of my protests at the meaningless and ungrammatical question, I was informed (towards the end of my struggle to gain certification) that the requirement set out in A5.11 had been dropped.]

By applying some simple technical controls when installing computers and network devices you can minimise inherent vulnerabilities and increase protection against common types of cyber attack.

Requirements under this technical control theme

Computers and network devices

The applicant must be active in its management of computers and network devices. It must routinely:

- remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)
- change any default or guessable account passwords (see password-based authentication)
- remove or disable unnecessary software (including applications, system utilities and network services)
- disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the internet)
- ensure authentication of users before allowing access to organisational data or services
- ensure appropriate device locking controls (see 'device locking', below) for physically present users.

Device unlocking credentials

Where a device requires the physical presence of a user to gain access to the services the device offers (e.g. laptop logon, mobile phone unlock) the user must unlock the device using a credential such as a biometric, password or PIN before gaining access to the services.

Biometric tests, passwords and PINs must be protected against brute-force attack by at least one of:

- 'throttling' the rate of attempts. This means the time the user must wait between attempts increases with each unsuccessful attempt. This should permit no more than 10 guesses in 5 minutes.
- locking devices after no more than 10 unsuccessful attempts

Technical controls must be used to manage the quality of credentials. If credentials are solely to unlock a device a minimum password or PIN length of at

[Suddenly, the applicant becomes 'it'. But the applicant is 'you'. The authors are in a muddle. Poor quality control again by NCSC.]

['the user's physical presence'. The possessive is one of the glories of English because it makes for concision. It's repeatedly avoided in this document.]

[Inconsistent list punctuation. Poor quality control by NCSC.]

['You must protect' or 'To protect against x, you must do y.']

least 6 characters must be used. When the device unlocking credentials are used elsewhere, then the full password requirements in 'user access control' must be applied to the credentials.

User access control

Applies to: servers, desktop computers, laptop computers, tablets, mobile phones, IaaS, PaaS, SaaS.

Objective

Ensure user accounts:

- are assigned to authorised individuals only
- provide access to only those applications, computers and networks actually required for the user to perform their role

Introduction

Every active user account in your organisation facilitates access to devices and applications, and to sensitive business information. By ensuring that only authorised individuals have user accounts, and that they are granted only as much access as they need to perform their role, you reduce the risk of information being stolen or damaged.

Compared to normal user accounts, accounts with special access privileges have enhanced access to devices, applications and information. When such accounts are compromised, their greater freedoms can be exploited to facilitate large-scale corruption of information, disruption to business processes and unauthorised access to other devices in the organisation.

'Administrative accounts' are especially highly privileged, for example. Such accounts typically allow:

- execution of software that has the ability to make significant and security relevant changes to the operating system
- changes to the operating system for some or all users
- creation of new accounts and allocation of their privileges

All types of administrator will have such accounts, including domain administrators and local administrators.

Now consider that if a user opens a malicious URL or email attachment, any associated malware is typically executed with the privilege level of the account that user is currently operating. Clearly, you must take special care over the allocation and use of privileged accounts.

Example

Jody is logged in with an administrative account. If Jody opens a malicious URL or email attachment, any associated malware is likely to acquire administrative privileges. Unfortunately, this is exactly what happens. Using Jody's administrative privileges, a type of malware known as ransomware encrypts all of the data on the network and then demands a ransom. The ransomware was able to encrypt far more data than would have been possible with standard user privileges, making the problem that much more serious.

[This is a clear and well-written paragraph.]

Requirements under this technical control theme

The applicant must be in control of its user accounts and the access privileges granted to each user account that has access to the organisation's data and services. Importantly, this includes accounts that third parties use for access, for example for device management or support services. It must also understand how user accounts authenticate and control the strength of that authentication. This means the applicant must:

- have a user account creation and approval process
- authenticate users before granting access to applications or devices, using unique credentials (see password-based authentication)
- remove or disable user accounts when no longer required (when a user leaves the organisation or after a defined period of account inactivity, for example)
- implement MFA where available. Authentication to cloud services must always use MFA.
- use separate accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)

[Here, 'It' means 'you'. Poor style. Inconsistency. Lack of quality control by NCSC.]

[MFA is used first on page 11 (4 pages before this). MFA is not used the first time 'multi-factor authentication' is used on page 4. Poor quality control.]

- remove or disable special access privileges when no longer required (when a member of staff changes role, for example)

Password-based authentication

All user accounts require the user to authenticate.

Where this is done using a password, the following protections should be used:

- Passwords are protected against brute-force password guessing by implementing at least one of:
 - using multi-factor authentication (see below)
 - 'throttling' the rate of attempts. This means the time the user must wait between attempts increases with each unsuccessful attempt. This should permit no more than 10 guesses in 5 minutes.
 - locking accounts after no more than 10 unsuccessful attempts
- Technical controls are used to manage the quality of passwords. This will include one of the following:
 - using multi-factor authentication (see below)
 - a minimum password length of at least 12 characters, with no maximum length restrictions
 - a minimum password length of at least 8 characters, with no maximum length restrictions and use automatic blocking of common passwords using a deny list.
- People are supported to choose unique passwords for their work accounts. This is enabled by:
 - educating people on how to avoid common or discoverable passwords, such as a pet's name, common keyboard patterns or passwords they have used elsewhere. This could include teaching people to use the password generator feature built into some password managers.
 - encouraging people to choose longer passwords. This can be done by promoting the use of multiple words (a minimum of three) to create a password, (e.g., 'Three Random Words')

- providing usable secure storage for passwords (for example a password manager or secure locked cabinet) with clear information about how and when it can be used.
 - not enforcing regular password expiry
 - not enforcing password complexity requirements
- There is an established process to change passwords promptly if the applicant knows or suspects the password or account has been compromised.

Multi-factor authentication (MFA)

As well as providing extra protection for passwords that are not protected by other technical controls (above), multi-factor authentication should always be used to provide additional protection to administrative accounts, and accounts that are accessible from the internet.

The password element of the multi-factor authentication approach must have a password length of at least 8 characters, with no maximum length restrictions.

There are four types of additional factor that may be considered:

- a managed/enterprise device
- an app on a trusted device
- a physically separate token
- a known or trusted account

Additional factors should be chosen so that they are usable and accessible. This may require user testing to verify if a factor is suitable for the users. For more information see the NCSC's guidance on MFA.

Information SMS is not the most secure type of MFA, but still offers a huge advantage over not using any MFA. Any multi-factor authentication is better than not having it at all. However, if there are alternatives ~~available~~ that will work for your use case, we recommend you use these instead of SMS.

Malware protection

Applies to: Servers, desktop computers, laptop computers, tablets, mobile phones, IaaS, PaaS, SaaS.

['MFA']

['your use case' is an astonishing phrase.]

['none']

Objective

Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

Introduction

The execution of software downloaded from the internet can expose a device to malware infection. Malware, such as computer viruses, worms and spyware, is software that has been written and distributed deliberately to perform malicious actions. Potential sources of malware infection include: malicious email attachments, downloads (including those from application stores), and direct installation of unauthorised software.

If a system is infected with malware, your organisation is likely to suffer from problems like malfunctioning systems, data loss, or onward infection that goes unseen until it causes harm elsewhere.

You can largely avoid the potential for harm from malware by:

- detecting and disabling malware before it causes harm (anti-malware)
- executing only software that you know to be worthy of trust (allow listing)
- executing untrusted software in an environment that controls access to other data (sandboxing)

Example

Acme Corporation implements code signing alongside a rule that allows only vetted applications from the device application store to execute on devices. Unsigned and unapproved applications will not run on devices. The fact that users can only install trusted (allow listed) applications leads to a reduced risk of malware infection.

Requirements under this technical control theme

The applicant must implement a malware protection mechanism on all devices that are in scope. For each such device, the applicant must use at least one of the three mechanisms listed below:

[Why are there 3 BOLD blue subheadings here that have a lower value in the hierarchy than the ROMAN blue headings earlier? See the heading for 'Malware protection' 2 pages earlier. This is typographical mayhem that causes chaos to readers who are trying to understand the hierarchy.]

Anti-malware software

- The software (and all associated malware signature files) must be kept up to date, with signature files updated at least daily. This may be achieved through automated updates, or with a centrally managed deployment.
- The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder.
- The software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself).
- The software must prevent connections to malicious websites on the internet (by means of deny listing, for example) – unless there is a clear, documented business need and the applicant understands and accepts the associated risk.

Application allow listing

- Only approved applications, restricted by code signing, are allowed to execute on devices. The applicant must:
 - actively approve such applications before deploying them to devices
 - maintain a current list of approved applications Users must not be able to install any application that is unsigned or has an invalid signature.

Application sandboxing

- All code of unknown origin must be run within a 'sandbox' that prevents access to other resources unless permission is explicitly granted by the user. This includes:
 - other sandboxed applications
 - data stores, such as those holding documents and photos
 - sensitive peripherals, such as the camera, microphone and GPS
 - local network access

Security Update management

Applies to: servers, desktop computers, laptop computers, tablets, mobile phones, firewalls, routers, IaaS, PaaS, SaaS.

[Why cap U?]

Objective

Ensure that devices and software are not vulnerable to known security issues for which fixes are available.

Introduction

Any device that runs software can contain security flaws, known as 'vulnerabilities'.

Vulnerabilities are regularly discovered in all sorts of software. Once discovered, malicious individuals or groups move quickly to misuse (or 'exploit') vulnerabilities to attack computers and networks in organisations with these weaknesses.

Caution

[Poor control of white space means the heading 'Caution' is nearer to the previous para than the para it relates to.]

Product vendors provide fixes for vulnerabilities identified in products that they still support, in the form of software updates known as 'patches' or security updates. These may be made available to customers immediately or on a regular release schedule (perhaps monthly).

['in-scope software' - hyphenate.]

Requirements under this technical control theme

The applicant must ensure all in scope software is kept up to date. All software on in scope devices must be:

- licensed and supported
- removed from devices when it becomes un-supported or removed from scope by using a defined "subset" that prevents all traffic to / from the internet
- have automatic updates enabled where possible
- updated, including applying any manual configuration changes required to make the update effective, within 14 days* of an update being released, where:
 - The update fixes vulnerabilities described by the vendor as 'critical' or 'high risk'
 - The update addresses vulnerabilities with a CVSS v3 score of 7 or above

[Why initial caps for these three listed items? Poor quality control.]

- There are no details of the level of vulnerabilities the update fixes provided by the vendor

[Use 'we'.]

For optimum security and ease of implementation it is strongly recommended (but not mandatory) that **all** released updates be applied within 14 days.

*It is important that these updates are applied as soon as possible. 14 days is seen as a reasonable period to be able to implement this requirement. Any longer would constitute a serious security risk while a shorter period may not be practical.

Information

If the vendor uses different terms to describe the severity of vulnerabilities, see the precise definition in the Common Vulnerability Scoring System (CVSS). For the purposes of the Cyber Essentials scheme, 'critical' or 'high risk' vulnerabilities are those with a CVSS3 score of 7 or above or are identified by the vendor as "critical or high risk.

[Use 'you'.]

[Use 'we'.]

Caution

Some vendors release security updates for multiple issues with differing severity levels as a single update. If such an update covers any 'critical' or 'high risk' issues then it must be installed within 14 days.

[Use 'be' - simple language.]

[Double quotes or single quotes? Muddle. Poor quality control.]

[No closing quote marks. Poor quality control.]

[Use a comma, then 'then' is unnecessary.]

[, you must install it...]

[Why cap G?]

Further Guidance

Back up your data

Backing up means creating a copy of your information and saving it to another device or to cloud storage (online).

Backing up regularly means you will always have a recent version of your information saved. This will help you recover quicker if your data is lost or stolen.

You can also turn on automatic backup. This will regularly save your information into cloud storage, without you having to remember.

If you back up your information to a USB stick or an external hard drive, disconnect it from your computer when a backup isn't being done.

Backing up your data is not a technical requirement of Cyber Essentials; however we highly recommend implementing an appropriate backup solution.

[Add a comma.]