

University of **Strathclyde** **Glasgow**

Mind the security gap: Evaluating the effectiveness of the UK Cyber Essentials scheme and its suitability for large enterprises

Andrew Cooper

This dissertation was submitted in part fulfilment of requirements for
the degree of MSc Cyber Security

Department of Computing and Information Sciences
University of Strathclyde

March 2023

1 Declaration

This dissertation is submitted in part fulfilment of the requirements for the degree of MSc of the University of Strathclyde.

I declare that this dissertation embodies the results of my own work and that it has been composed by myself. Following normal academic conventions, I have made due acknowledgement to the work of others.

I declare that I have sought, and received, ethics approval via the Departmental Ethics Committee as appropriate to my research.

I give permission to the University of Strathclyde, Department of Computer and Information Sciences, to provide copies of the dissertation, at cost, to those who may in the future request a copy of the dissertation for private study or research.

I give permission to the University of Strathclyde, Department of Computer and Information Sciences, to place a copy of the dissertation in a publicly available archive.

(please tick) Yes No

I declare that the word count for this dissertation (excluding title page, declaration, abstract, acknowledgements, table of contents, list of illustrations, references and appendices is **16,476**.

I confirm that I wish this to be assessed as a Type 1 2 3 4 5

Dissertation (please circle)

Signature: **Andrew Cooper**

Date: **23 March 2023**

2 Abstract

The Cyber Essentials scheme was launched in 2014 to help businesses in the UK demonstrate they had effective basic security controls in place. Later that year it was made a mandatory requirement by Crown Commercial Service for certain central government contracts and it is used today as an independent measure of assurance by public bodies such as the Ministry of Defence and the Scottish Government. Despite this, there have been high-profile compromises at UK organisations that held Cyber Essentials at the time of their attack. The aim of this research is to discover what could allow a low-level internet threat to bypass the Cyber Essentials controls which, after all, are designed to prevent such an attack from occurring. Is it the controls themselves, the requirements, scoping issues or the audit?

The aim of Cyber Essentials is to be a universal scheme, regardless of size. Despite this there have been criticisms of scaling issues which have been dismissed in blog posts by NCSC. The main theme of the research was therefore to look at whether there is something to this – does the scheme have fundamental issues when applied at scale which could allow a low-skill attack to occur? And since large public sector bodies are mandating this from suppliers and organisations they do business with, are there issues with using it as an independent measure of assurance?

A survey of large organisations was carried out to gather views on the pros and cons of the scheme and to help identify any issues they have with scale or assurance. These findings were then used to inform a literature review of the scheme documentation. This featured a methodical examination of every question related to scope and the security controls in Cyber Essentials, and an examination of each test in Cyber Essentials Plus. To provide further context an interview with a former Cyber Essentials assessor was carried out which helped identify further issues in the assurance process.

The research found that neither Cyber Essentials nor Cyber Essentials Plus could be used as an independent measure of assurance and that both had issues when applied at scale. 17 recommendations have been made which, if implemented, would dramatically improve the scalability of the scheme and the assurance it offers. Despite these recommendations future work should be carried out to consider whether the scheme actually addresses modern low-skill cyber threats.

3 Acknowledgements

This paper was only possible due to the support from the University of Strathclyde both as an academic institution and as my employer. My supervisor, Dr Daniel Thomas, has provided sage guidance and advice throughout the process. Thanks also to my line manager, Bruce Rodger, for allowing me the time to complete this degree and taking the considerable time to proof read this document.

Special mention must also be made for the people who took time to engage with the survey and the former Cyber Essentials assessor who graciously gave up time to be interviewed.

The biggest thanks are reserved for my wife and daughters who put up with my absence from family life at various points over the past six months while I worked on this. Thank you.

4 Table of Contents

1	Declaration.....	2
2	Abstract.....	3
3	Acknowledgements.....	4
5	Table of figures	8
6	Introduction	9
6.1	Cyber Essentials in context	9
7	Background Analysis	9
7.1	Literature review.....	9
7.2	Research Questions	11
8	Methodology.....	11
8.1	The survey	12
8.2	The literature review	14
8.3	The interviews.....	15
8.4	Other evidence.....	16
8.5	Methodology summary.....	16
9	Analysis	16
9.1	Survey results.....	16
9.1.1	Operating Systems and directory services.....	17
9.1.2	Device Management	17
9.1.3	Positives and challenges of the scheme	17
9.1.4	Communications	18
9.1.5	The assessment process.....	18
9.2	Cyber Essentials documentation.....	19
9.2.1	Scope	20
9.2.2	Firewalls	23
9.2.3	Secure Configuration	24
9.2.4	Security Update Management	25
9.2.5	User Access Control	29
9.2.6	Malware Protection	29
9.2.7	Cyber Essentials summary	30
9.3	The Assessors	30
9.4	Cyber Essentials Plus.....	31
9.4.1	Scope	32
9.4.2	Sampling.....	32
9.4.3	The Tests	33

9.4.4	Cyber Essentials Plus summary	36
9.5	Communication issues	36
9.5.1	Documentation	36
9.5.2	Carelessness	37
9.5.3	Nomenclature	38
9.5.4	Timing and transition periods	39
9.5.5	Engagement	39
9.5.6	Assessors	39
9.6	What's missing?	40
9.6.1	Evolution to address modern low skill threats	40
9.6.2	Lateral movement	40
9.6.3	Backups and encryption	40
9.6.4	Compensating controls	41
9.6.5	USB sticks	41
9.6.6	Evidence	41
9.6.7	Operational guidance	42
9.6.8	Vendor guidance	42
10	Conclusions and recommendations	42
10.1	Restore parts of the scheme	42
10.2	Scope issues	43
10.3	CE issues	43
10.4	CE+ issues	43
10.5	Communications	44
10.6	The missing control: Asset Management	44
10.7	Nudge	45
10.8	Future Work	45
11	Final thoughts	46
12	References	47
13	Appendix 1 – Questionnaire	58
13.1	Recruitment message	58
13.2	Questionnaire consent page	58
13.3	Main questionnaire page	59
14	Appendix 2 – File Types to block or warn about on inbound email	61
15	Appendix 3 – Device management tools from the survey results	61
16	Appendix 4 – More on Sampling	62
16.1	Clarifications on what is meant by a representative sample	62

16.2	Non-sampled compliance	63
17	Appendix 5 – Security Update Management Issues in the Real World	63
18	Appendix 6 – Evolution of low skill threats since 2014.....	63
19	Appendix 7 – How to pass without implementing the controls	64
19.1	Worked example part 1 – Cheating Cyber Essentials	65
19.2	Worked example part 1 – Summary	66
19.3	Worked example part 2 – Cheating Cyber Essentials Plus.....	66
19.4	Worked example part 2 – Summary	67
19.5	Summary	67

5 Table of figures

Figure 1 Coding of Q5	14
Figure 2 Demographics	17
Figure 3 Average operating system usage	17
Figure 4 Directory service in use	17
Figure 5 CE Inventory	24
Figure 6 Essential Eight inventory	24
Figure 7 Accounts guidance	25
Figure 8 Update guidance	26
Figure 9 Impact of a 1% failure rate	26
Figure 10 A6.5 Application updates	27
Figure 11 Java update elevation prompt	28
Figure 12 User driven update	28
Figure 13 Sampling guidance	32
Figure 14 Sampling as a percentage of population	33
Figure 15 Tests aligned with Scope and Control	34
Figure 16 Data leakage from IASME	37
Figure 17 Font differences	37
Figure 18 Mixed case	38
Figure 19 A2.4.1 Thin client guidance	39
Figure 20 A6.7 Unsupported software guidance	39
Figure 21 A7.17 MFA guidance	39
Figure 22 List of file types	61
Figure 23 Management tools in use	62
Figure 24 Cheating Cyber Essentials with Group Policy	67

6 Introduction

6.1 Cyber Essentials in context

In December 2020 the Scottish Environment Protection Agency (SEPA) suffered a major cyber-attack, thought to be delivered via a phishing email, which they are still recovering from two years later. At the time of the attack they had been certified as compliant with Cyber Essentials Plus (SEPA, 2021).

The UK Government describe Cyber Essentials (CE) as “a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats” which is “suitable for all organisations, of any size, in any sector” (GOV.UK, 2018). It comes in two versions; Cyber Essentials which is effectively a self-assessment questionnaire, and Cyber Essentials Plus which builds on this with “a technical audit of the systems that are in-scope for Cyber Essentials” (IASME, n.d.). If an organisation the size of SEPA can suffer such a major attack from a common online threat while holding the top tier CE certificate then some part of the process has not functioned as expected.

The scheme is also becoming mandatory for public sector organisations. The UK Government “requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme” (GOV.UK, 2018). If the certification failed to protect a larger organisation with 1,300 employees (SEPA, 2020) then is this enforcement misplaced? This research intends to identify what is wrong with scaling CE – the controls, the requirements, the scope or the audit – and come up with solutions which could offer other organisations assurance that, with some minor modifications, the scheme is still fit for purpose.

7 Background Analysis

7.1 Literature review

Cyber Essentials is positioned as a set of five simple controls with the implication that they are relatively easy to implement. NCSC describe CE as a “simple but effective” scheme to protect against attacks “basic in nature, carried out by relatively unskilled individuals” (NCSC, n.d.). This type of phrasing is seen in other commentary about the scheme such as “basic cyber hygiene” (Such, et al., 2019) which defends against “common cyber attacks” (IASME, n.d.), by the application of “simple technical controls” (NCSC, 2022). This messaging has resonated in the UK – the BMJ criticised all the hospitals examined after the 2017 Wannacry attack for failing to obtain CE describing it as “a basic set of minimum organisational security standards” (Martin G, 2018). However, one of the sources referenced by the BMJ was aware of the issues large complex organisations face in implementing these controls calling them a “high bar” to be assessed against (digitalhealth, 2018).

A key characteristic of CE is the minimisation of risk management. The requirements are prescriptive and there is no provision for compensating controls. A possible reason for this is that smaller organisations “are challenged more than large companies in evaluating possible IS-related risk” (Barlette & Fomin, 2008). This approach appears to be at odds with an Information Security Management System (ISMS) such as the widely used ISO27001 which at a fundamental level “provides risk management processes” to protect information security (Almeida, et al., 2018). Chris Ensor, an NCSC deputy director, hints at another reason risk is minimised in CE – “assessing whether alternative measures give an equal level of confidence that a risk is being managed is hard” (NCSC, 2021) and “whilst I’m sure there are many experienced Cyber Essentials assessors out there who can make [risk based] judgement[s], we have no way of knowing who they are.” The prescriptive nature of CE raises scope issues. (Kipchuk, et al., 2021) compare a number of security frameworks and suggest that the payment card industry’s PCI DSS can be more prescriptive than something like

ISO27001 because it has a reduced scope, that of the Cardholder Data Environment. CE is an outlier in that it is by default scoped to an entire organisation yet is very prescriptive.

Despite the lack of risk management (Such, et al., 2019) found that CE worked well for SMEs in part because “Cyber Essentials is one of the very few schemes for SMEs [...] that includes an assurance framework.” However, they also state that it requires “almost perfect adherence to the guidelines for implementing Cyber Essentials security controls.” This highlights the importance of the CE+ audit to ensure these controls are implemented correctly.

Cyber Essentials is not the first cyber assurance scheme backed by the UK Government. (Silva, et al., 2016) examine the reasons for the failure of the c: cure scheme which was launched in 1998 and discontinued 2 years later. This aimed to certify organisations against the risk based British Standard BS7799 (adopted internationally as ISO27002) but had 4 key problems – a lack of auditors caused by “rigorous auditor assessments,” implementation problems for SMEs (in particular the £3,000 to £5,000 cost), it was not a requirement to do business, and a cheaper alternative scheme was available. Importantly it evaluated security *management* not security *controls* (Dhillon & Backhouse, 2001). It seems like some institutional memory has in Cyber Essentials created a scheme which is the opposite of c: cure – a simplistic audit, simple for SMEs, mandatory for some and low cost. Viewed this way some of the design decisions of CE make sense, but again highlights that SMEs have different needs and approaches to cybersecurity. (Barlette & Fomin, 2008) explore this further and conclude that “there is a need for having at least 2 versions of the standards: one suitable for big SMEs and big companies, one for small SMEs simplified in terms of time, money and certification cost.” (Siponen & Willison, 2009) reinforce this by stating that information security standards that are “generic or universal in scope [...] do not pay enough attention to the differences between organizations and the fact that their security requirements are different.” Again, this appears to be at odds with the ‘one-size-fits-all’ approach that CE takes. Before even looking at technical controls, even implementing consistent policies “is not a straightforward and simple task of merely copying the best practices to local [information security] policies, as the best practices must be contextualized to fit the local conditions” (Niemimaa, 2017).

Prior to 2020 NCSC engaged with a number of bodies – referred to as Delivery Partners – to run the scheme. One such Delivery Partner – (CREST, 2014) – took a wider view of where Cyber Essentials sat stating “for an organisation to gain an appropriate level of assurance it [...] may need to consider the requirements of broader standards and frameworks, such as ISO 27001, PCI, COBIT, or the ISF Standard of Good Practice.” Interestingly they provided a chart of what types of organisations should be using CE and CE+ – SMEs using COTS (common off the shelf) products where IT was either a support tool or a business enabler. For medium and large enterprises where “IT is an integrated part of the business” considering alternatives was suggested.

Since April 1 2020 NCSC have partnered with IASME – the Information Assurance for Small and Medium Enterprises Consortium – to run the CE scheme. Whilst the name of the partner may reinforce the perception that CE has a size issue, NCSC echo the statements of the UK government that the scheme is suitable for any organisation “whatever its size” (NCSC, n.d.). Despite this, it has been noted that CE “was particularly designed to help facilitate and encourage smaller businesses to achieve a recognised standard” (Rae & Patel, 2019). NCSC’s Chris Ensor rejects this claim: “I’ve heard it often said that CE was designed for small organisations, but in reality it was designed to be size agnostic” (NCSC, 2017).

More recently Cyber Essentials (and Cyber Essentials Plus) have been used as an assurance method that an organisation has implemented basic security controls correctly. The Scottish Government’s

Cyber Resilience Unit sent out a questionnaire to public sector organisations in February 2023 which had the question “How has your organisation independently assured their critical technical controls (as set out in the Cyber Essentials Standard)?” (Scottish Government, 2023). Alongside ISO27001 and NIS, Cyber Essentials and Cyber Essentials Plus were listed as assurance methods.

The Ministry of Defence (MoD) also accept Cyber Essentials as a measure of security assurance in their Supplier Assurance Questionnaire Question Set Guide (Ministry of Defence, 2021). They have four categories of Cyber Risk – Very Low, Low, Moderate and High – and each has different requirements for policies and security baselines. CE is accepted as a baseline level of security assurance in the *Very Low* category. The *Low* category asks:

“Does your organisation have Cyber Essentials Plus certification that covers the scope required for all aspects of the contract, and do you commit to maintaining this standard for the duration of the contract?”

If the supplier can’t provide a certificate number it doesn’t meet the minimum level set out by the questionnaire (although an alternative standard can be provided).

Other government departments require CE for procurement (Cabinet Office, 2016) or CE+ for funding (ESFA, 2021). It may not have been designed this way but Cyber Essentials and Cyber Essentials Plus are being used as an assurance measure by public bodies.

7.2 Research Questions

Based on the literature review it is clear that Cyber Essentials is a compliance framework that is designed to provide a level of assurance that a selection of key security controls are in place. It is designed to be simplistic so that the assessment and auditing process can be affordable. An aim of the scheme is that it works for any size of organisation. Any research and recommendations would need to fit within these parameters to be acceptable for further adoption. The literature review also revealed that the approach taken to cybersecurity is different between different organisations and between different sizes of organisations. It also showed that large public bodies such as the Scottish Government and Ministry of Defence are using the scheme as an independent measure of assurance that other organisations and suppliers have implemented the controls correctly.

This has led to these questions:

1. Does the scheme have issues when scaled to enterprise environments?
2. Can Cyber Essentials be used as an independent measure of assurance?

8 Methodology

Two strands of research were initially carried out in parallel and the reasons for these choices will be explained shortly. Firstly, a qualitative survey was used to discover attitudes to CE in large organisations and whether there were any common issues experienced that may be due to scale.

Secondly, a detailed literature review of the CE documentation was carried out to look for assumptions that may cause issues when scaled to a very large number of users and devices. This also encompassed a literature review of the CE+ audit documentation. Historic CE documentation was found on the internet archive and used to provide context that was missing from current guidance.

The intention was that at the end of this portion of research there would be data from a sufficient number of large institutions on what areas of CE cause them difficulty and a list of controls and requirements that may have issues when applied at scale.

During the literature review it became clear that some information about the scheme was missing from the public domain. There is an illustrative test specification available from NCSC (NCSC, 2022), but the actual test specification used by IASME wasn't available. Additionally, there was no public information about sampling methods and other aspects of the scheme were unclear. To discover more and to provide further context it was decided that interviews with current and former Cyber Essentials assessors would be carried out.

8.1 The survey

The primary reason for the survey was to gather information that could not be found in the existing literature. The other studies identified in the literature review have considered the impact of the scheme on Small to Medium Enterprises. This area of research addresses a need for a data set on the challenges large organisations have with the scheme.

The decision to use a survey to gather responses instead of interviews was to obtain a relatively wide selection of semi-structured data in a format that could be more easily analysed for sentiment and trends. Larger organisations are by definition more complex than small ones, so bringing structure to the data gathering was key. Whilst a semi-structured interview could have been used instead, this would have introduced scheduling issues between the interviewer and interviewee and require transcription. For these reasons a qualitative survey with relatively specific questions but allowing for free form answers seemed the most balanced approach.

A decision was taken to only offer the survey to Higher Education (HE) institutions which may appear to introduce the risk that some of the issues identified are not to do with scale but instead due to peculiarities of the sector, weakening the overall arguments discussed in the paper. Whilst there are issues unique to the sector – such as allowing customers (students) to have accounts in the same directory service as the employees – the questions were chosen to elicit responses with respect to scale and assurance. The HE sector is also in a relatively unique situation where funding bodies are requiring Cyber Essentials before awarding money – obtaining CE is a business need for these organisations so the potential pool of respondents should have already had experience with the scheme. Finally the HE sector, by its very nature, is open about sharing information. An example of this is the Jisc annual security posture survey (Jisc, 2022). Jisc – who run the networking for most of the institutions in the UK – have seen a fall in organisations with CE, from 69% in 2020 to 58% in 2022. The numbers with CE+ has been relatively static since 2020, fluctuating between 31% and 29%. This would suggest HE is a good candidate for evaluation since many organisations have CE, most are considered large by the scheme, and there has been over a 10% drop in those maintaining their certification.

The questions were designed to elicit thematic results to cover:

- Scoping and sub-set definition
- Operating system and directory service used
- Positives of the scheme and challenges faced
- The CE+ audit
- How patching is implemented and monitored
- Communication from IASME and NCSC

A further open-ended question was offered to respondents for any other comments not addressed in the above categories.

The survey was distributed to organisations in a number of ways. Firstly, it was distributed to members of HEFESTIS – a shared CISO service for Scottish based universities and colleges. It was then circulated to members of a UCISA group dedicated to members wishing to share experiences of Cyber Essentials.

Due to the free-form nature of the survey care was taken categorising answers and gauging sentiment. As an example, to gather meaning about operating system, directory service and management tool used, the responses to Q3 about the breakdown of operating system usage and directory service and Q6 about patch compliance were combined and analysed.

Most responses were easy to categorise but some were less clear and interpretation had to be used. For example, one partial response to Q3 was “Some do, but most of them connect to Intune.” This was interpreted as a yes – they do use Active Directory for some of their devices. Another response contained the operating systems and the wording “all moving to Azure Active Directory” which was interpreted as they were moving from on-prem Active Directory. Another response was “Primarily Windows” so an approximation was required – since all the other responses had Windows use above 90% an average of these was used for this response. Any responses listing device numbers were converted to percentages to help anonymise the data and mobile devices such as iPhones and Android were excluded.

Some responses did not answer the Active Directory portion of Q3, but stated in Q6 that they used Microsoft Configuration Manager (SCCM) which requires the use of Active Directory (Microsoft, 2022) so this was used to answer Yes to that portion of Q3.

For Q4 on the benefits and challenges of the scheme the responses could be coded into categories. Benefits broadly fit into categories such as “Access to funding”, “Provides a security baseline” and “Enhances security”. Challenges were more diverse but some common themes were extracted. Q5 was approached in the same manner and a coding example is seen in Figure 1:

Coding	Free text
manipulable	Only way to p Numbers base
lack of evidence	Would be bet
manipulable	System can be
complex	Given the leve
scale	Almost impos
positive	at times picke
assessment quality	many ce requi
	most large org
complex	should be stra
assessor quality	assessors ofte
low assurance	minimal assur
scale	limitation on t
adequate	ce controls are
assessment quality	just passed bu
assessor quality	auditors vary
manipulable	ce+ process to

Figure 1 Coding of Q5

8.2 The literature review

The primary source of the Cyber Essentials scheme is the documentation. This includes the Question Set (SAQ) and the Requirements document. For this part of the research the analysis was carried out both within the context of the research questions but also informed by the responses from the survey. An example of this was in the Scoping section – the majority of respondents said their organisation used Active Directory so the impact of Active Directory when defining a sub-set was examined in detail. CE terminology was adopted such as ‘applicant’ for the organisation aiming for certification.

The SAQ is broken down into sections and each question is prefixed by the section number such as A1.1, A1.2 and so on. Some sections map directly onto the 5 controls and one of the sections maps directly to the scope. The strategy taken to analyse the SAQ was to consider each primary section in turn. During analysis it became clear that certain questions were similar so these were grouped together.

For Cyber Essentials Plus a similar approach was taken – there are 7 tests which were considered in turn. An issue here was that only the illustrative test specification from NCSC was available – IASME do not publish what their assessors see. This was not seen to be too big a problem as the NCSC expect their Delivery Partner (IASME) to implement the tests they specify. The main issue is that there are areas where the Delivery Partner can use their judgement to set parameters (such as the types of files that will be used in the malware test) and these were unavailable. Historic documents were searched to obtain these details but there is no guarantee they are what is in use today.

During this phase of the analysis each of the 7 tests were mapped to questions in the CE SAQ to discover which of the requirements in CE are actually tested in CE+. It also highlighted which requirements were *not* assessed in CE+ which helped answer part of the research question on assurance.

In a CE+ assessment sampling is used for some tests so accurate sampling is critical for confidence in the test results. Sampling issues and potential solutions were explored within the context of large organisations. The definition of a large organisation was obtained using the price breaks from the NCSC website (NCSC, 2023) which in turn appears to reference the EU standard definitions of small and medium enterprises (European Union, 2003).

Statistics on businesses in the UK was obtained from the (Department for Business, Energy & Industrial Strategy, 2022). This showed that at the start of 2022 there were 5.5 million businesses in the UK of which 99.2% would be considered Micro or Small under NCSC guidelines (NCSC, 2023). Only 35,900 businesses were considered Medium and 7,700 businesses considered Large. This helped provide further context within which to examine the scheme. It was also noted that 63% of the people employed in the UK work in Medium or Large organisations, 0.8% of the total number of businesses. At points during the analysis this tension was considered – were the scheme authors trying to protect the majority of UK businesses or the majority of UK users?

A critical part of the scheme is the assessors themselves and they were explicitly mentioned by a number of survey respondents. To explore whether they have an impact on assurance an examination of the training, qualifications and experience required to be an assessor was performed using IASME documentation.

Throughout the literature review parallels were seen with other assurance frameworks such as PCI DSS and the Australian Essential Eight (ACSC, 2023). When weaknesses were spotted in Cyber Essentials a comparison with these frameworks was made to find positive suggestions for improvement. If none were found then none were noted, but where good practice was found adaptations for CE were attempted.

A comparison with the worldwide PCI scheme set up by the major card providers (PCI Security Standards Council, n.d.) may seem unfair. The intention was to look for best practice and CE+ itself points to PCI documentation in Appendix A of the Test Specification (NCSC, 2022):

“for information on good practices with [scanning] tools see PCI Approved Scanning Vendors Program Guide”

Finally, where questions or intentions were at odds with commercial products this was noted with examples.

8.3 The interviews

By the time of scheduling the interviews there had already been a large volume of research produced – analysis of the scheme documentation was well underway and the survey had a number of responses which were being collated. The intention therefore was for the interviews to be relatively brief but to provide information that was not available through other means.

The intention was to use a semi-structured interview with the following categories some of which are similar to those used for the survey:

- Scoping and sub-sets
- Operating systems
- Challenges
- Sampling sizes
- Changes to the scheme over the years

Initially three interviewees were sought through direct contact with the head of consulting at a number of firms and through LinkedIn – a former CE assessor to provide historical context, a current CE assessor local to Scotland and a national larger assessor. Unfortunately, due to time constraints and scheduling issues, only the former CE assessor was available. While this may appear to be a weakness in the study it may actually be a strength – it means that this research is based only on publicly available information and historical assessor information. It also meant that the research wouldn't inadvertently place commercially sensitive current information into the public domain.

The interview was transcribed live which forced some limitations on the conversation. It was far briefer than intended and at points the interviewee was asked to stop talking and repeat or clarify information so that it could be captured accurately. These limitations also led to some direct questions which elicited some short, but useful, answers such as:

Q When you were carrying out assessments, how did you have confidence that what the applicant said on the questionnaire was true?

A When I was doing it we had to get screenshots

Due to the simple nature of the questions and responses, and the lack of participants, the interview was used as a source of data about the scheme rather than a source for further deduction. Even if there had been more participants the use of grounded theory could not have been used as the survey and literature review had provided a position which was being brought to the interviews – there was no expectation that new theories would emerge from the questioning. Thematic analysis would therefore have been used if there had been more data to review.

During the analysis the interviewee will be described as “the Former Assessor” to provide context or to backup arguments.

It was agreed with the participant ahead of time that the interview transcript would not be put in the appendix in case they mentioned commercially sensitive information but is available to the supervisor and external examiners.

8.4 Other evidence

To demonstrate operational issues some practical work was carried out. To evaluate issues with auto-updates older versions of software were installed and their update processes were observed. To analyse the NCSC Windows security guidelines a clean build of Windows was installed and the policies applied.

8.5 Methodology summary

A variety of different approaches were taken to examine the scheme. Crucially only publicly available sources were used and the opinions of enterprise customers and a former assessor. If this study were carried out again using the non-public documentation the results may differ. This provides an external viewpoint on Cyber Essentials which may be contradicted by private scheme guidance.

9 Analysis

9.1 Survey results

The survey had 21 responses but only 14 completed responses. The incomplete responses could be partially explained by the consent button on the first page of the survey. It is possible that responses were abandoned once the questions were presented on page two. Of the 14 responses the majority

were from organisations that are considered large by IASME, and 10 were from organisations with over 5,000 users or devices.

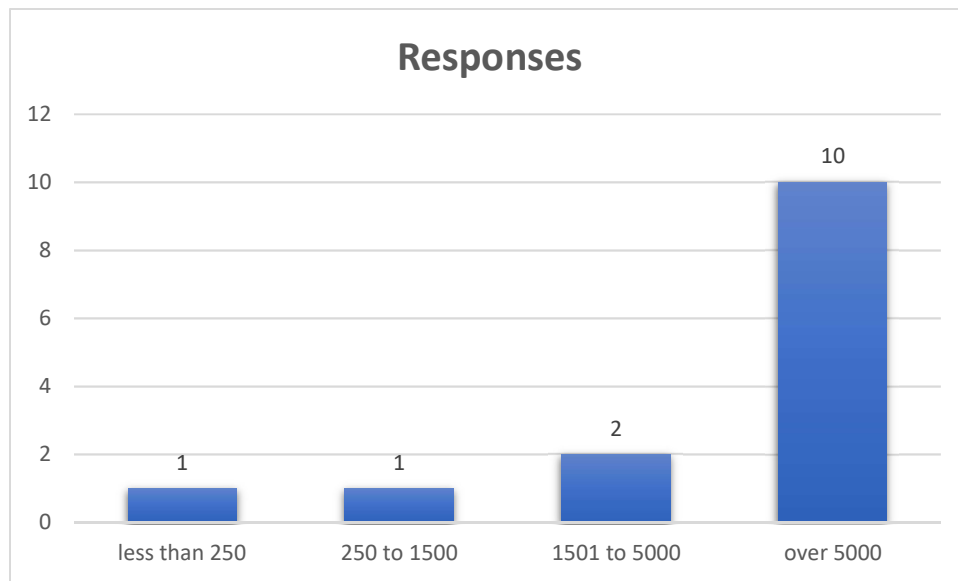


Figure 2 Demographics

9.1.1 Operating Systems and directory services

All responses that had values for operating systems demonstrated the dominance of Microsoft Windows on the endpoints. Two responses reported the lowest usage of Windows at 80% whilst three responses reported 100% usage of Windows.

Windows	MacOS	Linux
92%	7%	1%

Figure 3 Average operating system usage

Reported on-prem Active Directory use was 79% with Azure Active Directory making up the rest. Again, Microsoft dominates here and this reflects commercial realities (Microsoft, 2021).

On-prem AD	Azure AD
79%	21%

Figure 4 Directory service in use

9.1.2 Device Management

57% of respondents use Microsoft System Center Configuration Manager (SCCM) to manage their devices. Using SCCM is an important differentiator when exploring how organisations implement and audit their security controls. This will be explored later when considering how scope is defined. 35% of respondents used Intune, sometimes in combination with SCCM. PDQ was used by 14%. Other reported tools are discussed in Appendix 3.

9.1.3 Positives and challenges of the scheme

35% of respondents said that it provided access to funding for their organisation. 28% said that it provided a baseline level of security while 21% thought it improved security. Other responses said that it lowered the cost of Cyber Insurance and helped validate their security controls.

The only common challenge were the BYOD changes which was reported by 28% of respondents. Other challenges included a lack of detail in the scheme, the assessors, a lack of risk management,

perceived inflexibility, challenges around managing a large estate and implementation of technologies such as MFA and network segmentation.

9.1.4 Communications

Only one of the responses to the survey was positive about the communication around the scheme describing it as “clear and well timed.” The remaining responses fit broadly into two categories – negative and negative but with a view that it has recently improved. In the latter category the praise was qualified:

“[communications have] improved over the last 18 months but were not that good at the start”

“a significant amount of miscommunication but the direct sessions with NCSC [...] have helped hugely”

Three responses mentioned the timing of the communication around scheme changes leaving an “overly short time to implement”, which left another respondent “little time to prepare.” Another response stated:

“timescales for changes to the scheme are not compatible with the business and financial processes of large organisations.”

Another theme was around the lack of engagement by NCSC and IASME:

“[communication is] one way, there is no discussion, just an imposition of harder and harder compliance requirements”

“Poor [communication] in transmit mode only.”

Confusion around the requirements was also noted:

“[communications are] entirely confused and contradictory [...] often relying on obscure sources for clarification, with the information on the web-site (IASME) often incomplete.”

Reinforcing the above:

“[there is a] significant amount of miscommunication”

“a great deal of confusion and misinformation”

“there has been a lot of chopping and changing and i'm never sure if what i hear is correct.”

9.1.5 The assessment process

The positive comments stated the controls “are adequate for assurance” and it “picked up out of date software”.

3 responses suggested it was easy to cheat – the “system can be gamed”, it’s “too lightweight and manipulable” and one passed by narrowing scope to a point that “felt almost fraudulent.” A further comment was made about the lack of evidence required to pass.

2 comments were about scale and how the sample size did not provide “an appropriate level of assurance” and that it was “impossible for a large organisation on a wide scope.” Other comments mentioned that it “is overly restrictive and complex” and it “should be straightforward but it is not.”

The assessment quality was mentioned – “many ce requirements are not verified by the audit process.” Others mentioned the quality of the assessors and this will be examined later.

9.2 Cyber Essentials documentation

Cyber Essentials is both the name of the scheme and the name of one of the two levels of certification offered.

The Cyber Essentials portion of the Cyber Essentials scheme is a Self-Assessment Questionnaire (SAQ) whereas the Cyber Essentials Plus portion is an audited assessment of controls. Cyber Essentials is a pre-requisite to achieving Cyber Essentials Plus.

To analyse the scheme the primary sources as provided by NCSC and IASME will be used.

The documents analysed are based on the v3.0 version of the standard, also known as Evendine, the latest version at the time of writing. The following four documents were used as the primary source for analysis of the scheme:

- Cyber Essentials: Requirements for IT infrastructure v3.0 January 2022 (NCSC, 2022)
- Cyber Essentials Plus: Illustrative Test Specification v3.0 January 2022 (NCSC, 2022)
- Cyber Essentials Question Set – Evendine – July 2022 (IASME, 2022)
- Cyber Essentials Self-Assessment Preparation Booklet Version 13a July 2022 Evendine (IASME, 2022)

The Cyber Essentials questionnaire comprises 8 sections:

1. General questions about the organisation
2. Scope definition, asset management and a question on who is the person responsible for managing the systems within the scope
3. Questions that are used to offer free Cyber Insurance to certain sizes of organisation
4. Firewalls
5. Secure Configuration
6. Security Update Management
7. User Access Control
8. Malware Protection

Sections 1 and 3 are general questions about the organisation such as name, address, business type so they will not be analysed further. However, it’s worth noting Question A1.6:

“What is your website address?”

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

This offers a hint at the scaling issues to come in the rest of the SAQ.

Section 2 is about scope and will be examined first. The remaining sections 4 through 8 map directly on to the stated scheme controls and will then be analysed in turn.

9.2.1 Scope

In the background analysis it was shown that large organisations are using CE as an independent measure of assurance. The MoD explicitly ask whether the “certification [...] covers the scope required” but others do not. Knowing the scope and how it is defined is critical to understanding the security posture of the organisation being evaluated.

In the questionnaire there are 10 questions on scope – A2.1 through A2.10. Many of these are not on scope at all, but are instead asset management. 5 of the questions ask for lists of devices and in some cases make, model and operating system:

- A2.4 Laptops, Desktops and Virtual Desktops
- A2.4.1 Thin clients
- A2.5 Servers, virtual servers and virtual server hosts (hypervisor)
- A2.6 Tablets and mobile devices
- A2.8 Network equipment

In addition, A2.9 asks for a list of all cloud services used by the organisation. A2.4.1 is marked ‘information only’ and this will be explored later.

A2.10 asks for the “name and role” of the person responsible for managing all of the above systems. This is another scaling issue – in a smaller organisation it is reasonable for one person to be responsible for the management of all of these systems. In a larger organisation each category is likely to be managed by separate teams and the person with overall responsibility is likely to be sufficiently senior as to not be in a position to answer the questions in the SAQ.

9.2.1.1 Defining the scope

It is difficult to see within the SAQ how the scope is technically defined or assessed.

A2.1 asks whether the scope will be the entire organisation as a yes/no answer and, if no, A2.2 asks “what scope description would you like to appear on your certificate and website?” The phrasing of this question is odd as it doesn’t ask how this sub-set is technically separate, only for the applicant to list a high-level description. The guidance note attempts to clarify that it “should provide details of any areas of your business that have internet access and have been excluded from the assessment.”

A2.7 asks for a “list of the networks that will be in scope” but the guidance again only asks of name, location and purpose and specifically states “you do not need to provide IP addresses or other technical information.”

A2.8 asks for details of network equipment which is more asset management but again specifies “you do not need to provide IP addresses, mac addresses or serial numbers.”

Nowhere in these questions is the applicant asked how their technical controls achieve a separation within a sub-set.

The requirements document provides more detail. The preferred scope is “the whole IT infrastructure used to perform the business of the applicant” but a sub-set can be defined to reduce the scope providing that it is “separately managed.” There is a definition of a sub-set further up the document as “a part of the organisation whose network is segregated from the rest of the organisation by a firewall or VLAN.” This guidance is vague.

This is one of the few parts of CE that explicitly defines a specific technical control – implying that it is a requirement to segregate the sub-set from the rest of the organisation. However, even a properly configured firewall or VLAN will not segregate the sub-set if certain technologies are used.

The network segregation “by a firewall or VLAN” could be sensibly interpreted in a variety of ways, such as:

- A network isolated from the rest of the organisation via a firewall
- A VLAN where inbound connections from the rest of the organisation are blocked

However, because the guidance is not explicit, the following is within the letter of the standard if not within the spirit:

- A VLAN where traffic is routable to other parts of the network
- A VLAN where DHCP reservations are used

These do not provide sufficient technical separation between sub-sets of the organisation and should be explicitly ruled out. Perhaps a reason for this not being explicit is that inter-VLAN routing is not an option on small office/home office switches such as the Netgear GS308E (netgear, n.d.). It is only when using more expensive enterprise class devices that this becomes an option. The problem using a VLAN for a sub-set is compounded when you consider how enterprise organisations manage their devices.

9.2.1.2 Sub-sets and Active Directory

In the survey 79% of respondents used Active Directory (AD). Describing AD (Tenable, 2021) state that it is “the very foundation on which [an organisation’s] IT infrastructure is built” and that “every large-scale, infrastructure-wide attack that has crippled production capabilities in recent years has had an Active Directory exploit at its core.” (Qomplx, 2021) reinforce this referencing AD’s “95% market share in the enterprise” and it as the “attackers’ #1 target.”

A sub-set of the organisation cannot be easily defined when Active Directory is used because the sub-set cannot be technically isolated from the rest of the directory. A compromised device outside the sub-set but joined to the same Active Directory could easily compromise the devices in the entire sub-set. Even with a hardware firewall in place whoever controls the group policies in the domain can manage the security controls on the devices joined to that domain.

This increased risk is reflected in other areas of the cyber sector. The OSCP certification is one of a few allowed prerequisites for a CE+ Lead auditor but has recently shifted their syllabus to focus on AD because “having workable knowledge of Active Directory is a critical part of any information security professional’s skillset” (OffSec, 2021)

This risk has increased as the threat actors have improved. The LockBit 2.0 ransomware “has the capability to automatically deploy itself to Microsoft Active Directory clients via Group Policy Objects” (SecurityIntelligence, 2021). BlackMatter ransomware uses AD to enumerate all hosts and to look for accessible hosts (CISA.gov, 2021).

In Active Directory the security boundary is defined at the forest level (a forest being a collection of domains) (Microsoft, 2022), but insisting that an entire Active Directory forest should be the sub-set would make the assessment complex. Domains in AD are considered “Authentication and Authorization Boundaries” and “Units of Trust” (Microsoft, 2014) so it would seem reasonable to define a sub-set as an Active Directory domain.

From a scaling perspective the risk increases with the size of the organisation. In the scheme as currently defined, if the sub-set is a small proportion of a very large organisation, and the rest of that organisation is poorly managed, then the likelihood of AD compromise will be increased.

An alternative to including the entire AD domain in the sub-set could be to validate the security of the AD domain controllers and who has access to them. This is unlikely to be easy enough for a simple compliance framework but is noted here for completeness.

The key point here is that technical controls are mandated when a sub-set is used, but do not actually provide any segregation to the sub-set for the most common internet attacks in larger environments.

9.2.1.3 Sub-sets and Endpoint Management Tools

Much of the SAQ and the CE+ audit is focused on endpoints and ensuring that controls are implemented correctly on those devices. Yet there is no consideration that an endpoint management tool such as Microsoft System Center Configuration Manager (SCCM) may be used to implement or validate those controls. Over half the survey respondents use SCCM to manage their endpoints.

SCCM is designed for large organisations. According to a 2017 Twitter thread by David James, former Director of Engineering at Microsoft responsible for SCCM, the “median SCCM customer has about 7k devices” (James, 2017). He continues “if you ask me about customers [with less than] 100 machines - I don't see how/why they would ever use SCCM.” It also requires significant training (QA, 2023) and optional certification (Microsoft, 2018). James dryly notes “SCCM requires a freakin PhD to run it.”

When an organisation is large enough to use a tool such as SCCM then the underlying operational processes to set and monitor security controls will be different to those of a small organisation. The later examination of the SAQ questions and guidance will demonstrate the simplistic CE view of how to validate these controls.

For the scheme to scale there must be an appreciation that enterprises use management tools. This has the same implications as Active Directory – all devices managed by that management tool should be considered part of the same sub-set due to the risk of potential mis-use.

It should also imply that if a management tool is *not* used this would fail an assurance assessment for a large organisation. How could any large organisation have confidence that technical controls are in place if there is no tool to set and validate them?

It should be a requirement therefore that once an organisation is above a certain size a management tool such as SCCM must be used to set and validate security controls. This may be a controversial suggestion because of cost and resourcing implications – but the scheme has already made a recent clarification that has had a similar impact.

9.2.1.4 Bring Your Own Device (BYOD)

IASME are keen to stress that the scheme does not change over the years, points are instead clarified. However, these clarifications can have significant cost in both financial and resource terms. In the April 2021 update there were “no major changes” (IASME, 2021) just “a series of clarifications.” One clarification brought BYOD devices into scope.

To technically cope with this, a Mobile Device Management (MDM) or Mobile Application Management (MAM) solution needs to be implemented. This is not without cost. In 2021 the Microsoft solution – Intune – cost \$8 per user per month (redmondmag.com, 2021). For a small business of 10 users this would be an annual cost of \$960 a year. Scaled up to 10,000 users this would cost \$960,000, although this tends to be bundled with Enterprise agreements. Resourcing

cost should also be noted – processes need to be created, and dedicated support staff will be required during the initial enrolment.

The 2021 change also brought BYOD into scope for the full set of CE controls if connecting to a Virtual Desktop Environment (VDI). This seems odd. Unless drive redirection is enabled VDI provides *a view* of the data instead of *access to* the data and the virtual desktop can be subject to greater controls than BYOD.

This is at odds with commercial reference architectures on how to deliver remote IT to BYOD devices without a management agent (Citrix, 2022). Perhaps VDI has been confused with RDP – remote desktop protocol – reportedly used in 63.5% of ransomware attacks in 1Q2019 (Duo, n.d.) and arguably a common, rather than low-level, threat.

A seemingly small ‘clarification’ can have significant financial and resourcing costs.

9.2.1.5 *Sub-sets in a hybrid working environment*

Since the COVID-19 pandemic there has been a shift to hybrid work which has “exacerbated the decline of desktop PCs [and has] boosted the use of tablets and laptops” (Gartner, 2021). Does the above discussion of a technical control to segregate the devices within a sub-set have any relevance if the devices are mobile?

The answer has to be yes – what is intended to be included within the scope is not just endpoints but servers, routers and firewalls. But when portions of that sub-set are mobile and can move to untrusted locations this does introduce risk of bringing malware back to the trusted sub-set. Software firewalls are optional provided other controls are in place but should be mandatory.

Another naivety is on VPN connections. The guidance explicitly states that if a “home worker is using a corporate VPN, their internet boundary is on the company firewall or virtual/cloud firewall.” This is only true if this is a full-tunnel VPN – meaning all internet traffic goes via that tunnel. The alternative is a split-tunnel VPN where only corporate traffic goes via the tunnel and internet traffic can (depending on the configuration) go direct via the untrusted internet connection. Split-tunnel VPN has been recommended by Microsoft since the COVID-19 pandemic (Microsoft, 2022) so it seems likely than many organisations that use Microsoft tools have implemented this.

9.2.2 *Firewalls*

The firewall section runs from question A4.1 to A4.12.

A4.1 asks whether the applicant has a firewall and A4.2, A4.2.1, A4.3, A4.4 ask questions about password management on the devices.

A4.5, A4.5.1, A4.6 and A4.7 ask about what services are offered through the firewall and whether there are processes around the opening and closing of ports. A4.5.1 asks whether there are documented business cases for the open ports but does not ask to see them. An easy improvement therefore is to change that question from a “yes/no” to “provide the business cases.”

A4.8, A4.9 and A4.10 ask about whether the configuration settings are available over the internet and if so, how are they protected. This may be a common configuration if using a managed service provider.

Finally, A4.11, A4.12 and A4.1.1 ask about software firewalls. A4.11 and A4.12 ask whether they are configured on devices and if not, why not. A4.1.1 is has been added in this version of the question set and asks how the firewall controls are in place when devices are not on the internal network. The answer in the guidance is to either use “a corporate virtual private network (VPN) connected to your

office network [or] to rely on the software firewall.” This contains the same erroneous assumption about split-tunnel VPN described in the scoping section. This should be clarified or changed.

9.2.3 Secure Configuration

A5.1 asks whether all software and services that are not used have been removed. This is an excellent question as it implies a software review process needs to be in place and that devices are managed. The guidance is less good:

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

Figure 5 CE Inventory

This advice does not scale and does not provide any assurance. Applications may be installed but only show on other user profiles. Compare with the more comprehensive guidance from ACSC Essential Eight:

Below is a PowerShell script to output a list of installed applications with registered uninstall functionality. This list should be reviewed in conjunction with the list of installed applications within 'Control Panel – Programs – Programs and Features' to ensure no applications are missed.

```
function Analyze( $p, $f) {
    Get-ItemProperty $p |foreach {
        if ((($_.DisplayName) -or ($_.version)) {
            [PSCustomObject]@{
                From = $f;
                Name = $_.DisplayName;
                Version = $_.DisplayVersion;
                Install = $_.InstallDate
            }
        }
    }
}

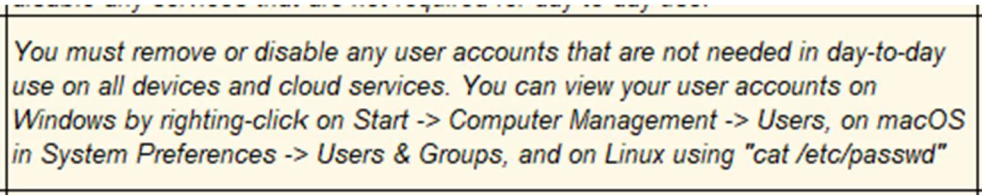
$s = @()
$s += Analyze 'HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\*' 64
$s += Analyze 'HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\*' 32
$s | Sort-Object -Property Name
```

The combined list of installed applications must be reviewed alongside the date of release for each application patch to determine whether the timeframe has been met.

If tools cannot be used, request a demonstration that shows the versions of installed applications and their install date. This allows for manual checking against the latest versions available from vendors.

Figure 6 Essential Eight inventory

A5.2 asks whether unnecessary user accounts have been removed. Again, the guidance is simplistic and cannot scale on Windows, but does provide some assurance:



You must remove or disable any user accounts that are not needed in day-to-day use on all devices and cloud services. You can view your user accounts on Windows by right-click on Start -> Computer Management -> Users, on macOS in System Preferences -> Users & Groups, and on Linux using "cat /etc/passwd"

Figure 7 Accounts guidance

A5.3 is another question about whether default passwords have been changed which is very similar to that in A4.2. This repetition appears again in A5.5 about password length and extra factors which is almost a verbatim copy of A4.3. And A5.6 asks for a description of “the process in place for changing passwords when you believe they have been compromised” which is very similar to A4.4 “do you change the firewall password when you know or suspect it has been compromised?” The password management questions in the firewall section would sit better here as they are about secure configuration.

A5.4 “Do you run external services that provides access to data (that shouldn't be made public) to users across the internet?” is very similar to A4.5 “Do you have any services enabled that can be accessed externally through your internet router, hardware firewall or software firewall?” Both of these questions are of the “yes/no” type with no follow up. It should be viewed in combination with A5.7 about how this external service is protected from brute forcing if MFA is not being used.

A5.8 asks whether there is a documented password policy for the external service with a yes/no answer. A simple improvement could be to ask for the document.

A5.9 asks whether “auto-run” has been disabled on all systems. This question is an outlier – the requirements document explicitly states that USB devices are out of scope, yet the guidance talks about stopping this from happening on a “DVD or memory stick.”

9.2.4 Security Update Management

This section runs from A6.1 to A6.7 and, like the scoping section, contains a lot of asset management. Applicants are expected to list all of the following within the scope:

- A6.2.1 Internet browsers
- A6.2.2 Malware protection
- A6.2.3 Email applications
- A6.2.4 Office applications

These are in the context of whether these applications will be eligible for security updates. A6.1 and A6.2 ask if all operating systems, firmware and software are supported and get regular security updates. A6.6 asks the follow up question about whether this software is removed when it is no longer supported. A6.3 asks whether the software is licensed correctly and this is important as unlicensed software may be excluded from updates.

A6.7 in an ‘information only’ question asking about what happens to unsupported software and how the applicant has mitigated the risk. The guidance states that it needs to be moved to a separate sub-set segregated via firewall or VLAN – this has all the problems examined in the scoping section.

A6.4 through A6.5.2 deal with updates.

9.2.4.1 14-day patching and Availability

A6.4 asks that “all high-risk or critical security updates for OS and firmware are installed within 14 days.” A6.5 asks the same of applications and plug-ins such as Java and Adobe Reader with guidance:

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

Figure 8 Update guidance

Aside from the obvious issue where a computer isn’t on for two weeks, there are many reasons why this is unlikely to be achievable at all times. Microsoft’s own figures from 2021 show that on-prem managed devices only achieve 55% patch completion within 14 days and up to 80% completion within 28 days (Microsoft, 2021). This is an unachievable target based on figures from the dominant OS vendor.

NCSC also have an article about the risks of patching (NCSC, 2019) where scale is acknowledged:

For small companies, a failed patch roll-out is painful. For large organisations, it can cause as much impact as a cyber attack, stop thousands of people from working, and require massive resources to fix.

Consider an update that has a 1% failure rate that causes the operating system to be unresponsive or have some other business impact. Here’s what that looks like for various sizes of organisations:

Devices	Failures
10	0 to 1
100	1
250	2 to 3
5,000	50
15,000	150
50,000	500

Figure 9 Impact of a 1% failure rate

For a small organisation with 250 devices or less, the result of this failure could be dealt with by a single person. For a large organisation the numbers start to become a major incident – the *impact* is greater. Although the increase in failure rate may be linear, the number of support staff available to deal with the failures is not – a large organisation will use economies of scale and a management tool to deal with larger numbers of devices. If the patch breaks the operating system or the management tool this will need to be dealt with manually and they are unlikely to have enough staff to deal with it. And due to the diverse amount of software and configurations seen in large organisations the *likelihood* of an adverse patch causing a problem is greater than in an SME. Consider the classic risk assessment metric:

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

As can be seen from the numbers above the risk increases as the organisational size increases. What is low risk in an SME becomes a greater risk in enterprises.

Microsoft release security updates on the second Tuesday of every month, known as “Patch Tuesday” (Microsoft, n.d.). An out-of-band patch is one that addresses a serious problem that can’t wait until the following Patch Tuesday. While large organisations will broadly align to a 14-day patch

cycle there will be times when they will make a risk-based judgment to use a temporary *compensating control* instead, particularly when these patches are out-of-band.

Another example is described in the Essential Eight (ACSC, 2022) where an unpatchable “low-risk Windows server” could be run with compensating controls while a two-month decommissioning plan is implemented.

This has only considered operating system risk. Risk has also to be considered with regards to the number of different applications that may be in use in a large organisation and the combination of moving software parts that may be changed during an update.

This is not to say a 14-day target isn’t desirable. A more frequent cadence may possibly be better in many situations. But to have a blanket refusal to allow for risk managed outcomes is not helpful.

What makes this requirement all the more frustrating is the NCSC guidance on patching (NCSC, 2019) lists a set of defence-in-depth or compensating controls “when patching is hard or impossible.”

9.2.4.2 The problem with auto updaters

A6.4.1 and A6.5.1 ask about enabling auto updates for operating systems and applications. In a small office this would be acceptable as there is unlikely to be any other tool available to control updates. A6.4.2 asks what is done if auto-updates aren’t enabled on the OS and A6.5.2 asks the same for applications.

Application auto-updaters are problematic. Some, like the Java updater specified in A6.5 (Figure 10) ask for administrative rights during the update process.

A6.5	Are all high-risk or critical security updates for applications (including any associated files and any plugins such as Java, Adobe Reader and .Net.) installed within 14 days of release?
-------------	--

Figure 10 A6.5 Application updates

Assuming the guidance on accounts is followed the user will not have those rights and will be prompted to elevate (Figure 11). Unless they contact an administrator the software may never update. Even if they can install the update (Vaniea & Rashidi, 2016) have shown that they may be reluctant to do so. Other updates can be suppressed indefinitely as seen in Figure 12.



Figure 11 Java update elevation prompt

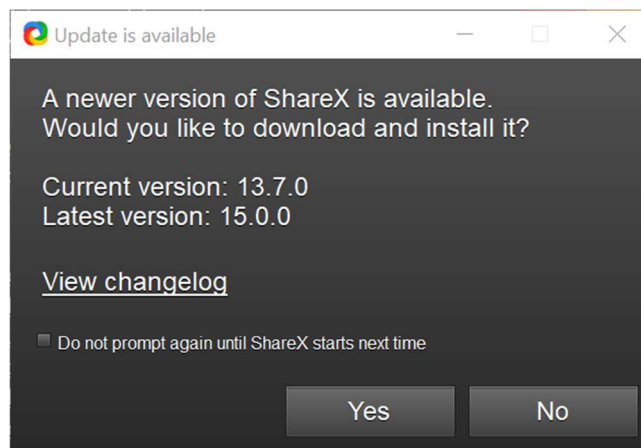


Figure 12 User driven update

Other auto-updaters take an alternative approach and run as system level services. This can introduce issues of their own, such as the SAP 750 updater allowing privilege escalation (packetstormsecurity, 2021).

Leaving updates to the endpoints means no control or visibility into the update process. A large organisation will have no guarantee that the update has taken place. The update processes make outbound connections and download executable files that, if run as a service, will install automatically with no guarantee what the update does. It could even install malware (pdfforge.org, 2012). Depending on the application this could use a considerable amount of data and bandwidth as every endpoint has to download their update over the internet.

An enterprise should require a management tool to control and validate these changes.

9.2.5 User Access Control

This section has the largest amount of questions. A7.1 to A7.4 deal with standard accounts, A7.5 to A7.9 with administrative accounts and A7.10 onward about protecting passwords from attack including A7.14 to A7.17 about MFA. From an assurance perspective most of these ask for descriptions of process instead of just a yes/no answer. Since some of these imply process documentation is in place then asking for a copy of that documentation would improve assurance.

A7.1 to A7.4 ask about process – is there an approval process before providing accounts, are accounts disabled or removed when staff leave, do they have the correct privileges and are all accounts unique. Apart from the unique account question all of these ask for detail – “describe the process.”

A7.5 asks whether there is a formal process for granting admin rights and to specify what it is. A7.6 and A7.7 ask how role separation is ensured – how non-admin accounts are prevented from carrying out administrative tasks and vice versa.

A7.8 and A7.9 ask about process – are the users with administrator access formally tracked and reviewed on a regular basis. However, unlike the others in this sub-section they are yes/no answers making them less robust.

The next sub-section has many questions that are similar to questions in other sections:

- A7.10 asks how the applicant protects against brute force password attacks which is almost the same as A5.7 for external services
- A7.11 asks about how password quality is technically enforced, very similar to A4.3 and A5.5
- A7.13 asks if the applicant has a “password policy that includes a process for when you believe passwords or accounts have been compromised?” which is similar to A4.4 and A5.6

A7.14 and A7.15 ask about MFA for cloud services – is it on all of them, and if not, list the ones that don’t have it.

A7.17 is another ‘information only’ question which was due to come into effect in January 2023 – “Has MFA been applied to **all** users of your cloud services?” This would appear to replace A7.16 which restricts the scope to “**all** administrators of your cloud services.” A7.16 appears to run contrary to the best practice advice from Microsoft concerning ‘break glass’ accounts (Microsoft, 2023). They suggest creating “two or more *emergency access accounts*” without MFA for situations when normal administrative accounts can’t be used.

A7.12 asks about how the applicant encourages staff to use good passwords. This appears to cover Security Awareness Training which is not meant to be part of the scheme. Perhaps it should be explicitly mentioned.

9.2.6 Malware Protection

This section provides three options to choose from to comply with. A8.1 asks whether anti-malware is installed, whether an approved set of apps is used via an app store or whether application sandboxing is used. At least one has to be used but all could be used in combination.

A8.2 and A8.3 ask about the anti-malware solution and its configuration. It has to update daily (which is not as often as some signatures are released) and to use on-access scanning. It is also meant to scan web pages but Windows SmartScreen is listed as an acceptable technology.

A8.5 asks about the app store and whether the applicant has a list of approved apps that are the only ones that can be installed.

A8.6 asks about sandboxing and how the applicant ensures the sandbox is separate from the rest of the network. This is the only question that allows for free text – the others are all yes/no answers.

The most interesting part of this section is that, unlike the rest of the scheme, alternatives are provided. Perhaps when revising the scheme NCSC and IASME could take inspiration from this section and apply it to the other controls.

9.2.7 Cyber Essentials summary

Too much of the SAQ is in yes/no format with no requirement for evidence. The guidance is simplistic, doesn't scale and sometimes provides little assurance. Furthermore, there are scope issues at scale.

Unless there is a significant amount of non-public guidance for the assessors it must be concluded that the CE certificate gives very little independent assurance. The positive, however, is that simple changes could improve the scheme dramatically.

9.3 The Assessors

In the research survey there were a number of comments about the quality or robustness of the audit process such as:

“we feel that the implemented controls/patching were not assessed appropriately”

“auditors vary wildly”

“assessors are often not qualified to assess in our experience.”

On that last point, let's consider what qualifies someone to carry out an assessment.

To carry out Cyber Essentials assessments a one-day training course is required at a cost of £500 (IASME, n.d.). In addition, “you will first need to have 3 years' experience of working in IT or Cyber Security”, “be based in the UK” and be required to pass an assessor skills exam. The assessor skills exam is waived if a candidate has one of the following certifications:

- (isc)2 CISSP
- ISACA CISM
- CCP SIRA, IA Auditor, or IA Architect at at least Practitioner level
- ISO27001 Lead Auditor

These are not entry level certifications. The CISSP is described as being for “experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles” ((isc)2, 2023). The CISM “indicates expertise in information security governance, program development and management, incident management and risk management” (ISACA, 2023).

For Cyber Essentials Plus a second one-day training course is required at a further cost of £500. The organisation must have a CE+ Lead Assessor who holds one of a number of penetration testing credentials. Others can carry out CE+ assessments if they meet the “3 years experience of working in IT or Cyber Security” requirement and pass IASME's Vulnerability Assessment Plus (VA+) exam. IASME provide further details about the exam on their website (IASME, n.d.) and explicitly state that

it “is a requirement for all Cyber Essentials Plus assessors that do not have a Lead Assessor qualification.” The learning objectives for the exam are:

- Understand Information security in the corporate world.
- Understand the laws and regulations involved with vulnerability assessing
- Understand **quantifying and measuring risks** associated with vulnerabilities
- Understand how to find internal and external vulnerabilities
- Understand how to test hardening measures for malware
- Report and explain vulnerabilities found throughout a project.

It is worth noting here that risk is explicitly mentioned as a learning outcome, and many of the qualifications that are acceptable for the CE role require an understanding of risk management. Another item worth noting by its absence is that of sampling and correctly defining a sample size. This will be explored later.

This means that there are 4 distinct categories of assessors

- CE assessors who have passed the IASME exam
- CE assessors who hold non-entry level qualifications such as CISSP
- CE+ Lead assessors who hold one of a variety of penetration testing qualifications
- CE+ assessors who have passed the IASME VA+ exam

At this point it is worth repeating a quote from the literature review from Chris Ensor (NCSC, 2021)

“whilst I’m sure there are many experienced Cyber Essentials assessors out there who can make [risk based] judgement[s], we have no way of knowing who they are.”

As can be seen from the above all assessors should be equipped to make risk-based judgements.

What is certain about these categories of assessors is that they will all have wildly differing initial experiences of IT and Cyber security. However, they should all have the ability to carry out an assessment based on a clearly defined question set and testing regime.

Note that there are additional requirements for the organisation that assessors work at but these have not been explored – this analysis was to provide context for the skills and background of the people who carry out assessments.

9.4 Cyber Essentials Plus

Scoping issues have already been discussed at length and the fact that how to scope a sub-set is not precisely defined may be one of the challenges for assessors.

For this portion of the analysis the Illustrative test specification (NCSC, 2022) will be used. Using this document is not without problems – this is not the exact test specification that will be used in practice. NCSC note that this document “exists to help the Cyber Essentials Delivery Partner develop their own test specifications for their Certification Bodies to carry out Cyber Essentials Plus assessments.” This made more sense before 2020 where NCSC engaged with a number of different Delivery Partners to run the scheme. However, since 1st April 2020 IASME have been the sole Delivery Partner (IASME, 2020) so this appears to be a historic quirk that has continued. There is no publicly available test specification from IASME so the NCSC sample will have to suffice.

The test specification has 7 test cases which an organisation has to pass to gain Cyber Essentials Plus

9.4.1 Scope

There are three technical scopes to apply in a Cyber Essentials Plus audit

1. The public facing IP addresses used by the organisation (including Infrastructure as a Service)
2. All cloud services used by the organisation
3. A representative number of devices in scope

The first is used for Test Case 1: Remote Vulnerability Assessment. The second is used for Test Case 6: Check Multi-factor authentication configuration. The final one is used for all other test cases and this is where confidence in the audit can be lost.

There is an issue with the scope of Test case 6 – it tests all cloud services that are in scope, but on “a representative number of devices.” And the largest issue is that what is tested is actually *a small number of user accounts* that use those sampled devices.

9.4.2 Sampling

9.4.2.1 Sample sizes – what is a “representative number”?

There is no official public guidance on how assessors should choose a sample size. However, it appears that multiple assessors have had the same guidance from somewhere. The following is found on the websites of Cyber Essentials assessors such as (IT Governance, 2022), (Indelible Data, 2021) and (Digital Origin, 2022):

Number of devices of each type	Sample Size
1	1
2-5	2
6-19	3
20-60	4
61+	5

Figure 13 Sampling guidance

Like other parts of the scheme the original source of this information does not appear to be public. It is possible that it could be from the IASME training. An unreliable source – a student’s flashcards for the IASME VA+ exam – can be found containing identical information to the above (Quizlet, 2021).

Whether or not this information is presented as part of the VA+ course lies at the heart of the problem with Cyber Essentials – inconsistency. If it is part of the syllabus then the sampling sizes are too small to be effective and will yield inconsistent results as will be shown shortly. If it is not part of the syllabus then assessors are making up their own guidance and sharing it among themselves.

A further uncertainty is who decides which devices are sampled – if this is the applicant then they can present devices guaranteed to pass.

9.4.2.2 Why do a manual check?

Before deciding to sample, (The Institute of Internal Auditors Australia, 2023) state that “whenever information is in electronic form the auditor’s first consideration” should be to use techniques that “can test all members of a population for an error condition” or anomalies. Since many of the CE+ tests can be automated and run across all of the scoped devices this should be preferred method.

9.4.2.3 Building a better sample

The problem with the above sample sizes becomes clear once one considers enterprise scale.

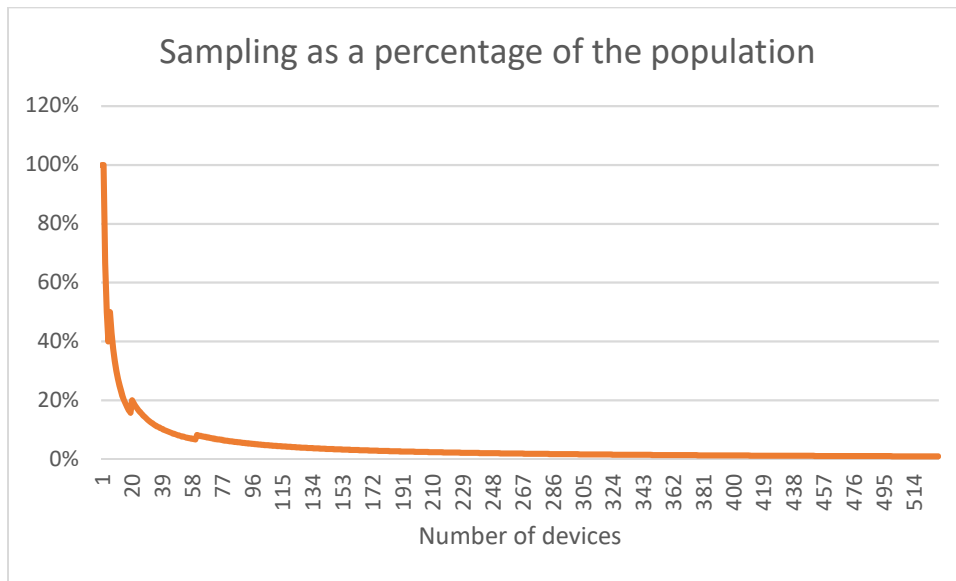


Figure 14 Sampling as a percentage of population

Once an organisation has over 500 devices the percentage of sampled devices drops below 1%. The guidance states sampling has to be “representative of all the devices in scope” so for any organisation above 500 devices extra assurances should be provided that these devices are representative.

As has already been seen, large organisations use tools like SCCM to set and validate their security controls. A simple way to improve the confidence of the audit is to ask for screenshots of the management tool. The burden would be on the applicant with no additional hands-on time for the assessor. This would allow stop-and-go sampling (AccountingTools, 2023) to be used, reducing the sample size.

Another point to consider is areas where control variance might occur. In a large organisation this is unlikely to be found between Windows versions (for example between 20H2 and 21H2) but instead found between 'builds.' A standard desktop model for the HR department is likely to have the same controls applied across differing iterations of Windows 10 in a consistent way via Active Directory Group Policy. These may differ from the controls applied to the Finance department on the same version of Windows (Microsoft, 2021). Representative devices should therefore not necessarily be selected by OS version, but in consultation with the applicant on the build types they have in their environment.

9.4.3 The Tests

The Evendine version of the standard introduced two new tests which were not present in previous versions. The following table summarises the tests alongside scope, control and SAQ question.

Test Case	Scope	Control	Question
Remote vulnerability assessment	All internet facing IP addresses	Firewalls	A4.1
Vulnerability scan of devices	Representative sample	Security Update Management	A6.4, A6.5, A6.6
Malware protection	Representative sample	Malware protection	A8.2 (partial), A8.4, A8.6
Malware delivered by email	Representative sample	Malware protection	A8.2 (partial)

Malware delivered through website	Representative sample	Malware protection	A8.3 or A8.2 (partial)
Multi-Factor Authentication	All cloud services	User Access Control	A7.16 A7.17
Account separation	Representative sample	User Access Control	A7.6

Figure 15 Tests aligned with Scope and Control

It should be clear from the above table that only 4 of the 5 controls are being tested. And of those only a small number of questions from the SAQ are tested. There may be an assumption that the answers given in the CE SAQ would be robustly tested. This is not the case and, as will be seen shortly, some being tested can't provide assurance for large organisations due to sampling issues.

Another point to note is although the tests *can* align to these questions, there are alternative ways of passing the tests. An example is the "malware delivered through website" test where standard on-access scanning antimalware is used but without the ability to warn about the malicious website as described in A8.3. This would mean a pass on that test in CE+ but a fail on the question in CE.

9.4.3.1 Test Case 1: Remote vulnerability assessment

Of all the tests this is the most robust since it tests all the externally facing IP addresses of an organisation. Due to this it has no issue with scale and offers good assurance that this control is in place *externally*. Unfortunately, it neither tests nor offers any assurance that the other components of this control are in place. In particular software firewalls on endpoints and servers are not tested which leads to a weakness in this part of the assessment.

If an end user device is taken outside the internal network and the software firewall is off then this leads to a possibility of bringing malware back to the internal network when that device returns.

9.4.3.2 Test Case 2: Check patching, by authenticated vulnerability scan of devices

This test uses an approved vulnerability scanning tool to find vulnerabilities on devices that are 'critical' or 'high risk' or have a CVSS v3 score of 7 or above or if the vendor hasn't published details. If a patch has been out for more than 14 days then this is a fail. Aside from the inventory questions this provides good coverage of the requirements within the Security Update Management control.

This test could improve its confidence if it was run on all devices in the sub-set but this could have operational implications.

The main problem with this test is the lack of compensating controls such as blocking network access or disabling an affected component while an upgrade process takes place.

9.4.3.3 Test Case 3: Check malware protection

This test is split in three for each type of malware protection that may be in use. For antimalware software it only checks that the definitions are less than 24 hours old and the engine has been updated within the last 30 days (if applicable). The scanning component of A8.2 is checked in other tests.

For application allow listing the checks comprise:

- Ensuring the trusted root certificates are what shipped with the OS or a subset
- Any other root certificates were knowingly added
- Unsigned and unchained executables do not run
- Code signing applies to all file formats

This is comprehensive but doesn't validate that there is a list of approved applications. This is asked about in A8.5 as a yes/no question, so there is no validation that such a list exists

For sandboxing the check is vague – “application sandboxing is operational and applies to all user-installed applications.” Unless this is clarified this is another area where assessor discretion (and variability) could come in.

All checks are manual but could be automated allow for increased sample size.

9.4.3.4 Test Cases 4 and 5: Check effectiveness of defences against malware

Both test cases test the ability of the infrastructure to defend against malware based on file type extensions. The list of extensions is not publicly available although there are guidance notes for the Delivery Partner in Appendix B of the requirements. Crest, a former Delivery Partner, published a list alongside their original test specification which is noted in Appendix 2 of this paper. This lack of transparency means that potential applicants have no way of knowing what will be tested in advance. The list has some surprising omissions such as .vbs (vbscript), and .iso which can be used as containers for malware (ACSC, 2022). Also missing is any mention of an exception process where 'suspect' filetype is actually required as a function of the business such as blocking the ability to download .py files for developers that use a web-based change management system.

The tests are carried out by sending the test files via email to an account belonging to the applicant (the email test), and by attempting to download them from a CE test website on each web browser installed on each sampled device (the download test).

Neither of these tests will be a full test of the antimalware software as email filters may block some filetypes and technologies such as Microsoft SmartScreen may block different downloads before the on-access scanner gets a chance to run.

USB devices are explicitly mentioned as being out of scope but as noted above the A5.9 question on auto-run shows that they are a concern. A simple improvement to this test is to have the samples on a write-protected USB stick and to test execution from there.

This test doesn't scale well so stop-and-go testing would be recommended here if there were sufficient validation that the settings were identical across the rest of the sample set.

9.4.3.5 Test case 6: Check Multi-factor authentication configuration (MFA)

This test is supposed to validate that MFA is configured on all cloud services. As mentioned in the scope section what it actually tests is whether the small number of sampled accounts have MFA configured.

The test is carried out on untrusted devices or on trusted devices using a private browsing session. If neither of these is an option it is carried out on the assessors machine within a private browsing session. Discounting any risk that the untrusted devices bring to production accounts, this can't validate anything other than MFA being enabled on this small sub-set of accounts.

The test is therefore subject to sampling issues – due to enterprise size and the risk posed in entering credentials into untrusted devices it is unlikely that any of the C-suite's accounts or any admin accounts will be sampled.

A better check would be to look at the MFA configuration and for the assessor to satisfy themselves that the configuration is correct and applying to all users. The existing check could then be used with stop-and-go sampling to verify that the technology is functional. Although the survey didn't ask

which MFA technology was in use an informed assumption would suggest that guidance for the Microsoft solution could be provided to assessors that would cover a large base of applicants.

9.4.3.6 Test case 7: Check account separation (Admin Rights)

This test requires interactively launching a process that requires administrator access. If it runs, or if a password box appears and the credentials for the account that is currently logged in allows it to run, then a fail needs to be recorded.

This check has to be run interactively and provides little assurance unless the sample size is very large.

A fundamental problem with this test is that the guidance is to choose a sample of *devices* when the it would be better tested with a sample of *users*. Even this would provide little assurance as a primary way of granting administrator rights on Windows devices is to place the domain account in the local Administrators group. A simpler check would therefore be to check what accounts or groups are present in the local Administrators group on Windows (or the similar admin group on MacOS). This could be scripted and run on all devices in scope giving a high level of assurance.

Another issue with this test is that it doesn't test whether tooling that can elevate users on demand is being used – this will be explored further later on.

9.4.4 Cyber Essentials Plus summary

A number of these tests are only testing whether industry standard technologies are working as advertised instead of whether the configurations are correct. Test 6 and 7 appear to have been added with little thought of their assurance problems at scale.

9.5 Communication issues

Most of the survey responses were critical of scheme communications and one even noted they were “not compatible with the business and financial processes of large organisations.”

9.5.1 Documentation

As a comparator PCI DSS is useful here – like Cyber Essentials it's a compliance framework with variety of documentation and guidance available. For Cyber Essentials this is not all held in the same place. Some is available from (NCSC, n.d.) or (IASME, n.d.). Clarification and date changes can be found in blogs from (NCSC, 2023) and (IASME, 2023). Sampling guidance is found across multiple assessor blogs (see above) and some information (like filetypes) isn't public at all.

PCI DSS solves this problem by having a document library. On the document library landing page (PCI Security Standards Council, 2023) there are 15 documents available including a copy of the standard, a summary of changes from the previous version, general guidance, a glossary, the forms required by the scheme and frequently asked questions. The page can be filtered to view archived scheme documents dating back to version 1.1 from September 2006. In total 373 current and archived documents are available.

There is also a risk here that if NCSC change delivery partner in future that some of this documentation may be lost since it is hosted on the IASME website. A website that is run independently of the delivery partner would also mitigate the risk that a commercial entity may delete archived documentation at a later date.

9.5.2 Carelessness

Some survey responses noted “contradictory” communication, “miscommunication” and “misinformation”. Proof-reading communications may help as there are examples of mistakes across multiple channels.

First of all, an IASME blog post (IASME, 2023). Figure 16 shows the leaking of the source of this NCSC URL as Tom.H@ncsc.gov.uk via Outlook safelinks:

<p>3. A link to the NCSC’s BYOD guidance added for information</p> <p>For further information and advice on the use of BYOD, please see the NCSC’s guidance.</p>	
<p>4. Clarification on including third party devices</p> <p>All end user devices that your organisation owns and that are loaned to a third</p>	<p>The screenshot shows a URL from Outlook safelinks protection. A red rectangular box highlights the email address 'Tom.H@ncsc.gov.uk' within the URL's data parameter.</p>

Figure 16 Data leakage from IASME

Carelessness is seen in the question set and the requirements documents. Figure 17 shows differing sizes of Calibri, some styled and some not:

A4.2	When you first receive an internet router or hardware firewall device it will have had a default password on it. Has this initial password been changed on all such devices?	Th V
A4.2.1	Please describe the process for changing the firewall password?	Y bi
A4.3	Is the new firewall password configured to meet the Password-based authentication requirements? Please select the option being used A. multi-factor authentication, with a minimum password length of 8 characters and no maximum length B. Automatic blocking of common passwords, with a minimum password length of 8 characters and no maximum length C. A password with a minimum length of 12 characters and no maximum length	A ar Es ht
		Pt

Figure 17 Font differences

This may cause accessibility issues because screen readers look for styles to aid navigation in documents (Gov.UK Central Digital and Data Office, 2023). This is replicated albeit in a very minor way in the test specification:

<p>Test Case 1: Remote vulnerability assessment</p> <p>Test Case 2: Check patching, by authenticated vulnerability scan of devices</p> <p>Test Case 3: Check malware protection</p> <p>Test Case 4: Check effectiveness of defences against malware delivered by email</p> <p>Test Case 5: Check defences against malware delivered through a website</p> <p>Test case 6: Check Multi-factor authentication configuration</p> <p>Test case 7: Check account separation</p>
--

Figure 18 Mixed case

The lack of care in the presentation of the scheme is in contrast with PCI DSS or Essential Eight. At a minimum the accessibility issues should be investigated and fixed.

9.5.3 Nomenclature

The naming and versioning of the scheme may be a further cause for confusion. The previous, current and future versions of the scheme are named:

- Beacon – previous
- Evendine – current
- Montpellier – future

The documentation for these versions may also reference a version number, such as 2.0 or 3.0. There does not appear to be any kind of pattern to this – the first letter of each word doesn't increase in a sequential manner as seen in Google's Android versioning. For a layperson it is difficult to know the current version of the standard since name and number are used interchangeably.

Compare this with PCI DSS:

- 3.2 – previous
- 3.2.1 – current
- 4.0 – future

There are no code names, just the version number. This numbering scheme is not the only way to version a standard, ISO 27001 uses years and amendments to publish updates (ISO, 2022) such as

- ISO/IEC 27001:**2005**
- ISO/IEC 27001:**2013**
- ISO/IEC 27001:**2022**

Cyber Essentials appears to undergo an annual review so therefore versioning it based on year and dropping the codenames would improve clarity of communication.

A further issue that causes confusion is the difference between Cyber Essentials the scheme, Cyber Essentials the certificate and Cyber Essentials Plus. Some assessors have started to describe the base certificate as Cyber Essentials Basic (IndelibleData Ltd, 2022) to help differentiate between them.

9.5.4 Timing and transition periods

As the research for this paper progressed the latest version of the scheme was announced on 23rd January 2023 and it was due to come into force on 24th April 2023 (IASME, 2023). This is 13 weeks' notice. As was seen in the survey a number of responses mentioned the theme of an "overly short time to implement" scheme changes, so something should be done to address this. IASME state that any assessments started before 24th April 2023 can certify against the previous question set but there is presumably a time limit on completion although this is not noted by IASME.

In Evendine there are three questions marked 'information only' with a requirement date of January 2023 – A2.4.1 on thin clients, A6.7 on moving unsupported software to a sub-set and A7.17 on MFA for all devices:

This question is currently for information only. From January 2023 this question will require that your thin clients are supported and receiving security updates and will be marked for compliance. Thin clients are currently in scope for all other controls.

Figure 19 A2.4.1 Thin client guidance

This question is for information only. From January 2023 this question will require that all unsupported software have been moved to a segregated sub-set and internet access removed and will be marked for compliance.

Figure 20 A6.7 Unsupported software guidance

This question is currently for information only. From January 2023 this question will require that all user accounts are protected by MFA on cloud services and marked for compliance.

Figure 21 A7.17 MFA guidance

PCI can inform here – it has the concept of future dated requirements which are designed explicitly to "give organizations additional time to complete their implementations" (PCI Council, 2021).

Interestingly the future dated requirement is noted as best practice until the point in which the date is reached. Once that date is reached it then becomes mandatory. If this was adopted by Cyber Essentials (with sensible future dates) it would allow the scheme to have clearly defined transition periods for enterprises and directly address some of the criticism seen in the survey. This would also help improve cyber security budget and operations planning.

9.5.5 Engagement

Several of the survey respondents stated that communication felt "one-way". An example of this was seen with the changes to BYOD requirements – a seemingly simple clarification had wider budgetary and resourcing impact for enterprises.

This should have been easy to catch if the authors had engaged with enterprises before making the clarification. Again, PCI DSS can show a way forward here. It has a clearly defined RFC process with a web page featuring all current RFCs and who can participate in them (PCI Council, 2023).

9.5.6 Assessors

To directly address the issue of variations in assessor quality and lack of publicly available information about the scheme another part of PCI DSS should be considered.

The PCI council have two kinds of assessors – external and internal. The use of an internal Cyber Essentials assessor could be a quick way to improve the quality of enterprise assessments, and improve communication and engagement.

The external PCI assessor is called a Qualified Security Assessor (QSA) while the internal is named Internal Security Assessor (ISA). Importantly both go through the same training and exams (Network Assured, 2023). The main difference is that an ISA can only sign off on behalf of the company they work for while a QSA can sign off on any company that contracts with them.

For CE the training and exam are already in place and could be offered to Internal Assessors (IA) with minimal changes. The main issue would be deciding how the IA would engage with the External Assessor (EA).

This would allow enterprises to prepare their SAQ returns to a standard that would make external assessments easier since all the evidence would be already gathered internally. EAs would have named contacts within enterprises with a deep understanding of the scheme.

Another benefit would be a strong feedback loop between enterprises and the NCSC and the delivery partner. IAs would be (or should be) party to the same internal information as the current EAs and issues with changes could be identified and dealt with early.

9.6 What's missing?

9.6.1 Evolution to address modern low skill threats

Cyber Essentials was launched on the 5th June 2014 with the express intention of allowing organisations to “show consumers that they have measures in place to help defend against common cyber threats, such as the recent GOZeuS and CryptoLocker malware attacks” (UK Government, 2014).

The CryptoLocker ransomware was primarily delivered via email and infected single computers (NCA, 2013). Contrast this with the propagation methods of NotPetya from 2017:

- Email
- Microsoft networking with known credentials
- Exploiting vulnerabilities in the SMBv1 protocol

The key difference here is that modern low skill threats can rapidly spread laterally, particularly in a Microsoft Active Directory network. This can pose an existential threat to a business, especially for one without backups (which are not a requirement of the scheme).

As IASME are keen to point out Cyber Essentials hasn't changed over the years. It should.

9.6.2 Lateral movement

Part of the reason ransomware like NotPetya can be so devastating is that it can spread rapidly round a network. CE does allude to this by suggesting firewalls or (presumably non-routable) VLANs for sub-sets. As has been seen above, these would still not prevent some lateral movement.

A minimum recommendation therefore is unique administrator passwords for every device. A5.3 alludes to this in the guidance note but it should be explicit considering the risk. Microsoft offer free tools to facilitate this (Microsoft, 2023).

9.6.3 Backups and encryption

Another oddity of the scheme is that this sentence from early versions of the standard still applies:

“This document does not cover supporting detective and recovery controls or the management of information risk”

In 2014 it may have seemed reasonable to exclude backups from the scheme but with ransomware the top risk to UK businesses it seems odd that the question “Do you back up your data” is missing from the current SAQ.

Notably absent too is an encryption requirement. Reading corporate data on a CE+ device left on a train is trivial if encryption isn’t used. This is especially concerning considering the number of government laptops that are lost or stolen (ComputerWeekly, 2021).

9.6.4 Compensating controls

PCI DSS has the concept of a compensating control. This allows an organisation to claim that they can’t meet a requirement because of “legitimate technical or documented business constraints” (PCI Security Standards Council, 2018) but have mitigated the risk through other means.

Allowing compensating controls could allow enterprises to meet the spirit of the scheme without meeting some of the requirements that only scale to small businesses.

Interestingly Cyber Essentials used to allow compensating controls. In the QG SAQ (Indelible Data, 2017) they state:

*Take steps as necessary to **ensure that your organisation meets every requirement**, throughout the scope you have determined. If you can’t, highlight any **compensating controls** you have put in place to mitigate the risk.*

There appears to be no public statement on why this was dropped. This may be another factor explaining why large organisations that had previously certified are now finding it increasing difficult.

9.6.5 USB sticks

One problem noted in the Firewall section is that of taking a device away from the trusted network, it being infected, then being brought back to the internal network where the malware spreads. A very similar threat model occurs with USB sticks which are explicitly stated as being out of scope for Cyber Essentials.

Consider an employee who uses a USB stick to transfer files between the office and their personal PC at home. The personal PC is out of scope for Cyber Essentials since it does not connect to the network defined in the Scope or sub-set. This home PC could be running with no firewall or antimalware, fully compromised and so malware could be introduced by transferring work documents between this untrusted zone back to the trusted zone.

A5.9 partly addresses this risk by asking for auto-run to be disabled, but does not address infected documents or executables. This risk should be explicitly defined as part of the standard.

9.6.6 Evidence

It’s hard to tell whether evidence gathering was just a feature of early versions of the scheme or a feature of other Delivery Partners but now appears missing. This is probably the biggest reason it can’t be used for assurance and would be the easiest to solve. The Former Assessor noted:

“Since it moved to IASME the scheme lost some of its benefit. The main one being not having to provide proof of what you’re saying. [Before IASME] if we were marking and there was no evidence we wouldn’t accept the answer.”

This is backed up by an earlier question set from QG – a former Delivery Partner. From their CE questionnaire used by the assessor (Indelible Data, 2017):

*“As a Cyber Essentials scheme Applicant, you must ensure that your organisation meets all the requirements. You are also required to supply various forms of evidence before Indelible Data Ltd can award certification at the level you seek. Please use **screen grabs** and **insert policy notes** where possible.”*

This was also a concern from one of the respondents in the survey:

“It would be better to demonstrate the policies both paper and technical to show how we comply and if there are areas for improvement”

It would improve the level of assurance markedly if this was re-adopted. Additionally, guidance for assessors on what is acceptable would help address assessor variability.

9.6.7 Operational guidance

NCSC provide operational guidance on how to secure various operating systems. Since Windows was the dominant OS from the survey the Windows guidance was examined (NCSC, 2021). The guidance is relatively high level but has reference group policies (GPOs) available (NCSC, 2022).

A fresh install of Windows 20H2 was installed as per the guidance and the GPO was applied.

The guidance provided would not pass the Cyber Essential Plus test.

In particular the CE+ Test 5 failed in part because the list of prohibited file types was missing.

9.6.8 Vendor guidance

It has already been mentioned that requirement A7.16 appears to run contrary to the best practice advice from Microsoft concerning ‘break glass’ accounts (Microsoft, 2023) but other requirements also seem to run contrary with commercial products sold as security solutions.

In the scope section it was shown that the VDI guidance appeared at odds with the reference architecture for BYOD from Citrix (Citrix, 2022).

Microsoft have introduced Endpoint Privilege Management as part of their top tier endpoint management and security suite (Microsoft, 2023). This allows users to elevate their day-to-day account on demand to carry out administrative tasks. This is explicitly prohibited in A7.6 “you must use a separate administrator account from the standard user account,” A7.7 and CE+ test 7.

These are premium solutions from leading vendors. Before UK organisations invest in these solutions it should be clarified whether they are compliant with CE.

10 Conclusions and recommendations

It should be clear after the above analysis that there are significant issues with Cyber Essentials when applied at scale. It should also be clear that small changes to CE should alleviate many of these issues. These can be broken down as follows

10.1 Restore parts of the scheme

From the publicly available information it appears that older implementations of the scheme addressed current concerns large organisations have on assurance and controls, so the obvious conclusion to address these concerns is:

Recommendation 1: Revert back to insisting on screen grabs for evidence, with guidance on what is acceptable evidence

Recommendation 2: Revert back to allowing compensating controls to mitigate risk when requirements can't be met

A more radical option is to revert back to having more than one Delivery Partner. If IASME have difficulty accommodating the above recommendations:

Recommendation 3: Implement a second Delivery Partner to focus on large organisations or organisations who need greater assurance. Let IASME continue to work with SMEs

Bringing the entire scheme in house to the NCSC should also be considered but due to the current scheme set-up this is unlikely to occur.

10.2 Scope issues

Both the SAQ and the audit have difficulty defining an appropriate scope for a large organisation. The SAQ allows a sub-set to use the same Active Directory domain as the rest of the organisation. By definition this means the sub-set can be trivially compromised by the remaining parts of the organisation if the Active Directory is compromised. Additionally, VLAN segregation should not be considered a valid security boundary if it is routable. These lead to:

Recommendation 4: If Active Directory is used then the entire AD Domain should be included when defining a sub-set

Recommendation 5: If a VLAN is used to define a sub-set ensure inter-VLAN routing is disabled or, if not, that a firewall is in place

10.3 CE issues

A number of questions ask very similar questions for no apparent reason across different sections. In some they are almost verbatim (A4.3 and A5.5). This leads to:

Recommendation 6: A full review of the question set should be undertaken to see if parts can be simplified or consolidated – in particular the password management for firewalls questions could be moved into the Secure Configuration category

Many questions have yes/no answers where an explanation would offer more assurance, leading to:

Recommendation 7: Where documentation is presumed to exist, as in A5.8 “do you have a documented password policy,” ask to see it instead of just accepting yes as an answer

10.4 CE+ issues

Further issues are seen in the audit. In five of the seven test cases the percentage of sampled devices drops below 1% for any business over 500 devices. It would be impractical for an assessor to look at enough physical machines so this leads to:

Recommendation 8: If the organisation or sub-set has more than 500 devices then a management tool should be used to configure the security controls

Recommendation 9: If the organisation or sub-set has more than 500 devices then screenshots and an explanation of how the management tool configures the controls should be provided to the assessor

By definition the management tool can manage the security controls on devices, therefore:

Recommendation 10: If a management tool is used within a sub-set then all devices connected to that instance of the management tool should be considered part of the same sub-set

The test cases for CE+ do not cover all the components of the controls and in some cases miss critical ones, leading to:

Recommendation 11: Software firewalls on laptops should be checked to ensure they are on and correctly configured

Additional checks using the management tool would increase the audit time, but intelligent sampling could help such as:

Recommendation 12: Use stop-and-go sampling to reduce the sample size when the management tool backs up initial findings

10.5 Communications

Communications from NCSC and the Delivery Partner, IASME, leave little time for larger organisations to implement changes – most acutely the clarification around MDM/MAM had non-trivial financial and resourcing implications. Additionally, the actual test documentation is not published, only the NCSC illustrative one. This leads to the following:

Recommendation 13: NCSC should ensure that the Delivery Partner publish the actual test specification

Recommendation 14: NCSC should follow the lead of the PCI Council and ISO 27001 in running two versions of the scheme concurrently – the newer version being best practice until the retirement of the old version

To improve the communications with large organisations, to speed up the assessment process and to allow for compensating controls:

Recommendation 15: Create Internal Assessors using the existing IASME coursework and exams

10.6 The missing control: Asset Management

Over 10% of the questions in the SAQ are to do with hardware and software asset management. No enterprise could answer these questions accurately without an asset management system. NCSC provide guidance on this and why it should be considered important (NCSC, 2021). The questions have been noted in other parts of this paper but listing them together demonstrates the importance of Asset Management to the scheme:

- A2.4 Laptops, Desktops and Virtual Desktops
- A2.4.1 Thin clients
- A2.5 Servers, virtual servers and virtual server hosts
- A2.6 Tablets and mobile devices
- A2.8 Network equipment
- A6.2.1 Internet browsers
- A6.2.2 Malware protection
- A6.2.3 Email applications
- A6.2.4 Office applications

The NIST framework treats asset management as the foundation of good cyber security and the first of five key functions (NIST, 2021). Cyber Essentials encompasses this but in a jumbled manner under separate headings. Explicitly defining Asset Management as a control would bring visibility to how critical a function of cyber security it actually is.

Moving these asset questions out of the Scope and Software Update sections leaves them highly focused. This allows for more targeted analysis of those sections by the assessor. This also allows the assessor to gauge how well the applicant performs asset management and could lead to explicit questions in the SAQ asking about the source of the information. This leads to the following:

Recommendation 16: Define Asset Management as an explicit control

Recommendation 17: Add questions asking for the source of the asset information and when it was gathered

10.7 Nudge

One conclusion to these findings that can't be discounted is that all of this is by design. Consider that CE:

- was "designed in consultation with SMEs" (HM Government, 2015)
- has scaling issues above 500 devices
- is run in partnership with an organisation whose *very name* contains the phrase **Small to Medium Enterprise**

Perhaps CE *is* designed just for SMEs. On this subject the Former Assessor said the scheme authors had a problem to solve.

"[They thought] how do we make small businesses take it? For them to make that happen, they thought we'll push it to larger businesses then the small ones will follow."

In short, a **nudge**.

The UK Government created a Behavioural Insights Team or 'Nudge Unit' in 2010 to improve policy outcomes by considering human behaviour when designing messaging. (Halpern, 2015) describes how writing the words "most people pay their tax on time" in tax bills boosted repayments.

Consider the messaging from the UK Government about Cyber Essentials within this context:

Simple but effective.

Basic cyber hygiene.

For all organisations, of any size in any sector.

If the scheme were complex, or targeted specifically at SMEs, it would be a barrier to adoption. A simple, universal scheme is a lot easier to sell to SMEs.

10.8 Future Work

The NCSC was created in 2016 to bring together several existing organisations to "provide a unified national response to cyber threats" (ico., n.d.). In this context why is such an important baseline provided by a third-party? Examining the risk this brings and whether other nations have adopted a similar approach would be helpful. IASME, for example, provide their own governance standard that features fundamentals missing from CE. Is it in their commercial interests to bring these to CE?

Taking this idea further, another question arises – why are there multiple national schemes instead of a definitive international one? An examination of other national schemes and their common features could shed light on this. Collating examples such as the practical guidance to address modern low-level threats and maturity model from ACSC Essential Eight would help create a library of best practice.

Perhaps there is a better way to implement the CE scheme than what is there at present. This paper was focused on minor adaptations to the current scheme but perhaps a reworking from scratch based on the requirements would be more suitable for modern cyber requirements. An obvious missing component to this research is looking at Zero Trust (Microsoft, 2023). The scheme has an antiquated view of networks where there is a hard perimeter and a soft inside, so looking at this might be fruitful.

Another finding from the research is that as the size of the organisation increases the impact and likelihood of a patch failure increases. A closer examination of the other risks of a blanket security baseline on a large organisation would be interesting. (Barlette & Fomin, 2008) suggest the need for two different schemes so is this actually true? This paper has suggested improvements to CE but is it unfixable?

The 2021 clarification for BYOD devices has required large organisations to implement MDM/MAM. It should be possible to quantify whether this has resulted in spend being diverted from projects that may have addressed larger risks in enterprises in order to get a certificate. Has this pushed back projects designed to prevent lateral movement for example?

11 Final thoughts

The premise of this research was to try to understand why a large organisation could suffer a cyber-attack despite holding a valid Cyber Essentials Plus certificate. Some broad themes have surfaced.

On the first research question – can the scheme be used as an independent measure of assurance? – (Such, et al., 2019) noted that it requires “almost perfect adherence to the guidelines for implementing [the] security controls.” The basic SAQ doesn’t require screenshots and is not further examined in the Plus assessment. The Plus assessment has confidence issues at scale and doesn’t test all the controls. The only conclusion to draw is that the scheme cannot be used as an independent measure of assurance.

The second research question – does it have issues with scale? – is equally easy to answer. Whether it is naivety with VLANs, VDI or VPNs, the lack of consideration of lateral movement and AD, or something as simple as defining a sample size, the scheme has significant problems when applied at scale.

In the book Nudge (Halpern, 2015) notes that ‘Perfect models’ can be at odds with ‘messy reality’. Removing risk from the scheme makes it difficult for enterprises to pass. By not including the difficult ‘messy reality’ of how large organisations run operational IT we are left with a simplistic ‘perfect scheme’ that may work in theory but can’t work for large enterprises.

12 References

- (isc)2, 2023. *CISSP – The World's Premier Cybersecurity Certification*. [Online]
Available at: <https://www.isc2.org/Certifications/CISSP>
[Accessed 27 Feb 2023].
- AccountingTools, 2023. *Stop-or-go sampling definition*. [Online]
Available at: <https://www.accountingtools.com/articles/stop-or-go-sampling>
[Accessed 22 Mar 2023].
- ACSC, 2022. *Australian organisations should urgently adopt an*. [Online]
Available at: <https://www.cyber.gov.au/sites/default/files/2022-02/2022-02%20Australian%20organisations%20encouraged%20to%20urgentlyadopt%20an%20enhanced%20cyber%20security%20posture.pdf>
[Accessed 13 Mar 2023].
- ACSC, 2022. *Essential Eight Assessment Process Guide*. [Online]
Available at: <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-assessment-process-guide>
[Accessed 18 Mar 2023].
- ACSC, 2023. *Essential Eight*. [Online]
Available at: <https://www.cyber.gov.au/acsc/view-all-content/essential-eight>
[Accessed 09 Mar 2023].
- Almeida, R., Lourinho, R., Silva, M. M. d. & Pereira, R., 2018. A Model for Assessing COBIT 5 and ISO 27001 Simultaneously. *2018 IEEE 20th Conference on Business Informatics (CBI)*, 11-14 July.
- Barlette, Y. & Fomin, V. V., 2008. Exploring the Suitability of IS Security Management Standards for SMEs. *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*, pp. 308-308.
- Cabinet Office, 2016. *Procurement Policy Note 09/14: Cyber Essentials scheme certification*. [Online]
Available at: <https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification>
[Accessed 19 Mar 2023].
- Cannon, D. L., 2016. *CISA Certified Information Systems Auditor Study Guide*. 4th ed. Indianapolis: Wiley.
- Chief Information Officer for Health and Social Care, NHS England, 2018. *Lessons learned review of the WannaCry Ransomware Cyber Attack*. [Online]
Available at: <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf>
[Accessed 22 Mar 2023].
- CISA.gov, 2021. *Alert (AA21-291A) BlackMatter Ransomware*. [Online]
Available at: <https://www.cisa.gov/uscert/ncas/alerts/aa21-291a>
[Accessed 08 01 2023].
- Citrix, 2022. *Citrix named a Leader and Fast Mover in ZTNA market*. [Online]
Available at: <https://www.citrix.com/blogs/2022/06/07/citrix-named-a-leader-and-fast-mover-in>

[ztna-market/](#)

[Accessed 07 Mar 2023].

Citrix, 2022. *Reference Architecture - Protect apps and data on bring-your-own devices*. [Online]
Available at: <https://docs.citrix.com/en-us/tech-zone/design/reference-architectures/protect-apps-and-data-on-byo-devices.html>

[Accessed 07 Mar 2023].

ComputerWeekly, 2021. *Parliamentary devices left in taxis, buses, trains and pubs*. [Online]
Available at: <https://www.computerweekly.com/news/252502749/Parliamentary-devices-left-in-taxis-buses-trains-and-pubs>

[Accessed 22 Mar 2023].

CREST, 2014. *A Guide to the Cyber Essentials Scheme*. [Online]

[Accessed 30 09 2022].

Department for Business, Energy & Industrial Strategy, 2022. *National statistics: Business population estimates for the UK and regions 2022: statistical release*. [Online]

Available at: <https://www.gov.uk/government/statistics/business-population-estimates-2022/business-population-estimates-for-the-uk-and-regions-2022-statistical-release-html>

[Accessed 06 Mar 2023].

Dhillon, G. & Backhouse, J., 2001. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, 11(2), pp. 127-153.

Digital Origin, 2022. *Improving defences against Cyber Attacks & Intrusion*. [Online]

Available at: <https://www.digital-origin.co.uk/wp-content/uploads/2022/04/Improving-Defences-Against-Cyber-Attacks-Intrusion-v1.pdf>

[Accessed 28 Feb 2023].

digitalhealth, 2018. *NHS trusts fail post-WannaCry cyber security checks*. [Online]

Available at: <https://www.digitalhealth.net/2018/02/nhs-trusts-fail-post-wannacry-cybersecurity/>

[Accessed 28 09 2022].

Duo, n.d. *ATTACKERS COMBINE ATTACKS AGAINST RDP WITH RANSOMWARE*. [Online]

Available at: <https://duo.com/decipher/attackers-combine-attacks-against-rdp-with-ransomware>

[Accessed 20 Mar 2023].

ESFA, 2021. *Cyber security essentials*. [Online]

Available at: <https://esfahelp.education.gov.uk/hc/en-gb/articles/360016887559-Cyber-security-essentials>

[Accessed 18 Mar 2023].

European Union, 2003. *Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises*. [Online]

Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361>

[Accessed 06 Mar 2023].

Gartner, 2021. *Gartner Forecasts Global Devices Installed Base to Reach 6.2 Billion Units in 2021*. [Online]

Available at: <https://www.gartner.com/en/newsroom/press-releases/2021-04-01-gartner-forecasts-global-devices-installed-base-to-reach-6-2-billion-units-in-2021>

[Accessed 28 Feb 2023].

Gov.UK Central Digital and Data Office, 2023. *Publishing accessible documents*. [Online]
Available at: <https://www.gov.uk/guidance/publishing-accessible-documents>
[Accessed 14 Mar 2023].

GOV.UK, 2018. *Cyber Essentials Scheme: overview*. [Online]
Available at: <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview>
[Accessed 30 08 2022].

Halpern, D., 2015. *Inside the Nudge Unit: How small changes can make a big difference*. s.l.:Penguin.

HM Government, 2014. *Cyber Essentials Scheme - Requirements for basic technical protection from cyber attacks*. [Online]
Available at:
<https://web.archive.org/web/20160405003549/https://www.cyberstreetwise.com/cyberessentials/files/requirements.pdf>
[Accessed 02 Mar 2023].

HM Government, 2015. *Cyber Essentials Scheme Assurance Framework*. [Online]
Available at:
<https://web.archive.org/web/20150420055643/https://www.cyberstreetwise.com/cyberessentials/files/assurance-framework.pdf>
[Accessed 02 Mar 2023].

IASME, 2020. *PROTECTING ORGANISATIONS AGAINST CYBER ATTACK IASME is the National Cyber Security Centre's Cyber Essentials Partner*. [Online]
Available at: <https://iasme.co.uk/cyber-blog/cyber-essentials-and-the-launch-of-a-new-partnership-between-iasme-and-the-national-cyber-security-centre-a-part-of-gchq/>
[Accessed 20 Jan 2023].

IASME, 2021. *CHANGES TO CYBER ESSENTIALS REQUIREMENTS – APRIL 2021 UPDATE*. [Online]
Available at: <https://iasme.co.uk/cyber-blog/changes-to-cyber-essentials-requirements-april-2021-update/>
[Accessed 14 Mar 2023].

IASME, 2022. *Cyber Essentials Question Set - Evendine - July 2022*. [Online]
Available at: <https://iasme.co.uk/wp-content/uploads/2021/11/Question-Set-Cyber-Essentials-only-vEvendine.xlsx>
[Accessed 20 Jan 2023].

IASME, 2022. *Cyber Essentials Self-Assessment Preparation Booklet*. [Online]
Available at: https://iasme.co.uk/wp-content/uploads/2021/11/Cyber-Essentials-only-question-booklet_vEvendine.pdf
[Accessed 20 Jan 2023].

IASME, 2023. *Cyber Blog*. [Online]
Available at: <https://iasme.co.uk/category/cyber-essentials/>
[Accessed 18 Mar 2023].

IASME, 2023. *What are the changes to Cyber Essentials this year?*. [Online]
Available at: <https://iasme.co.uk/articles/what-are-the-changes-to-cyber-essentials-this-year/>
[Accessed 20 Feb 2023].

IASME, n.d. *BECOME AN ASSESSOR*. [Online]

Available at: <https://iasme.co.uk/become-an-assessor/>
[Accessed 27 Feb 2023].

IASME, n.d. *Cyber Essentials Plus Find Out More*. [Online]

Available at: <https://iasme.co.uk/cyber-essentials/cyber-essentials-plus-find-out-more/>
[Accessed 30 08 2022].

IASME, n.d. *Get ready for CYBER ESSENTIALS*. [Online]

Available at: <https://getreadyforcyberessentials.iasme.co.uk/>
[Accessed 28 09 2022].

IASME, n.d. *THE BENEFITS OF CERTIFICATION*. [Online]

Available at: <https://iasme.co.uk/cyber-essentials/>
[Accessed 18 Mar 2023].

IASME, n.d. *VULNERABILITY ASSESSMENT PLUS EXAM*. [Online]

Available at: <https://iasme.co.uk/vulnerability-assessment-plus-exam/>
[Accessed 27 Feb 2023].

ico., n.d. *The role of the National Cyber Security Centre (NCSC)*. [Online]

Available at: <https://ico.org.uk/for-organisations/the-guide-to-nis/the-role-of-the-national-cyber-security-centre-ncsc/>
[Accessed 20 Mar 2023].

Indelible Data, 2017. *Cyber Essentials - Requirements for IT Infrastructure Questionnaire v1*. [Online]

Available at:
https://web.archive.org/web/20181126040141if_/http://www.indelibledata.co.uk:80/images/Cyber-Essentials-Questionnaire-v1-050.docx
[Accessed 07 Mar 2023].

Indelible Data, 2021. *Cyber Essentials Plus checklist for remote testing*. [Online]

Available at: <https://www.indelibledata.co.uk/cyber-essentials/cyber-essentials-plus-checklist-remote/>
[Accessed 28 Feb 2023].

IndelibleData Ltd, 2022. *Cyber Essentials Evendine – what you need to know..* [Online]

Available at: <https://www.indelibledata.co.uk/cyber-essentials/the-cyber-essentials-evendine-update-what-you-need-to-know/>
[Accessed 09 Mar 2023].

ISACA, 2023. *Boost your career with an ISACA Certification—while you gain recognition and credibility*. [Online]

Available at: <https://www.isaca.org/credentialing/certifications>
[Accessed 27 Feb 2023].

ISO, 2022. *ISO/IEC 27001:2013*. [Online]

Available at: <https://www.iso.org/standard/54534.html>
[Accessed 27 Feb 2023].

IT Governance, 2022. *Cyber Essentials FAQs*. [Online]

Available at: <https://www.itgovernance.co.uk/cyber-essentials-faqs>
[Accessed 28 Feb 2023].

James, D., 2017. *twitter*. [Online]

Available at: <https://twitter.com/djammmer/status/913909403664883712>
[Accessed 20 Feb 2023].

James, D., 2017. *twitter*. [Online]

Available at: <https://twitter.com/djammmer/status/913910343373426688?s=20&t=9-rRHmMED4eTjUM3qsym5w>
[Accessed 20 Feb 2023].

Jisc, 2022. *Cyber security posture survey results 2022 - Higher Education*. [Online]

Available at: <https://repository.jisc.ac.uk/8955/1/cyber-security-posture-survey-2022-he-full-report.pdf>
[Accessed 26 Jan 2023].

Kipchuk, F., Sokolov, V., Skladannyi, P. & Ageyev, D., 2021. Assessing Approaches of IT Infrastructure Audit. *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*, 05-07 10.

Martin G, G. S. K. J. H. C. D. A., 2018. WannaCry—a year on. *BMJ*, 04 June.

Microsoft, 2013. *Microsoft Security Intelligence Report*. [Online]

Available at: <https://go.microsoft.com/fwlink/p/?linkid=2036139>
[Accessed 02 Mar 2023].

Microsoft, 2014. *Microsoft Security Intelligence Report Volume 17*. [Online]

Available at: <https://go.microsoft.com/fwlink/p/?linkid=2036137>
[Accessed 02 Mar 2023].

Microsoft, 2014. *What Are Domains and Forests?*. [Online]

Available at: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073\(v=ws.10\)#forests-as-security-boundaries](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)#forests-as-security-boundaries)
[Accessed 08 01 2023].

Microsoft, 2018. *Administering Microsoft System Center Configuration Manager and Cloud Services Integration*. [Online]

Available at: <https://web.archive.org/web/20190419215630/https://www.microsoft.com/en-us/learning/exam-70-703.aspx>
[Accessed 20 Feb 2023].

Microsoft, 2021. *Achieving world-class Windows monthly patching efficiency*. [Online]

Available at: <https://techcommunity.microsoft.com/t5/windows-it-pro-blog/achieving-world-class-windows-monthly-patching-efficiency/ba-p/2572945>
[Accessed 06 Mar 2023].

Microsoft, 2021. *Creating an Organizational Unit Design*. [Online]

Available at: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/creating-an-organizational-unit-design>
[Accessed 13 Mar 2023].

Microsoft, 2021. *KB5005408—Smart card authentication might cause print and scan failures*. [Online]

Available at: <https://support.microsoft.com/en-us/topic/kb5005408-smart-card-authentication->

[might-cause-print-and-scan-failures-514f0bc5-ecde-4e5e-8c5a-2a776d7fb89a](https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/microsoft-recognized-by-the-idc-marketscape-as-a-leader-in/ba-p/2464411)

[Accessed 03 Mar 2023].

Microsoft, 2021. *Microsoft recognized by the IDC MarketScape as a Leader in Worldwide Advanced Authentication for AAD*. [Online]

Available at: <https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/microsoft-recognized-by-the-idc-marketscape-as-a-leader-in/ba-p/2464411>

[Accessed 14 Mar 2023].

Microsoft, 2022. *Create configuration baselines in Configuration Manager*. [Online]

Available at: <https://learn.microsoft.com/en-us/mem/configmgr/compliance/deploy-use/create-configuration-baselines>

[Accessed 13 Mar 2023].

Microsoft, 2022. *Gathering Information about Your Active Directory Deployment*. [Online]

Available at: <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/gathering-information-about-your-active-directory-deployment>

[Accessed 08 01 2023].

Microsoft, 2022. *Overview: VPN split tunneling for Microsoft 365*. [Online]

Available at: <https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-vpn-split-tunnel?view=o365-worldwide>

[Accessed 09 Mar 2023].

Microsoft, 2022. *Sign in failures and other issues related to Kerberos authentication*. [Online]

Available at: <https://learn.microsoft.com/en-us/windows/release-health/resolved-issues-windows-10-22h2?source=recommendations#2953msgdesc>

[Accessed 06 Mar 2023].

Microsoft, 2022. *Support for Active Directory domains in Configuration Manager*. [Online]

Available at: <https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/configs/support-for-active-directory-domains>

[Accessed 17 Feb 2023].

Microsoft, 2023. *Embrace proactive security with Zero Trust*. [Online]

Available at: <https://www.microsoft.com/en-us/security/business/zero-trust>

[Accessed 22 Mar 2023].

Microsoft, 2023. *Manage emergency access accounts in Azure AD*. [Online]

Available at: <https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access>

[Accessed 07 Mar 2023].

Microsoft, 2023. *The Microsoft Intune Suite fuels cyber safety and IT efficiency*. [Online]

Available at: <https://techcommunity.microsoft.com/t5/microsoft-intune-blog/enable-windows-standard-users-with-endpoint-privilege-management/ba-p/3755710>

[Accessed 07 Mar 2023].

Microsoft, 2023. *What is Windows LAPS?*. [Online]

Available at: <https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview>

[Accessed 17 Mar 2023].

Microsoft, n.d. *Security Update Guide FAQs*. [Online]

Available at: <https://www.microsoft.com/en-us/msrc/faqs-security-update-guide>
[Accessed 06 Mar 2023].

Ministry of Defence, 2021. *Cyber Security Model: Supplier Assurance Questionnaire (SAQ) Question Set Guide*. [Online]

Available at: <https://www.gov.uk/government/publications/supplier-cyber-protection-service-supplier-assurance-questionnaire-workflow/cyber-security-model-supplier-assurance-questionnaire-saq-question-set-guide>
[Accessed 24 Feb 2023].

MITRE, 2022. *Enterprise Mitigations*. [Online]

Available at: <https://attack.mitre.org/mitigations/enterprise/>
[Accessed 26 09 2022].

MITRE, n.d. *CWE/CAPEC Board*. [Online]

Available at: <https://cwe.mitre.org/about/board.html>
[Accessed 30 09 2022].

National Audit Office, 2001. *A Practictal Guide to Sampling*. [Online]

Available at: <https://www.nao.org.uk/wp-content/uploads/2001/06/SamplingGuide.pdf>
[Accessed 13 Mar 2023].

NCA, 2013. *ALERT - Mass ransomware spamming event targeting UK computer users*. [Online]

Available at:
<https://web.archive.org/web/20131211183431/https://nationalcrimeagency.gov.uk/news/256-alert-mass-spamming-event-targeting-uk-computer-users>
[Accessed 17 Mar 2023].

NCSC, 2017. *A brief history of Cyber Essentials*. [Online]

Available at:
<https://web.archive.org/web/20180913181012/https://www.cyberessentials.ncsc.gov.uk/2017/11/27/The-NCSC-and-Cyber-Essentials.html>
[Accessed 30 08 2022].

NCSC, 2019. *The problems with patching*. [Online]

Available at: <https://www.ncsc.gov.uk/blog-post/the-problems-with-patching>
[Accessed 09 Mar 2023].

NCSC, 2020. *Cyber Essentials Plus: Illustrative Test Specification v2.2*. [Online]

Available at: <https://www.ncsc.gov.uk/files/Cyber-Essentials-Plus-Illustrative-technical-specification-2-2.pdf>
[Accessed 20 Jan 2023].

NCSC, 2021. *Asset management: Implementing asset management for good cyber security..* [Online]

Available at: <https://www.ncsc.gov.uk/guidance/asset-management>
[Accessed 20 Jan 2023].

NCSC, 2021. *Cyber Essentials: It isn't a risky business....* [Online]

Available at: <https://www.ncsc.gov.uk/blog-post/cyber-essentials-it-isnt-a-risky-business>
[Accessed 30 08 2022].

- NCSC, 2021. *Device Security Guidance*. [Online]
Available at: <https://www.ncsc.gov.uk/collection/device-security-guidance/platform-guides/windows>
[Accessed 07 Mar 2023].
- NCSC, 2022. *Cyber Essentials Plus: Illustrative Test Specification*. [Online]
Available at: <https://www.ncsc.gov.uk/files/Cyber-Essentials-Plus-Illustrative-Technical-Specification-v3-0-January-2022-.pdf>
[Accessed 20 Jan 2023].
- NCSC, 2022. *Cyber Essentials: Requirements for IT infrastructure*. [Online]
Available at: <https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf>
[Accessed 28 09 2022].
- NCSC, 2022. *Device-Security-Guidance-Configuration-Packs/Microsoft/Windows/*. [Online]
Available at: <https://github.com/ukncsc/Device-Security-Guidance-Configuration-Packs/tree/main/Microsoft/Windows>
[Accessed 07 Mar 2023].
- NCSC, 2023. *Cyber Essentials*. [Online]
Available at: <https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=Cyber%20Essentials&sort=date%2Bdesc>
[Accessed 18 Mar 2023].
- NCSC, 2023. *Frequently asked questions*. [Online]
Available at: <https://www.ncsc.gov.uk/cyberessentials/faqs>
[Accessed 06 Mar 2023].
- NCSC, n.d. *About Cyber Essentials*. [Online]
Available at: <https://www.ncsc.gov.uk/cyberessentials/overview>
[Accessed 30 08 2022].
- NCSC, n.d. *Products & Services Cyber Essentials*. [Online]
Available at: <https://www.ncsc.gov.uk/section/products-services/cyber-essentials>
[Accessed 28 09 2022].
- netgear, n.d. *GS308E — 8-Port Gigabit Ethernet Plus Switch*. [Online]
Available at: <https://www.netgear.com/support/product/gs308e.aspx>
[Accessed 31 Jan 2023].
- Network Assured, 2023. *PCI Qualified Security Assessors: A Buyer's Guide*. [Online]
Available at: <https://networkassured.com/compliance/pci-qualified-security-assessor-qa/>
[Accessed 02 Mar 2023].
- Niemimaa, E. N. & M., 2017. Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, 26(1), pp. 1-20.
- NIST, 2021. *Getting Started with the NIST Cybersecurity Framework*. [Online]
Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf>
[Accessed 03 Mar 2023].

OffSec, 2021. *OSCP Exam Change*. [Online]

Available at: <https://www.offsec.com/offsec/oscp-exam-structure/>
[Accessed 08 Mar 2023].

packetstormsecurity, 2021. *SAPSetup Automatic Workstation Update Service 750 Unquoted Service Path*. [Online]

Available at: <https://packetstormsecurity.com/files/161894/SAPSetup-Automatic-Workstation-Update-Service-750-Unquoted-Service-Path.html>
[Accessed 09 Mar 2023].

PCI Council, 2021. *Updated PCI DSS v4.0 Timeline*. [Online]

Available at: <https://blog.pcisecuritystandards.org/updated-pci-dss-v4.0-timeline>
[Accessed 16 Mar 2023].

PCI Council, 2023. *Request for Comments*. [Online]

Available at: https://www.pcisecuritystandards.org/get_involved/request_for_comments/
[Accessed 14 Mar 2023].

PCI Security Standards Council, 2018. *PCI DSS Quick Reference Guide*. [Online]

Available at: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
[Accessed 07 Mar 2023].

PCI Security Standards Council, 2023. *Document Library*. [Online]

Available at: https://www.pcisecuritystandards.org/document_library/
[Accessed 27 Feb 2023].

PCI Security Standards Council, n.d. *About Us*. [Online]

Available at: https://www.pcisecuritystandards.org/about_us/
[Accessed 05 Mar 2023].

pdfforge.org, 2012. *Please drop bundled installer, it is installing stuff considered malware*. [Online]

Available at: <https://forums.pdfforge.org/t/please-drop-bundled-installer-it-is-installing-stuff-considered-malware-e-g-babylon-toolbar/3722/41?page=3>
[Accessed 14 Mar 2023].

QA, 2023. *Basic Administration of Microsoft Endpoint Configuration Manager*. [Online]

Available at: <https://www.qa.com/course-catalogue/courses/basic-administration-of-microsoft-endpoint-configuration-manager-qamssccm/>
[Accessed 20 Feb 2023].

QA, 2023. *Mastering Modern Desktop and Mobile Device Administration with Microsoft EndPoint Manager*. [Online]

Available at: <https://www.qa.com/course-catalogue/courses/mastering-modern-desktop-and-mobile-device-administration-with-microsoft-endpoint-manager-intune-qamsmem>
[Accessed 20 Feb 2023].

Qomplx, 2021. *Active Directory is Your #1 Cyber Risk. Start Treating It That Way..* [Online]

Available at: <https://www.qomplx.com/blog/active-directory-is-your-top-cyber-risk-start-treating-it-that-way/>
[Accessed 14 Mar 2023].

Quizlet, 2021. *VA+ flashcards*. [Online]

Available at: <https://quizlet.com/565199176/va-flash-cards/>

[Accessed 28 Feb 2023].

Rae, A. & Patel, A., 2019. Defining a New Composite Cybersecurity Rating Scheme for SMEs in the U.K.. *ISPEC 2019: Information Security Practice and Experience*, pp. 362-380.

redmondmag.com, 2021. *Microsoft Increasing Intune and EMS 'Standalone' Prices in July*. [Online]

Available at: <https://redmondmag.com/articles/2021/02/22/intune-ems-price-hike.aspx>

[Accessed 24 Jan 2023].

Scottish Government, 2023. *Public Sector Cyber Resilience Assurance Survey 2023*. Scotland: Cyber Resilience Unit.

SecurityIntelligence, 2021. *LockBit 2.0: Ransomware Attacks Surge After Successful Affiliate Recruitment*. [Online]

Available at: <https://securityintelligence.com/posts/lockbit-ransomware-attacks-surge-affiliate-recruitment/>

[Accessed 08 01 2023].

SEPA, 2020. *How we work*. [Online]

Available at: <https://www.sepa.org.uk/about-us/how-we-work/>

[Accessed 20 09 2022].

SEPA, 2021. *SEPA Internal Audit Report 2020/21 Cyber Attack – Lessons Learned*. [Online]

Available at: <https://www.sepa.org.uk/media/593779/azets-cyber-attack-lessons-learned.pdf>

[Accessed 30 08 2022].

Silva, L., Hsu, C., Backhouse, J. & McDonnell, A., 2016. Resistance and power in a security certification scheme: The case of c:cure. *Decision Support Systems*, Volume 92, pp. 68-78.

Siponen, M. & Willison, R., 2009. Information security management standards: Problems and solutions. *Information & Management*, 46(5), pp. 267-270.

Such, J. M. et al., 2019. Basic Cyber Hygiene: Does It Work?. *Computer*, 52(4), pp. 21-31.

Tenable, 2021. *A Global Threat to Enterprises: the Impact of AD Attacks*. [Online]

Available at: <https://www.tenable.com/whitepapers/a-global-threat-to-enterprises-the-impact-of-ad-attacks>

[Accessed 08 01 2023].

Thaler, R. H. & Sunstein, C. R., 2012. *Nudge*. The Final Edition ed. s.l.:Penguin.

The Behavioural Insights Team, 2015. *EAST - Four simple ways to apply behavioural insights*. [Online]

Available at: https://www.bi.team/wp-content/uploads/2015/07/BIT-Publication-EAST_FA_WEB.pdf

[Accessed 28 Feb 2023].

The Institute of Internal Auditors Australia, 2023. *Internal Audit Sampling*. [Online]

Available at: https://www.iaa.org.au/sf_docs/default-source/technical-resources/2018-whitepapers/iaa-whitepaper_internal-audit-sampling.pdf?sfvrsn=2

[Accessed 13 Mar 2023].

UCISA, 2023. *UCISA Home Page*. [Online]

Available at: <https://www.ucisa.ac.uk/>

[Accessed 24 Feb 2023].

UK Government, 2014. *New scheme to help businesses defend against cyber threats goes live*.

[Online]

Available at: <https://www.gov.uk/government/news/new-scheme-to-help-businesses-defend-against-cyber-threats-goes-live--2>

[Accessed 02 Mar 2023].

Vania, K. & Rashidi, Y., 2016. *Tales of Software Updates: The process of updating software*. San Jose, CA, USA, s.n.

ZDnet, 2019. *Microsoft's killer Windows 7 patch: Breaks networking, flags legit PCs as 'Not genuine'*.

[Online]

Available at: <https://www.zdnet.com/article/microsofts-killer-windows-7-patch-breaks-networking-bricks-legit-not-genuine-pcs/>

[Accessed 06 Mar 2023].

13 Appendix 1 – Questionnaire

13.1 Recruitment message

I am a postgraduate student at the University of Strathclyde studying Cyber Security. I also manage the IT Services Cyber Security team at Strathclyde and am responsible for our annual recertification of Cyber Essentials. For my research project I'm looking at the effectiveness of the UK Cyber Essentials scheme and in particular it's suitability for large organisations.

I'm looking for participants who work at larger organisations who would be willing to complete a short single page questionnaire on their experiences with the scheme. The responses will be anonymised and any organisational specific comments will be removed. Participation in the study is voluntary and the information provided will be used for academic purposes. My supervisor is Dr Daniel Thomas of the Computer and Information Sciences department at the University of Strathclyde. The departmental ethics committee can be contacted at ethics@cis.strath.ac.uk

13.2 Questionnaire consent page

Mind the security gap: Evaluating the effectiveness of the UK Cyber Essentials scheme and its suitability for large enterprises

This questionnaire is part of a research study undertaken as part of the MSc in Cyber Security at the University of Strathclyde.

The researcher is Andrew Cooper (andrew.cooper@strath.ac.uk)

The supervisor is Dr Daniel Thomas (d.thomas@strath.ac.uk)

Research topic

For my research project I'm looking at the effectiveness of the UK Cyber Essentials scheme and in particular it's suitability for large organisations. This questionnaire is designed to gather information about the experience of the scheme when applied to larger organisations.

Eligibility

Participants should:

- Work at an organisation that either has achieved Cyber Essentials or is aiming to achieve Cyber Essentials
- Be responsible in that organisation for some or all of the attainment of

Cyber Essentials

Confidentiality

The responses will be anonymised and any organisational specific comments will be removed.

Consent

You are under no obligation to complete this questionnaire or to answer any particular question. The data collected will be used in a postgraduate dissertation. You have the right to withdraw your answers at any time until the dissertation is submitted in March 2023.

Further questions

If you have questions about this study that are not answered here please contact the researcher Andrew Cooper (andrew.cooper@strath.ac.uk)

The University of Strathclyde Department of Computer and Information Sciences ethics committee can be contacted at ethics@cis.strath.ac.uk

Please click below if you consent to continue with this survey

Yes, I give consent to continue with this survey

[13.3 Main questionnaire page](#)

What size is your organisation?

- less than 250 users
- 250 to 1500 users
- 1501 to 5000 users
- Over 5000 users

Does your organisation currently hold Cyber Essentials (CE) or Cyber Essentials Plus (CE+)? If it does, can you briefly describe the scope and any reasons why you have chosen a whole organisation scope or a sub-scope?

If your organisation holds CE or CE+, what operating systems are running on the endpoints that are within your scope? Please keep this high level without the version information. For example, 80% Windows, 20% MacOS. Do these devices connect to a Microsoft Active Directory domain?

How do you feel Cyber Essentials helps (or would help) improve the security of your organisation and what challenges has your organisation faced in the certification process? Is it a requirement for your organisation to do business?

If you hold (or are aiming for) CE+ do you have any comments on the audit process? Do you feel it gives an appropriate level of assurance that the CE controls are in place?

How do you ensure the endpoints in your organisation comply with the 14-day requirement for critical or high-risk patches? Does your organisation use a management tool such as Microsoft Configuration Manager (SCCM) or PDQ Deploy to manage your devices?

Thinking about the changes (or clarifications) to the scheme over the years. How do you feel they have been communicated since you first started looking at CE?

Do you have any further comments about the Cyber Essentials scheme not addressed above?

As a participant in this research you have the right to withdraw from the study. If you feel like you may wish to withdraw your responses in future please enter your email address below. The email address will only be used for the explicit purpose to identify your submission if you wish to end your participation in this study. You will not be able to withdraw your responses once the research project is complete.

Click below to submit your answers

14 Appendix 2 – File Types to block or warn about on inbound email

This is the list of file types that were published by Crest when they were one of the NCSC Delivery Partners. This list does not appear to be public now that IASME are the sole Delivery Partner.

Executables	Exploit targeting extensions	Containers
.com	.pdf	.zip
.bat	.doc	.7z
.exe	.docx	.rar
.pif	.ppt	.tar.gz
.scr	.pptx	.tar
.msi	.xls	.gz
.ps1	.xlsx	
.jar	.png	
.sh	.jpg	
.py	.mp4	
.dmg	.avi	
	.mov	

Figure 22 List of file types

15 Appendix 3 – Device management tools from the survey results

The following tools were listed as answers in the survey.

Tool	Comment	Webpage	License
SCCM	System Center Configuration Manager. Also known as Microsoft Endpoint Configuration Manager (MECM)	https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager	Typically licensed as part of an Enterprise agreement with Microsoft
PDQ		https://www.pdq.com/	Licensed per administrator
Fog		https://fogproject.org/	“Open source network cloning and management solution”
WSUS	Windows Server Update Services. Microsoft on-prem patch management solution	https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus	Licensed as part of Windows Server
Jamf	An Apple focused management solution that can integrate with Microsoft SCCM and Intune	https://www.jamf.com/	Licensing per device or per user

Intune	A Microsoft cloud based Mobile Device Management / Mobile Application Management solution. This is part of the Microsoft Endpoint Manager suite of tools and is cloud based	https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/microsoft-intune	This is licensed via the mid-tier Microsoft Cloud Enterprise Agreements with further add-ons available
Dell Command Center	Not a management tool in the traditional sense, but an add-on piece of software for Dell computers that updates drivers and firmware. The survey response that listed this software wasn't too clear on how it was used – Dell offer a wide variety of tools to assist with large scale management of devices	https://www.dell.com/support/kbdoc/en-uk/000126750/dell-client-command-suite	License permits use on Dell computers
NVT	This was listed in one survey response but it is not clear what this is. It could be a Network Vulnerability Tool or Network Visualisation tool, the Dell Network Validation Tool, or the NVT group who are an MSP	https://csrc.nist.gov/csrc/media/publications/conference-paper/1999/10/21/proceedings-of-the-22nd-nissc-1999/documents/papers/p7.pdf https://www.dell.com/support/kbdoc/en-uk/000019313/deployment-kb-dell-technologies-network-validation-tool-nvt https://www.nvtgroup.co.uk/managed-services/systems-monitoring/	

Figure 23 Management tools in use

16 Appendix 4 – More on Sampling

16.1 Clarifications on what is meant by a representative sample

There is an interesting line in the v3.0 specification What's New section – “Removed the 90% sample set rule in relation to devices tested.” This does highlight a major change in sampling from the previous version. In version 2.2 (NCSC, 2020) this read:

“We recommend that you aim to satisfy yourself that, in total, your testing is representative of at least 90% of all the devices in scope.”

In version 3.0 this now reads:

“We recommend that you aim to satisfy yourself that, in total, your testing is representative of all the devices in scope.”

This demonstrates the desire to validate the controls on every device in scope, not just a proportion. For small to medium enterprises this is entirely feasible to validate with good confidence by choosing a manageable sample set. It is unfeasible to do this in a larger enterprise with thousands, tens of thousands or hundreds of thousands of devices. This reinforces the need for a different approach as suggested in the paper.

16.2 Non-sampled compliance

In the main paper there is discussion of using automation to audit all devices in scope.

Assuming the SCCM usage seen in the survey is replicated across other enterprises this could be provided as an SCCM compatible compliance baseline download which could not only report on but enforce the CE controls on devices (Microsoft, 2022) – in effect a continuous audit and remediation process. Even without SCCM there are methods that could be used to automate much of the assessment. Whilst this may seem like deviating from simple changes to the scheme this type of assessment could easily be carried out by an Internal Assessor if that recommendation was adopted.

17 Appendix 5 – Security Update Management Issues in the Real World

Without real world examples the discussion in the main body of the paper may make it seem like patching problems are theoretical. At scale they can have major business impact.

On 8th November 2022 Microsoft released a patch that broke Kerberos authentication for some organisations causing user sign ins to fail (Microsoft, 2022). An out-of-band fix was released 10 days later. Large organisations had to make a risk-based decision on this patch and by the time of the fix had only 4 days to deploy it to be compliant with CE.

Other recent issues with patches have seen printing break (Microsoft, 2021), networking fail and the operating system licensing being marked as “not genuine” (ZDnet, 2019).

18 Appendix 6 – Evolution of low skill threats since 2014

A key concept in Cyber Essentials is that it is primarily intended to address low level commodity internet attacks.

The early CE documentation reinforces the recent messaging that the scheme is designed to mitigate or prevent common internet attacks. In the January 2015 assurance framework documentation organisations are asked to identify systems that “are at risk from Internet based threat actors with low levels of technical capability” (HM Government, 2015). For the CE+ portion this phrasing about low levels of technical capability is repeated.

The first requirements document (HM Government, 2014) lists the same controls as in the current version of the scheme. It does however list two example “Low level cyber threats”:

“#1 Involves malware infection that requires user action such as opening an infected email attachment or clicking on a malicious website link”

“#2 Involves the use of automated tools that exploit known vulnerabilities in Internet connected servers and network devices”

These sound reasonable even 9 years on, however the types of tools and vulnerabilities and the types of malware have changed dramatically. A key question is whether the scheme has kept up with what a “low level” cyber-attack carried out by a “threat actor with low levels of technical capability” would be, because the top threats seen in 2023 are very different from those when this scheme was designed. The key differential here is the impact of ransomware.

The word “ransomware” is not found in the Microsoft Security Intelligence Report for 2H2013 (Microsoft, 2013). In the first half of 2014 Trojans were the most common category of malware with “Ransomware and Other Malware categories all remain[ing] stable at around 0 to 1 percent each quarter” (Microsoft, 2014). At this point ransomware didn’t always encrypt data – it could display fake messaging suggesting that a government agency had caught the user doing something illegal and that they had to pay a fine.

Compare this to wannacry only four years later. In NHS England 80 of 236 Hospital Trusts were affected by this ransomware – not just individual machines (Chief Information Officer for Health and Social Care, NHS England, 2018). Although this malware spread via unpatched machines it highlighted the danger posed by internal lateral movement. Additionally, as seen in the main body of the paper, CE requires strict adherence to the controls for them to be effective and based on the research this is not adequately tested by assessors. Furthermore, modern malware, as described in the main paper, can spread without requiring unpatched devices. Instead it can spread using stolen credentials from the initially attacked machine.

19 Appendix 7 – How to pass without implementing the controls

A number of the survey results said that it was too easy to cheat:

“[the] system can be gamed”

“too lightweight and manipulable”

“[the scope was narrowed so far that it] felt almost fraudulent.”

“I know of one organisation who showed assessor data from 4 desktops and passed”

“many CE requirements are not verified by the audit process”

“Minimal assurance”

“We just passed CE/CE+ [and] we feel that the implemented controls/patching were not assessed appropriately”

This is a major concern. As was seen in the main body of the paper large organisations are using CE/CE+ as a measure of assurance. If it can be easily passed by cheating the assessment process it could mean government or military data is being shared with companies that do not even meet the basic requirements.

The main body of the paper has examined the areas that have assurance or scaling issues in depth but a worked example may help reinforce why this is such a large issue. Note that this will use the publicly available documentation and the comments from the survey responses and the Former Assessor – there may be additional private guidance for assessors which would alter this example.

19.1 Worked example part 1 – Cheating Cyber Essentials

Consider a 250 user Sales department that is part of a larger 10,000 user organisation. They need Cyber Essentials Plus to win a contract. They decide to apply on their own without telling the rest of the organisation. In this example the department isn't deliberately attempting to mislead, but it should be easy to see where the system can be gamed.

Problem 1: When the documentation is complete it has to be signed by someone at “board level or equivalent.” Is this role checked or verified by the assessor? What is meant by an equivalent? It would appear that the Director for Sales could sign off on this without the form going to any other part of the organisation. This is a particular problem here because Sales are not responsible for the network.

The network is run by the IT department. It uses private addressing in the form 192.168.x.y with a subnet mask of 255.255.255.0. All subnets are on separate VLANs to delineate subnet boundaries but all are routable. There are no firewalls in place and all devices can talk to each other across subnet boundaries. Some examples are:

- 192.168.10.x – Sales
- 192.168.11.x – Finance
- 192.168.12.x – HR
- 192.168.13.x – Datacentre

Problem 2: Sales have said that they are on a separate VLAN which is true. It meets the letter of the specification. Yet this is not segregated from the rest of the organisation. This is an area where a different assessor may go back and ask what segregation is in place.

Faced with the possibility of failing the department goes back to the assessor and suggest that because they use DHCP reservations on their VLAN no other devices can be connected to the VLAN.

Problem 3: The assessor doesn't fully understand that this still doesn't provide segregation but decides to accept this as a sub-set boundary. There appears to be no further checks on this and when Cyber Essentials Plus is considered later, that doesn't check the boundary either.

The department are asked for a list of devices in their sub-set and a list of BYOD devices that their users use. They use a spreadsheet as an asset register so get their list of PCs from this, and they assume, but don't check, that all their devices are running the latest version of Windows because they've configured Windows Update. They take the spreadsheet and add the version of Windows, then send this to the assessor structured in the following way:

- SALESPC-1, Dell, Optiplex, Windows 10 22H2
- SALESPC-2, Dell, Optiplex, Windows 10 22H2

They say that they have no users who check work email on their phone which is not true. Those personal devices should be in scope but when pressed by the assessor they say that those systems are run by the IT department and are actually part of the IT departments scope. The assessor isn't totally convinced. They then backtrack and say they were mistaken and no-one in their sub-set uses personal devices.

They also list all the applications they *think* they use but because they have no management tool they can't be certain. They're pretty sure they're up to date because they sometimes ask staff to approve the updates when they get prompted.

Problem 4: There are no additional checks. The assessor might ask questions such as “are you sure this is correct” but if the applicant is insistent the assessor doesn’t appear to have any further recourse to check or validate those answers. There is no way of telling if the applications they use are listed, nor is there any way of telling if they are up to date.

The remaining questions are answered in a similar way. They find old documentation sent to them from a few years ago about their firewall setup from IT and supply that on the form. It seems correct and since the firewalls are still supported the assessor is happy.

They state that no-one has admin rights on their devices. They haven’t realised that one of their IT team has manually put all members of the senior departmental team into the Administrators group on each device because they complained it took too long to get software installed on their devices. Similar answers are given for anti-malware.

Problem 5: There is no additional verification of any of these answers

19.2 Worked example part 1 – Summary

This department would be awarded a Cyber Essentials certificate. The scope would be invalid and not a security boundary and there is no assurance that they are actually implementing any of the controls as defined in the standard. In this example the department is trying to do the right thing but are confused by the technologies. Worryingly any organisation should be able to pass by simply lying about some of the answers as there is no further verification.

This portion of the example should help reinforce the concerns from the survey. At present a Cyber Essentials certificate shouldn’t be used as an independent measure of assurance. Cyber Essentials Plus is not much better.

19.3 Worked example part 2 – Cheating Cyber Essentials Plus

After the Cyber Essentials certificate has been approved the team move on to Cyber Essentials Plus. This requires a hands-on assessment of devices in scope and an external scan of the organisations IP address range.

As was discussed in the paper the Firewall test provides a good level of assurance and won’t be explored further. However, it’s the sampling issues that will be explored.

This department has 250 devices. When the assessor carries out Test 2 – the authenticated vulnerability scan it would reveal that patching isn’t working. However, this assumes the assessor carries it out on all devices. In reality this would not be the case – it would be on a representative number of devices agreed with the applicant.

Problem 6: The sampling can be of devices that the applicant knows will pass, or that are not representative of the full estate

In our example the department has worked with the assessor and they are going to fail – the operating system hasn’t been patched for months and the version of Java installed is very old. They manually fix these issues but notice another – the controls aren’t in place. They have delegated access to their portion of the company Active Directory. Realising that mandating these controls won’t be popular in their department they decide to move these sample devices to a different Organisational Unit (OU) within the Active Directory. This is a different part of the Active Directory where different controls can be applied for as long as a device is in that area.

An example of how to do this can be seen in Figure 24. In this example all of the computers are normally found in the Computers OU with no security controls applied. The CyberEssentials OU has a Group Policy applied to set the controls. Group Policy is a technology built in to Active Directory to set controls on devices. When the assessor arrives the 5 sample machines are placed in this OU.



Figure 24 Cheating Cyber Essentials with Group Policy

An important concept about Active Directory Group Policy is that when it no longer applies – in this example when the machines are moved back into the main Computers OU – the settings are removed from the devices. In this example the security controls that were assessed are removed as soon as the devices have been moved by the department.

Problem 7: Since the assessment is a point-in-time audit the ‘representative devices’ can be placed in an area where the controls only apply on the day when the assessor visits, but are removed for the rest of the year

19.4 Worked example part 2 – Summary

Due to the lack of further checking this organisation will be issued a Cyber Essentials Plus certificate. Consider what the assessor has missed:

- they have no idea what operating system versions are running
- they have no idea what software is actually installed, or if it is up to date
- they have no idea what users are in the local Administrators group in Windows
- they have no idea if the antimalware software is running or if it is up to date
- requirements such as disabling auto-run have not been tested or checked
- the sample for CE+ is not reflective of the devices in use
- Active Directory has been used to create a machine that is guaranteed to pass and that can be reverted back to an insecure state within minutes of the assessor leaving
- the IT department has not been engaged during this process

Further to this, other parts of the organisation may have administrative control over all the devices within their scope with the ability to change security and firewall settings via Group Policies set at a higher level.

The only thing that can be guaranteed here is that the external firewall meets the requirements and the five devices supplied for sampling had up-to-date software and the controls applied at the time of the test. It may be argued that this is expected – Cyber Essentials Plus is a point-in-time assessment of the controls being applied correctly. But in this example the other 245 machines could be running anything, even SCO Unix or Windows 95, and without further checks this would not be discovered.

19.5 Summary

It should not be so easy to game the scheme. Perhaps there is additional guidance to assessors to stop the above from occurring, but this is not public, and unfortunately the example above is sadly not far-fetched. It highlights probably the biggest assurance problem in the scheme – the results of

the controls are tested but there is no verification of the process used to set them and no additional checks to ensure that samples are representative.

Without change it will still be exceptionally easy to cheat to get a CE+ certificate by selecting known good machines once a year then reverting back to bad practice. The tests can't validate that patching occurs within 14 days, just that patching occurs at least once every 365 days.

The recommendations from the main paper would resolve many of these issues if adopted.