Department for Science, Innovation & Technology

Process Evaluation of the Cyber Essentials Scheme

Final Report (v3)

Non-markdown version

25th April 2023

Pye Tait Consulting
info@pyetait.com
www.pyetait.com

Cert No: QEC19593371/0/Q

Contents

List of Figures

List of Tables

Acknowledgements

The Department for Science, Innovation and Technology (DSIT), along with Pye Tait Consulting, gratefully acknowledge the contributions of all organisations and individuals who helped to make this process evaluation possible. This includes representatives from IASME, NCSC, other government and industry stakeholders, former Accreditation Bodies, Certification Bodies, as well as current, lapsed and non-users of Cyber Essentials.

Executive Summary

Background

The modern digital age presents significant opportunities for organisations, as well as complexities and risks. The UK government, as part of its commitment to making the UK the safest place in the world to start and grow a digital business, has set out ambitious policies to protect the UK in cyberspace. These are set out in its National Cyber Strategy 2022.

The government-owned Cyber Essentials scheme aims to help organisations of all sizes defend themselves against the most common cyber threats and reduce their online vulnerability. It defines a focused set of five technical controls which offer cost-effective, basic cyber security, via two levels of certification:

- **Cyber Essentials (CE):** The basic verified self-assessment option
- **Cyber Essentials Plus (CE Plus):** As above, but independent technical verification is also carried out by the Certification Body

Cyber Essentials is operated in partnership between the Department for Science, Innovation and Technology (DSIT)[1] and the National Cyber Security Centre (NCSC). It is delivered through the IASME Consortium Ltd. (IASME).

The government wishes to increase the number of organisations holding Cyber Essentials. A total of 132,094 Cyber Essentials certificates have been awarded since the scheme began. IASME's latest records (as of the end of May 2023) show a total of 27,027 unique Cyber Essentials certified organisations across the UK in the past 12 months, with 35,434 total certifications awarded in the past 12 months. The difference between the two figures denotes 8,407 CE Plus certifications which are counted additionally to standard CE certifications.

Analysis shows steady year-on-year-growth, for example fewer than 500 certificates were issued per month in January 2017, rising to just under 3,500 in the month of January 2023.

Since Cyber Essentials certification is renewed annually, it is important to note that the figures in the preceding two paragraphs do not take into account any that may have lapsed.

Throughout this report, the term Cyber Essentials is used to refer to the overall scheme (including both levels mentioned above) and the separate terms CE and CE Plus are used when referring to one particular level.

Evaluation aims

In December 2022, the (then) Department for Digital, Culture, Media and Sport (DCMS), commissioned Pye Tait Consulting to undertake a process evaluation of the Cyber Essentials scheme. This is supplemented by a feasibility study for a subsequent impact

[1] In February 2023, parts of the UK government responsible for cyber security policy moved to the Department for Science, Innovation and Technology (DSIT) from the Department for Digital, Culture, Media and Sport (DCMS).

evaluation to be conducted at a later date. The findings are intended to enable DSIT, NCSC and IASME to ascertain whether the current implementation approach is working and allowing the scheme to meet its objectives.

Methodology

The evaluation methodology comprised the following main components:

- Rapid desk research to understand relevant policy, developments and existing research and evaluation findings in relation to Cyber Essentials (January 2023)

- 12 qualitative interviews with strategic stakeholders that have close involvement with Cyber Essentials, including representatives from government and industry (UK, including devolved nations) as well as IASME, NCSC and a sample of former Accreditation Bodies. (January 2023)

- Online survey of Certification Bodies[2] (95 responses), representing a 30% response rate of the total population of 315 mailed Certification Bodies

- Online survey spanning current Cyber Essentials users (528 responses) and lapsed Cyber Essentials users (47 responses)

- Small-scale phone survey of organisations that had never held Cyber Essentials (74 responses based on a 60-85 target)

Cyber Essentials decision-making

Among surveyed current and lapsed users, the standard CE certification is the most commonly held. CE Plus is more prevalent among large organisations, for which it accounts for just over half (51%) of certifications, compared to just 17% among micro organisations.

The small sample of lapsed users had held their certification for varying lengths of time, with drop-offs highest after the first year (45%) then 32% after two years and 21% after three or more years.

Among micro organisations, overall responsibility for certification is most commonly handled by the owner or manager. The larger the size-band of the organisation, the more common it is to place overall responsibility for Cyber Essentials certification in the hands of a dedicated in-house IT or data security specialist.

With the exception of the ISO 27001 standard on Information Security and Management, which more than half (56%) of Cyber Essentials users had considered and a further 23% taken up, most had not heard of or considered other specific schemes and standards asked about in the survey.

Some organisations believe that Cyber Essentials provides a benchmark standard that companies ought to naturally strive for, even if considering other security schemes or

[2] Certification Bodies are companies across the UK responsible for delivering the Cyber Essentials scheme. They have qualified assessors and certify organisations on behalf of IASME, the Accreditation Body.

standards such as ISO 27001. Others reflected on the differences between Cyber Essentials and other schemes, indicating that they each have their own place in the market.

Qualitative insights reveal that Cyber Essentials is broadly regarded by users as a basic and accessible security standard compared to other schemes or standards. However, large organisations in particular expressed the view that ISO 27001 is more rigorous and appropriate to their setting.

Factors driving Cyber Essentials certification

When asked why their organisation first decided to become Cyber Essentials certified, current and lapsed users mentioned a range of factors, including those which are reactive to others' requirements and perceived needs, and those which are proactively aimed at benefiting their own organisation.

The most common single main reason (mentioned by just over a third, 34%) is that Cyber Essentials is a requirement of a public sector contract. Micro businesses in particular appear to be less strongly motivated by improving their own cyber security and resilience, and more strongly motivated by external influencers such as customer or contractual requirements. This suggests that Cyber Essentials certification is, in some cases, serving as a means to an end – a view also reflected in some of the qualitative feedback.

The majority of respondents (82%) consider it important to understand the perceived benefits of becoming Cyber Essentials, and most also place importance on planning various logistical inputs in terms of expertise, resources and costs. This makes it essential that organisations are clear from various information and guidance what the Cyber Essentials scheme expects of them.

The most prominent reason for current and lapsed users opting for CE as opposed to CE Plus was that they saw no obvious need for CE Plus (65% of respondents). Conversely, most of those opting for CE Plus did so to maximise cyber security and resilience (54%).

The top three reasons for Cyber Essentials certification lapsing, each mentioned by a minority of respondents, are that it was too difficult to keep up with changing controls (28%), too expensive (23%) and too time-consuming (19%). This points to some challenges in a scheme which by its very nature is prescriptive rather than risk-based.

Cyber Essentials information and guidance

The most widely accessed information and guidance sources about Cyber Essentials include the IASME website, followed by NCSC, DCMS and Certification Body websites. This suggests that organisations are generally accessing information from trusted sources. Large organisations are more inclined to draw on a wider range of sources including conferences, seminars and networking events.

Two thirds of current and lapsed users (66%) needed to ask questions or seek help during the certification process. The figure is 80% among large organisations, indicating a need for more bespoke support appropriate to the complexities of their organisation. The most common place to turn to is the Certification Body (53%), making it important that Certification Bodies are open and willing to provide the assistance needed to help organisations achieve the ultimate end goal of becoming more cyber resilient.

Support during the certification process is generally viewed positively, with more than half of respondents (54%) describing it as very helpful and 36% quite helpful. More than a fifth (21%) of lapsed users describe support as not very or not at all helpful – three times higher than the proportion of current users – which may have contributed to these organisations' decisions not to renew.

Some concerns raised by survey respondents are that existing scheme guidance adopts a 'one-size-fits-all' approach which does not adequately speak to or benefit certain types and sizes of organisation. Indeed, half of current and lapsed users (50%) would like to see better tailoring of online information and guidance by organisation size or complexity, followed by more detailed guidance (42%) and clearer guidance (41%).

The majority also call for greater clarity around Cyber Essentials assessment requirements, especially where elements can be too easily open to interpretation. For their part, several Certification Bodies stressed the need to provide more foundational information to help users understand the importance of cyber security and threats in a more general sense.

Cyber Essentials customer journey

The overall cost and time involved for organisations to obtain certification varies considerably between organisations and especially between size-bands. The overall mean spend (excluding outliers) is estimated at £4,941. This factors in resources needed to meet the technical controls such as consultancy support and changes to hardware, software and updated policy implementation.

Whilst cost and time were not among the main difficulties cited by users in their customer journey, the fact that these featured among the top three reasons for certification lapsing suggests that cost and time stresses are almost certainly being felt by some organisations. This points to a potential need to review the pricing structure for Cyber Essentials.

On the whole, most surveyed current and lapsed users have had a positive certification experience, with the majority rating various specific aspects of the customer journey as very or quite good. However, and building on the previous section, the quality and suitability of information and guidance is considered by more than a quarter (29%) to be very or quite poor.

The vast majority of surveyed current and lapsed users (86%) report working with their Certification Body to have been very or quite easy, which is important given the reliance many organisations place on their Certification Body for support. However, views are more divided on the ease of fulfilling the technical controls. Whilst the majority (62%) consider this very or quite easy, more than a third (38%) do not.

Qualitative insights reveal that the most positive aspects of the customer journey relate to: i) feedback, support and guidance from Certification Bodies and assessors; ii) ease of completing the process; and iii) improving security. The most difficult aspects relate to: i) lack of clarity or understanding of aspects of the process; ii) difficulties meeting the technical controls; and iii) keeping up with changes.

On a perceptual scale from 1 (not at all appropriate) to 10 (completely appropriate) organisations rate the technical controls at a moderate 7.1. Among micro and large

organisations, the means are lower (6.6 and 6.5 respectively) – a significant difference. There appear to be distinct issues facing the largest and smallest organisations. For large organisations, the controls can be difficult to implement at scale due to IT infrastructure complexities. For micro organisations, the main challenge lies in the perceived cost, time and expertise required to implement them, especially where they lack access to an expert IT resource.

Academic institutions also appear to face unique barriers, as evidenced from this and other research. The prevalence of Bring Your Own Device (BYOD) practices in these settings has led to some of these organisations expressing concern about their perceived ability to meet the requirements of Cyber Essentials.

There is a significant difference between the perspectives of Certification Bodies and of current and lapsed users in how well changes to control arrangements are communicated. Only a minority of current and lapsed users consider changes to have been communicated very or quite well, which points to a possible disconnect in how well Certification Bodies believe certain communications have been deployed compared with the user base.

Cyber Essentials scheme effectiveness and improvement

With respect to Cyber Essentials scheme governance, strategic stakeholders say partnership working has increased. They suggest that it could be strengthened by a greater commitment to transparency, sharing information that would benefit all parties, and taking on board feedback with a view to making changes that would serve the greater good.

In terms of scheme implementation, strategic stakeholders (representatives from government and industry) stressed the challenge of the current ‘one-size-fits-all’ approach where there are quite different challenges to implementing cyber security measures by organisations of different types, sizes and sectors. As such they advocate more in-built flexibilities where this would be possible. The Pathways pilot project (cf. section 1.2) is one example of this.

In relation to consistency of work between Certification Bodies, a minority of stakeholders questioned the appropriateness of Certification Bodies fulfilling the dual roles of assessor and advisor to organisations seeking certification. However, this argument needs to be balanced against the importance users place on the support they get from Certification Bodies and the ultimate goal, which is about building organisations’ protection against threats.

The majority of current and lapsed users believe that going through the Cyber Essentials process has improved their cyber security awareness and understanding (71%) and, as a result, they are better able to mitigate cyber security risks in their own organisation (52%).

Just over two thirds (67%) would recommend Cyber Essentials to others. These users, especially registered charities and trusts, view the scheme as cost-effective and accessible. Users that would not recommend Cyber Essentials to others do not typically believe that the controls are applicable or relevant to the workings of their own organisation. This points to a need to consider how, if at all, the controls could be more flexible or adaptable.

Current and lapsed users were asked to what extent they agree that the Cyber Essentials scheme overall represents good value for money. The emerging picture is mixed. While the

majority (58%) strongly agree or agree, just over a quarter (26%) are ambivalent and a minority (16%) disagree or strongly disagree. This offers an opportunity to help organisations better understand what they are getting in return for their investment.

Certification Bodies, which were also asked about the scheme's effectiveness and improvement, compliment it for providing an effective and accessible security baseline for certified organisations. However, a key perceived challenge is that users and potential users lack a sufficiently detailed understanding about cyber security. These findings emphasise the importance of more effectively conveying to current and prospective users the importance of cyber security, why they should take it seriously and how Cyber Essentials provides a cost-effective solution to starting that journey.

The majority of Certification Bodies (59%) are very or quite confident that the Cyber Essentials scheme is being delivered consistently by different Certification Bodies, although 36% are not very or not at all confident. Most mentioned differing requirements, standards and capabilities between Certification Bodies as being potential reasons for lack of consistency.

All surveyed organisations were asked in what ways they think the Cyber Essentials scheme could be improved in the future. Suggestions fall into the following five main themes: i) better tailoring and scalability; ii) improvements in communication, guidance and support; iii) reduced cost; iv) quality and scrutiny of assessments; and v) synergy with other security schemes.

Non-users of Cyber Essentials

Among 74 surveyed organisations that have never held Cyber Essentials, eight in ten consider cyber security very important to their organisation. However, of the 15% answering not very or not at all important, all are micro organisations. These businesses could therefore be the hardest to engage in terms of future take-up.

The minority stating ‘not very or not at all important’ mentioned mainly doing business on their phone, doing little business online, using paper-based records, being content to use free internet security software and in one case not trusting the government.

Almost two thirds (64%) of the 74 surveyed organisations that have never held Cyber Essentials had not heard of it prior to taking part in the survey. The vast majority had also not heard of other specified cyber security schemes or standards, which points to a potential target market for Cyber Essentials that may lack cyber security and an understanding of the importance of becoming more cyber secure.

Among 11 of these organisations that had hitherto heard of and considered taking up Cyber Essentials, their main reasons for not taking it up were that they considered it too time-consuming or lacking compatibility with different devices. These are issues that marketing, information and guidance could potentially help to address where there are misconceptions.

All 74 organisations were asked what would be needed for their organisation to consider obtaining Cyber Essentials certification in the future. The top three answers are primarily reactive, including: if it is required by a contract we want to work on (58%), if it is a

requirement of our customer(s) (47%) and if senior leaders in our organisation asked for it (35%).

Many non-Cyber Essentials users indicated that they would be interested in finding out more about the scheme, had an open mind about it, would be willing to discuss it with their third-party IT providers (as appropriate) and, in some cases, are considering reviewing their cyber security needs in the near future. These responses indicate potential opportunities to improve awareness and understanding of Cyber Essentials in the market, including its value.

Conclusions

The following are high-level conclusions. More detail on each is provided in section 8.1.

1. The most common reasons for adopting Cyber Essentials are reactive rather than proactive, risking the scheme being perceived as a “hoop to jump through” in order to fulfil contract requirements.

2. Stronger focus should be placed on promoting the dangers and threats associated with conducting business online, so organisations can better appreciate why a cyber security solution such as Cyber Essentials is important.

3. There is evidence that the certification process is making a positive difference to users’ cyber behaviours, although there is a mixed picture concerning perceived value for money.

4. The cost and time inputs needed to go through the certification process vary widely between organisations, with high costs (including, but not limited to, scheme pricing) potentially affecting take-up and retention of Cyber Essentials certification.

5. Some of the largest and smallest organisations face substantial yet quite different obstacles to meeting the technical controls, indicating inherent challenges to the scheme’s prescriptive (i.e. rather than risk-based) and one-size-fits-all concept.

6. Updates to the technical control requirements are clearly important but communications about changes – especially major updates – appear to be inadequate and are not sufficiently timely for organisations to plan ahead.

7. Existing information and guidance could be improved with better tailoring and simplification for different types and sizes of organisation.

8. There is a clear market opportunity for Cyber Essentials among organisations that have never been certified under the scheme and which consider cyber security very important.

9. Anecdotal evidence points to pockets of weakness in the rigour of the Cyber Essentials assessment process. This could be overcome through education and guidance aimed at users in relation to cyber threats, risks and potential consequences, as well as the benefits of becoming more cyber resilient.

Recommendations

The following are top-level recommendations aimed at DSIT, IASME and NCSC to consider as part of a coordinated approach. More detail on each is provided in section 8.2.

1. **Increase awareness and understanding about cyber security threats and provide users with an informed choice about the most appropriate solution for them.**

    a. Help to build a more foundational awareness among organisations of the importance of being cyber secure.

    b. Develop more and better information about the features and benefits of the Cyber Essentials scheme in comparison to alternative schemes and standards.

    c. Consider not mandating Cyber Essentials in public sector procurement contracts where suitable alternatives are already held.

2. **Improve information, tools and guidance aimed at current and potential users.**

    a. Provide more and better information to articulate the differences between the standard and Plus schemes.

    b. Produce more information and training resources via webinars, videos and infographics to help convey key aspects of the Cyber Essentials scheme.

    c. Improve the clarity and simplicity of scheme information and guidance.

    d. Produce and share best practice case studies on the customer journey.

    e. Consider introducing an online chat interface.

    f. Deploy user testing to help improve the clarity of assessment questions.

3. **Provide more tailored information to different types and sizes of business, and consider more targeted and high-profile marketing and communications.**

    a. This could include tools to help organisations self-assess whether Cyber Essentials is right for their organisation and setting.

    b. Consider a targeted marketing campaign to other key enablers in the cyber security space, such as IT support sector businesses.

    c. Consider producing and running hard-hitting media adverts about the risks of a cyber breach – via television, radio or social media depending on the costs involved.

4. **Consider the feasibility of adapting aspects of the Cyber Essentials scheme to be more responsive to current user needs.**

    a. Build in flexibilities where possible, especially those which would help large organisations and academic institutions to meet the technical controls.

    b. Put in place a coordinated communications plan to more frequently and timeously distil information through Certification Bodies about changes and updates to control arrangements.

    c. Explore further the relative merits of increasing the length of certification to three years, albeit with annual audits comparable to ISO 27001.

    d. Allow more time for organisations to provide additional information in response to requests during the assessment process.

    e. Review the scheme's pricing structure, for example explore further whether the fee for assessment is a barrier to certification, or consider a more nuanced approach to assessment fees, such as a special rate for startups or lower reassessment costs at annual renewal.

5. **Commit to strengthening scheme robustness and transparency**

    a. Consider how the scheme is positioned in relation to other NCSC schemes to ensure there is no risk of competing narratives.

    b. Actively encourage organisations to provide regular feedback to IASME and NCSC.

    c. Continue to work collaboratively with Certification Bodies towards greater consistency.

    d. Consider an education campaign, potentially combined with more robust protocols to guard against organisations potentially providing false information in order to gain Cyber Essentials certification.

1. Introduction

This chapter sets the scene by explaining the UK government's commitment to ensuring a cyber secure economy, providing background information about the government-backed Cyber Essentials scheme and how it works, and presenting the evaluation aims, objectives and methodology. It also presents a brief rundown of key evidence and statistics from approximately the last five years that are relevant to the process effectiveness of the Cyber Essentials scheme.

1.1 UK cyber resilience

The world is now more connected than ever before, with technology driving extraordinary opportunity, innovation and progress. However, the pace of change in the digital age also gives rise to additional complexity and risk.

The UK government is committed to making the UK the safest place in the world to be online and the best place in the world to start and grow a digital business. A key aspect of this is the government's National Cyber Strategy (NCS) 2022 which sets out ambitious policies to protect the UK in cyberspace, backed by a £2.6 billion investment to put technology at the heart of plans for national security.

Under Pillar 2 of the Strategy – building a resilient and prosperous digital UK – the government has set the following objectives to 2025:

1. Improve the understanding of cyber risk to drive more effective action on cyber security and resilience

2. Prevent and resist cyber attacks more effectively by improving management of cyber risk within UK organisations and providing greater protection to citizens

3. Strengthen resilience at national and organisational level to prepare for, respond to and recover from cyber attacks

As part of this effort, the government aims to continue to promote take-up of accreditations and standards such as the Cyber Essentials certification scheme.

1.2 About Cyber Essentials

Cyber Essentials is a government-owned scheme that was developed to help organisations of all sizes defend against the most common cyber threats. It provides reassurance to organisations and their customers that systems are more resilient to basic cyber-attacks.

The scheme has three main functions, aimed at increasing the cyber resilience of the wider economy by raising the baseline of cyber security. These functions are:

1. To help organisations put in place fundamental technical controls that increase their resilience and build their confidence in their security posture

2. To enable organisations to manage third-party cyber security risks, receiving assurance from suppliers and partners that they have implemented core technical controls effectively

3. To provide Cyber Essentials certification for organisations in order to give assurance of basic cyber hygiene to the market (consumers, customers, suppliers and other business partners)

The purpose of implementing these measures is to significantly reduce an organisation's vulnerability. Indeed, the government's Procurement Policy Note 09/14 introduced a mandatory requirement for Cyber Essentials certification for organisations working on UK central government contracts to meet certain criteria, notably where this involves handling personal information and providing certain ICT products and services.

It should be noted that Cyber Essentials does not offer a silver bullet to protect against all cyber security risks. For example, it is not designed to address more advanced, targeted attacks, hence organisations facing these threats should consider additional measures as part of their security strategy. What Cyber Essentials does do is define a focused set of controls which offer cost-effective, basic cyber security for organisations of all sizes. It protects certified organisations against common cyber threats which are readily available for attackers to employ who themselves have little technical expertise.

There are two levels of certification:

1. **Cyber Essentials:** This is the basic verified self-assessment option. The scheme is centred around five technical controls designed to significantly reduce the impact of common cyber attack approaches.

   Steps to certification typically involve working with a Certification Body to apply for an online assessment account, paying the relevant certification fee, completing the online assessment, and supporting documents, and submitting this information for review, resulting in the award of a certificate valid for one year.

2. **Cyber Essentials Plus:** Takes the same approach and aims to put the same protections in place but in this case, independent technical verification is also carried out by the Certification Body.

Throughout this report, the term Cyber Essentials is used to refer to the overall scheme (including both levels mentioned above) and the separate terms CE and CE Plus are used when referring to one particular level.

The five technical controls are:

1. **Firewall configuration:** Prevents unauthorised access to or from private networks

2. **Secure configuration**: Ensures that systems are configured in the most secure way for the needs of the organisation

3. **User access control:** Ensures that only those who should have access to systems access them at the appropriate level

4. **Malware protection:** Ensures that virus and malware protection is installed and up to date, including application 'allow' listing

5. **Security update management:** Ensures that the latest supported hardware, software and cloud services are used, and that the necessary patches supplied by vendors have been applied

The technical controls are reviewed on a 12-month rolling basis and ensure that the Cyber Essentials scheme continues to help UK organisations guard against the most common cyber threats. In 2022, a major update was made to the technical controls – the biggest since the scheme started in 2014. Updates to technical controls are published online with an 'effective from' date. All applications started on or after that date are subject to the new requirements and associated assessment questions.

Governance and delivery mechanisms

Cyber Essentials is a government scheme, operated in partnership between the Department for Science, Innovation and Technology (DSIT)[3] and the National Cyber Security Centre (NCSC). It is delivered through the IASME Consortium Ltd. (IASME). The scheme launched on 5th June 2014 and, from April 2020, IASME became the NCSC's sole Cyber Essentials partner responsible for the management and delivery of the scheme. Prior to that, it was delivered by five Accreditation Bodies, which included IASME.

Partnership meetings between IASME and NCSC take place once a quarter and create a platform to discuss the collaborative relationship and any strategic issues that may arise. These meetings are in addition to weekly business as usual meetings, marketing and communications meetings and customer service meetings. A technical working group is also in place to review and update the technical requirements of the scheme. The input of NCSC's subject matter experts also helps to ensure Cyber Essentials controls align with evolving threats and attack vectors.

IASME has accredited over 300 Certification Bodies[4], comprising over 800 individual assessors, across the UK which are trained and licensed to certify organisations to the Cyber Essentials Scheme.

Latest available Cyber Essentials uptake data

The government wishes to increase the number of organisations holding Cyber Essentials. A total of 132,094 Cyber Essentials certificates have been awarded since the scheme began. IASME's records (as of the end of May 2023) show a total of 27,027 unique Cyber Essentials certified organisations across the UK in the past 12 months, with 35,434 total certifications awarded in the past 12 months. The difference between the two figures denotes 8,407 CE Plus certifications which are counted additionally to CE.

[3] In February 2023, parts of the UK government responsible for cyber security policy moved to the Department for Science, Innovation and Technology (DSIT) from the Department for Digital, Culture, Media and Sport (DCMS).
[4] Certification Bodies are companies across the UK responsible for delivering the Cyber Essentials scheme. They have qualified assessors and certify organisations on behalf of IASME, the Accreditation Body.

Trend analysis shows steady growth, with fewer than 500 certifications issued per month in January 2017, rising to just under 3,500 in January 2023. In the calendar year of 2022, there were 24,300 CE certifications, of which 16,554 were recertifications and 7,746 new certifications. Since Cyber Essentials certification is renewed annually, the above figures do not take into account any that may have lapsed.

Monthly data from April 2021 also shows a steady growth in the number of accredited Certification Bodies, from 269 in April 2021 to 315 in January 2023.

Scheme developments

In November 2021, NCSC and IASME completed a major technical review of the scheme, the results of which informed the updated January 2022 requirements that make up the controls. The update includes revisions to the use of cloud services, as well as home working, multi-factor authentication, password management, security updates and more. Cyber Essentials-certified organisations are required to meet revised control requirements when seeking renewal of their Cyber Essentials certification.

NCSC recently launched a Funded Cyber Essentials Programme which, according to published information, offers “some small organisations in high-risk sectors” practical support at no cost to help put baseline cyber security controls in place. The initiative, funded by government and delivered by IASME, will see eligible organisations receive 20 hours of expert support to help implement the five technical controls needed to gain Cyber Essentials certification.

As part of another scheme, qualified Cyber Advisors will be able to offer consultancy services to help their customers understand and meet the five technical controls. Organisations who have a qualified Cyber Advisor on their staff will be able to apply to become an NCSC Assured Service Provider to deliver these services. It should be noted that NCSC will be looking to extend the scope of Cyber Advisor services to cover aspects of basic cyber security other than Cyber Essentials over the coming years.

Additionally, for large organisations with complex IT infrastructure, IASME is working with NCSC on a Pathways pilot project. Based on the typical risk scenario outlined above, Pathways offers a route to test the veracity of alternative technical controls an organisation may have implemented to protect itself from such commodity attacks. This will involve deploying a set of tests similar to a simulated attack and organisations that pass will achieve a Cyber Essentials Plus certificate. The results of the pilot are expected in the second quarter of 2023 with the potential for wider roll-out if deemed successful. The scheme is likely to be comparatively more expensive than Cyber Essentials Plus due to the more specialist expertise needed in the assessment stage.

1.3 Evaluation aims and objectives

In December 2022, the (then) Department for Digital, Culture, Media and Sport (DCMS), commissioned Pye Tait Consulting to undertake a process evaluation of the Cyber Essentials scheme. This is supplemented by a feasibility study for a subsequent impact evaluation to be conducted at a later date. The findings are intended to enable DSIT, NCSC and IASME to ascertain whether the current implementation approach is working and allowing the scheme to meet its objectives.

The evaluation objectives can be summarised as follows:

1. Identify organisations' Cyber Essentials certification characteristics, decision-making and motivations for becoming Cyber Essentials certified
2. Explore organisations' views on Cyber Essentials information and guidance
3. Understand how aspects of the Cyber Essentials customer journey work in practice
4. Determine how well the scheme is perceived to be operating
5. Offer suggestions for improving the scheme
6. Set out the feasibility for a possible subsequent impact evaluation

The feasibility study for a subsequent impact evaluation can be found in Appendix 1.

1.4 Methodology and participant numbers

The evaluation methodology comprised the following main components:

Component	**Details**	**Dates**
Rapid desk research	To understand relevant policy, developments and existing research and evaluation findings in relation to Cyber Essentials	January 2023
12 qualitative strategic stakeholder interviews	Conducted with representatives from government and industry (UK, including devolved nations) as well as IASME, NCSC and a sample of former Accreditation Bodies	January 2023
Online survey of Certification Bodies	95 responses, representing a 30% response rate of the total population of 315 mailed Certification Bodies	27 January – 17 February 2023
Online survey spanning current and lapsed Cyber Essentials users	528 responses (current users) 47 responses (lapsed users)	27 January – 17 February 2023
Small-scale phone survey of organisations that had never held Cyber Essentials	74 responses	February 2023

The online survey of Certification Bodies was facilitated with the support of IASME.

The online survey link for current and lapsed users was sent by email to Certification Bodies for onward email distribution to their own users. It was also distributed by IASME to a further sample of users for which IASME held contact details and consent to take part in market research.

The phone survey of organisations that had never held Cyber Essentials (hereinafter referred to as non-Cyber Essentials organisations) was intentionally small-scale to provide a gauge of attitudes, perceptions and motivations among this audience to supplement evidence from those that had already been through the process.

Due to the protracted approach to distributing the online survey link to current and lapsed users, the total number invited to take part through Certification Bodies is not known. This prohibits a response rate being accurately calculated for these audiences.

Overall margins of error

Survey of Certification Bodies: Based on a population of 315 Certification Bodies, a total of 95 survey responses yields an overall margin of error for the survey of ±8.4% at the 95% confidence level.

Survey of current users: Based on a total count of 24,955 Cyber Essentials certified organisations in the month of survey launch (IASME, January 2023), a total of 528 survey responses from current users yields an overall margin of error for the survey of ±4.2% at the 95% confidence level.

Margins of error have not been calculated for the surveys of lapsed users and non-users since these surveys are very small scale and the findings should therefore be treated with extreme caution.

It should be noted that margins of error are inevitably higher for questions not answered by all respondents and where cross-tabulations of the results are performed.

1.5 About the presentation of findings in this report

This report presents the findings of the process evaluation by theme, with the perceptions of strategic stakeholders threaded throughout to complement survey insights on similar topics and questions.

Chapters 2 to 6 present the survey results using narrative descriptions and charts. These are supplemented (where applicable) by tables showing further breakdowns. Some questions were asked of all respondent groups (i.e. Certification Bodies, current and lapsed users) and some only of certain respondents.

The base number of respondents, along with the respondent groups applicable to a particular survey question, are shown in each chart. These appear either in the Y axis labels (to show bases per respondent group) or below the X axis (to show overall respondents) depending on the type of question.

Most survey results from current and lapsed users show cross-tabulations by employment size-band. This is on the assumption that organisation size is a key influencing criterion in

relation to the opportunities and barriers to obtaining Cyber Essentials certification. Size-bands have been defined as follows:

- Micro (fewer than 10 staff)
- Small (10-49 staff)
- Medium (50-249 staff)
- Large (250+ staff)

There are a small number of exceptions where breakdowns by size-band are not displayed – either where this would require a substantial amount of tabulated data or where base numbers are low.

Statistical significance tests have been carried out on certain questions to assess whether differences in the distribution of results per size-band and per organisation type (Certification Bodies, current and lapsed users, as applicable) are due to chance or whether they represent meaningful differences between the groups. The term 'significant' is therefore used throughout this report to denote statistically significant differences.

Chapter 7 presents findings separately from the smaller number of organisations that have never held Cyber Essentials certification. For this cohort, not all results are expressed in percentage terms or using charts or tables, i.e. where the base number to a question falls below 40 responses.

A detailed breakdown of survey respondent numbers by different profiling characteristics (including employment size-band) can be found in Appendix 2.

The overarching evaluation questions, along with the two survey questionnaires aimed at: i) current and lapsed users; and ii) non-users of Cyber Essentials, are available as a separate Annex to this report.

1.6 Process effectiveness – evidence to date

A limited body of recent research relating to cyber resilience and cyber security measures has paid discrete attention to Cyber Essentials. This section summarises key findings from key recent publications where broadly relevant to this process evaluation.

In summary, existing research pays strong attention to aspects of Cyber Essentials awareness among users, motivations for becoming certified (including differences by size-band of organisation) and barriers to uptake. However, insights to date have been more limited with respect to the detail of the customer journey, helpfulness of support received, and views on how specific aspects of scheme processes could be strengthened. These are areas which this evaluation explores in particular detail, combining survey research that draws comparisons between different audience groups, combined with perceptions of strategic stakeholders.

Firstly, the Cyber Security Breaches Survey 2022 (based on responses from 1,243 businesses and 424 charities) found just 16% of surveyed businesses to be aware of Cyber Essentials. However, there has been a steady increase over the past seven years with awareness having doubled from 8% in 2017. Awareness as recorded by this survey is highest among large organisations (62%), followed by medium-sized organisations (49%)

leading to the conclusion that more could be done to raise awareness of Cyber Essentials among small and micro organisations.

The Cyber Security Longitudinal Study is focused on medium and large businesses (50+ employees) and high-income charities (annual income of more than £1 million). The findings from Wave Two (December 2022, which surveyed 1,741 organisations) found an increase compared to Wave One (a year earlier) in the proportion of organisations certified to at least one of three standards asked about in the study: CE, CE Plus, or the ISO 27001 Standard for Information Security Management Systems. For example, between Wave One and Wave Two the proportion rose from 32% to 40% among businesses, and from 29% to 36% among charities. It found Cyber Essentials to be most often adhered to by businesses (25%) and charities (28%) compared to other certifications, with both shares higher than in Wave One.

The Review of Cyber Essentials influence on cyber security attitudes and behaviours in UK organisations (2020) involving 542 organisations, identified that Cyber Essentials-certified organisations were more likely than their non-certified counterparts to be:

- Aware of the risks posed by cyber-attacks (including at a senior level)
- Confident that they were protected from these attacks
- Implementing cyber security controls, including taking steps beyond the technical controls required to become certified
- Positive about the scheme, particularly its impact on customer and investor confidence

On the one hand, this suggests that messaging and processes through the Cyber Essentials scheme are making a tangible difference. However, the same research indicated that, for medium-sized and large organisations in particular, Cyber Essentials seemed to be reinforcing existing attitudes and behaviours rather than driving them.

A main indicated barrier to more organisations becoming certified was an apparent lack of knowledge about the scheme overall, including its costs and value. Another finding from the research among organisations that had yet to be certified was that a large minority felt that they were already following some or even all of the technical controls (with 25% claiming to follow all of them). Key recommendations from the above study included the need to improve awareness and knowledge of Cyber Essentials among non-certified businesses, encourage organisations to look for Cyber Essentials across their supply chains and use certification as an opportunity to drive other behaviours and awareness.

In their 2021 article A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs, Karen Renaud and Jacques Ophoff, citing sources, asserted that there are signs of improving awareness among small and medium-sized enterprises (SMEs) of the cyber security domain. They argue that this “could be attributed to more focused cyber security awareness campaigns targeting SMEs”.

The same article describes the Cyber Essentials scheme as providing advice and certification, and the Cyber Aware campaign of providing sole traders and small businesses with a bespoke action plan to improve their cyber security. However, it adds, citing sources, that “there is an unwritten assumption that SMEs will seek out advice related to precautions

to be taken from reliable sources", which it says "is likely to be naïve". It also highlights that SMEs can be unaware that the threats they are being warned about are relevant to them, whilst at the same time lacking resources to deal with them.

This evidence points to the theory – as noted by Steven Kemp (2022) in Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach – that providing cyber security advice does not necessarily promote organisational behaviour change; there is a complex relationship between knowledge of threats and responses and changes in behaviour.

Osborn and Simpson (2017) in their journal article On small-scale IT users' system architectures and cyber security: A UK case study highlighted how costs can impede smaller companies following standards designed to foster good cyber security practices. They specifically mentioned how business processes in smaller organisations and the perceived complexity of the Cyber Essentials programme could combine to limit uptake.

Renaud and Ophoff, in their (unpublished) 2021 report What is Preventing UK SMEs from taking Cyber Security Precautions?, identified the following obstacles to uptake:

Advice issues

- Government advice not being useful
- Too much advice
- Uncertainty
- Information avoidance
- Poor understanding of strong password requirements

Perceptions

- Realisation of need for more resources
- Realisation of need for more support
- Halo effect (a perception that current practices are so good that they cannot be improved upon)
- Feeling insignificant

Social

- No pressure from customers
- Employees not supporting each other

In 2023, Vodafone published a report titled The business of cyber security: protecting SMEs in the changing world of work. Although this report does not include information regarding the sampling and survey methodology used, it asserts that with the cyber security risks faced by SMEs coming in various guises, help is needed, and that for some businesses, there is a real risk of loss of staff and even of business collapse. The report points to a lack of basic digital skills as well as a vast disconnect between how vulnerable most business leaders think they are and how vulnerable they are in reality.

Vodafone's polling of over 400 SMEs shows the extent to which these organisations are currently experiencing attempted cyber attacks, the scale of the risk they pose and what – if anything – they are doing about it.

Key findings are summarised as follows:

- Almost one in five (19%) of SMEs polled said that an average cyber attack deemed to cost £4,200 (a figure prompted to respondents based on an average taken from the Cyber Security Breaches Survey) would destroy their business

- The majority (54%) had experienced an attempted cyber attack in the past 12 months

- 18% said their business was not protected with cyber security software and a further 5% did not know

- Only 28% were aware of the Cyber Essentials scheme – with more SMEs saying they had heard of a cyber security product that does not actually exist

The report remarks that many SMEs are insufficiently persuaded or lack the knowledge and finance they need to put that protection in place. It adds that the government should do more to support the delivery of local cyber security skills and welcomes progress that has been made with the establishment of nine regional Cyber Resilience Centres (CRCs) across England and Wales.

Finally, the National Cyber Resilience Centre Group (NCRCG) is a not-for-profit company, funded and supported by the Home Office, in conjunction with policing and other partners. It aims to strengthen the reach of cyber resilience across the business community, particularly among SMEs and supply chains. The nine CRCs are mapped according to the location of each police Regional Organised Crime Unit. Each CRC retains regional leadership and the freedoms to deliver tailored, trusted and affordable support to local organisations.

2. Cyber Essentials Decision-Making

This chapter explores how Cyber Essentials certification has been implemented and managed by surveyed current and lapsed users of the scheme, including why they opted for a particular level of certification. It also looks at which other schemes and standards users have considered or taken up (with reasons), their main motivations for taking up Cyber Essentials and – where appropriate – why certification lapsed.

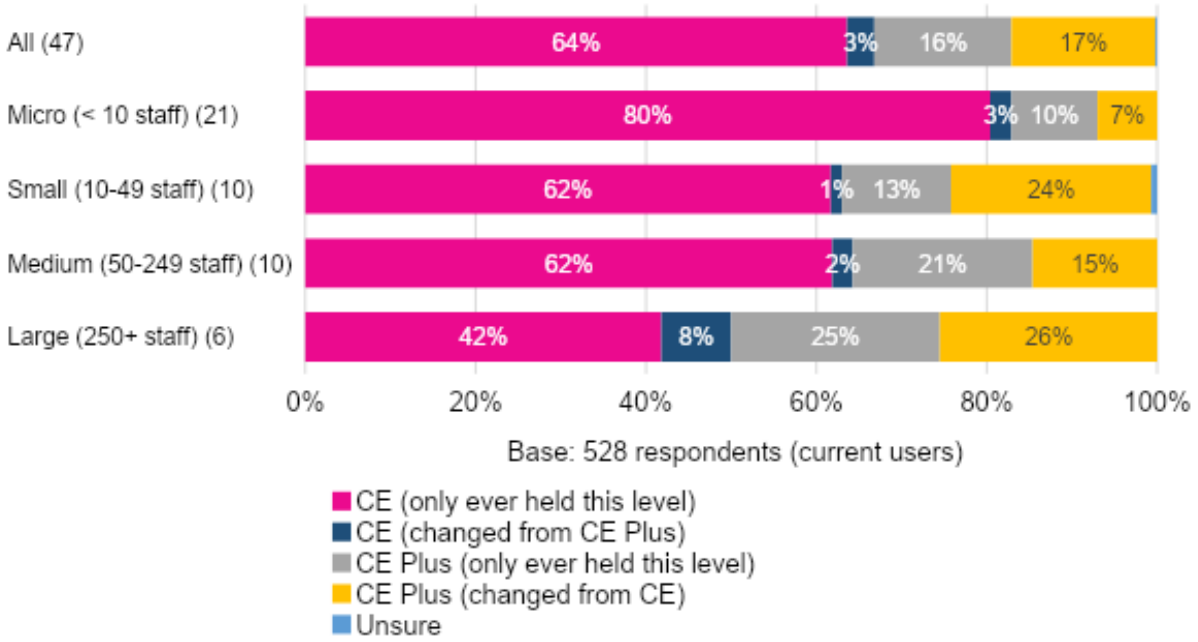
2.1 Characteristics of certification

Level of certification

Firstly, looking at the levels of Cyber Essentials certification held by surveyed current users, CE is more common than CE Plus. Almost two thirds (64%) have only ever held CE, compared to less than a fifth (16%) who have only ever held Plus. There is a much stronger prevalence of users changing from CE to CE Plus than those changing from CE Plus to CE.

The proportion of micro organisations that have only ever held CE is significantly higher (80%) than other size-bands. Similarly, the proportion of large organisations that have only ever held CE Plus (a quarter, 25%) or changed to CE Plus (26%) is significantly higher than micro businesses (Figure 1).

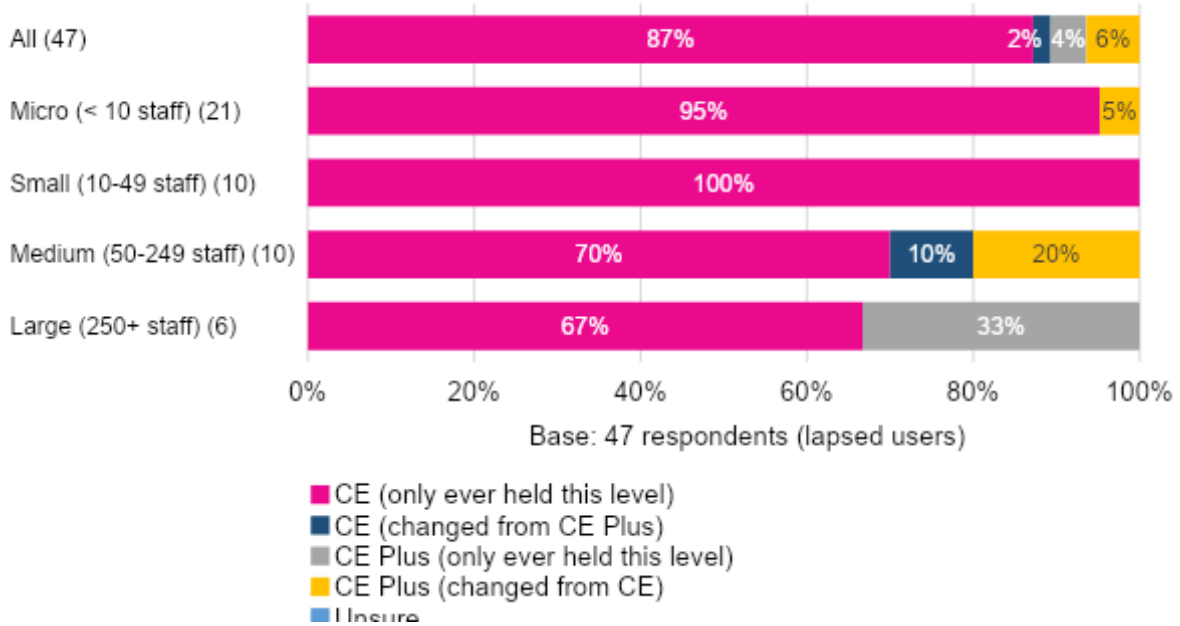
Figure 1 Level of Cyber Essentials held (current users by size-band)



Among surveyed organisations whose Cyber Essentials certification has lapsed, the vast majority (87%) had only ever held the standard level. Among medium and large organisations whose certification lapsed, there is a greater prevalence of Plus having been previously held (the difference between large and micro organisations is significant).

A fifth (20%) of medium sized firms changed to CE Plus at some point before their certification lapsed, suggesting that this may only have been needed it for a certain period of time or that they did not wish to maintain it for another reason (Figure 2). Factors motivating organisations to take up certification or allow it to lapse are explored further in Chapter 3.

Figure 2 Level of Cyber Essentials previously held (by size-band)

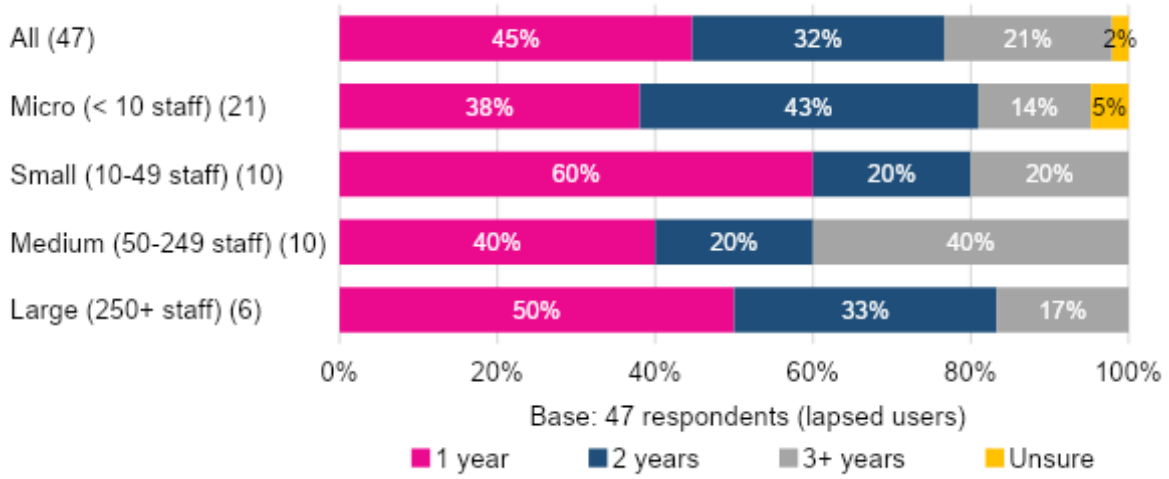


Length of time certification held

The small sample of lapsed users report having held their certification for varying lengths of time, with drop-offs highest after one year (45%) then 32% after two years and 21% after three or more years (Figure 3).

The pattern is similar across the size-bands. Whilst an above average 40% of surveyed medium sized organisations reported having held their certification for three or more years before it lapsed, this is not statistically significant given the low base numbers involved.

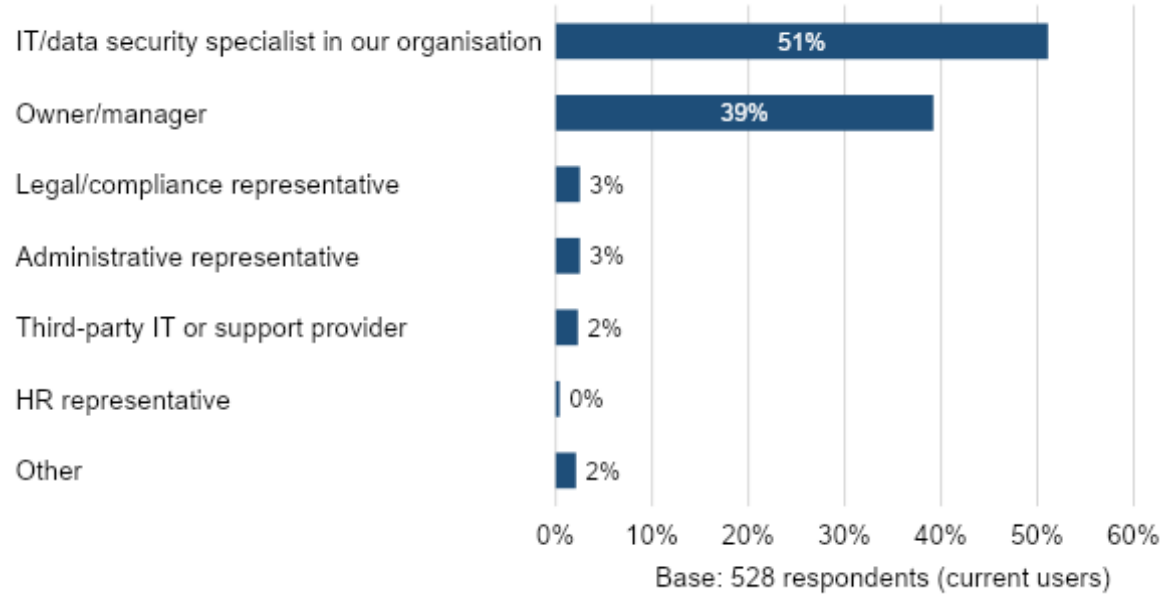
Figure 3 Total time Cyber Essentials certification previously held (by size-band)



2.2 Responsibility for certification

Among organisations that currently hold Cyber Essentials, the vast majority (90%) assign overall responsibility for certification to either the owner or manager, or to the IT or information security specialist within their organisation (Figure 4). This could mean that these organisations are either confident in meeting the scheme's requirements without the need for external consultancy support or would like help if they had access to it.

Figure 4 Assignment of Cyber Essentials overall certification responsibilities



Reported job roles classified as 'Other' include: associate; compliance; director (operations); director (industry solutions); project manager; service delivery manager; technical director.

Analysis by size-band reveals that, among micro businesses, overall responsibility for certification is far more commonly handled by the owner or manager – a significant

difference compared with small, medium and large organisations. This is probably due to having less dedicated in-house IT support.

The larger the size-band of the organisation, the more common it is to place overall responsibility for Cyber Essentials certification in the hands of a dedicated in-house IT or data security specialist. For example, this occurs in 84% of large businesses compared with 17% of micro businesses compared – a significant difference (Table 1).

Table 1 Assignment of Cyber Essentials overall certification responsibilities (by size-band)

Business function	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base	**528**	**158**	**149**	**123**	**98**
IT/data security specialist in our organisation	**51%**	17%	48%	74%	84%
Owner/manager	**39%**	76%	36%	19%	11%
Legal/compliance representative	**3%**	1%	4%	2%	3%
Administrative representative	**3%**	4%	4%	-	-
Third-party IT or support provider	**2%**	2%	3%	2%	1%
HR representative	**0%**	-	1%	1%	-
Other	**2%**	1%	5%	2%	1%

2.3 Consideration and take-up of other schemes and standards

Several strategic stakeholders[5] interviewed for the research described Cyber Essentials as "lighter touch" than other schemes and standards relating to cyber security, such as ISO 27001 and NIST. The implicit message here is that the Cyber Essentials scheme's intention of offering protection against common threats compares negatively against other schemes that are reportedly "offering stronger security". This has implications for the Cyber Essentials scheme in terms of ensuring its intended position in the market is clear to prospective users, including what it does and does not do.

One stakeholder was complimentary about the scheme but added that you "get what you pay for", arguing that larger organisations would typically only benefit from Cyber Essentials to meet an external requirement, especially if they already had stronger standards in place.

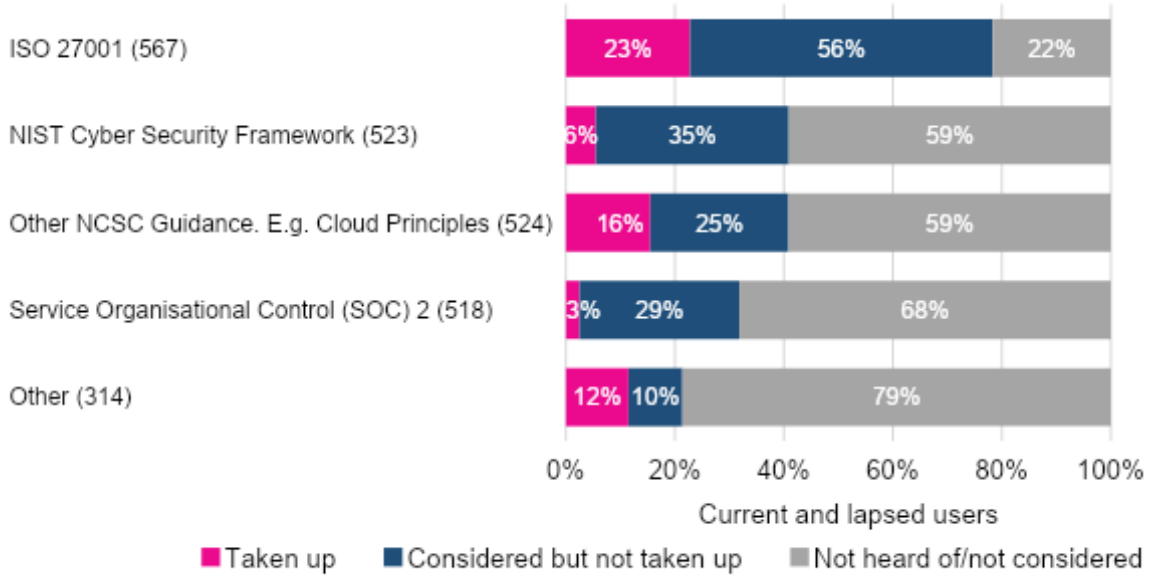
Current and lapsed Cyber Essentials users were asked which, from a list of other specific cyber security schemes, standards and principles, they had also considered or taken up. The proportions taking up or considering taking up the ISO 27001 standard on Information Security and Management are significantly higher than for the other listed schemes, standards and principles. Indeed, the majority had not heard of or considered each of the others (Figure 5).

The data suggests that Cyber Essentials could be providing a solution to a market that might not otherwise have considered another option. In cases where organisations hold more than one solution, e.g. Cyber Essentials in tandem with ISO 27001, this could mean that Cyber

[5] Strategic stakeholders interviewed for the research include those that have had close involvement with Cyber Essentials, including representatives from government and industry (UK, including devolved nations) as well as IASME, NCSC and a sample of former Accreditation Bodies.

Essentials is complementary to other products. Conversely – and especially where Cyber Essentials is mandated in government contracts, as discussed in the next section – it could mean that some organisations feel no choice but to adopt both.

Figure 5 Consideration and take-up of other schemes and standards



The most common schemes and standards classified as 'Other' included: ISO 9001 (6 responses) IASME Cyber Assurance, also referred to by some respondents as IASME Governance (7 responses), CIS Critical Controls (5 responses), PCI-DSS (4 responses), ISO 27701 (2 responses) and NHS Digital Toolkit (2 responses).

Looking across the size-bands, the proportion of surveyed micro organisations that have taken up ISO 27001 is significantly lower than other size-bands, while the proportion of large organisations that have taken up NIST, NCSC Guidance and SOC 2 is significantly higher than some or all of the other size-bands in (Table 2). This suggests that comparatively larger organisations may be more cyber aware and more discerning in finding a solution that works for their organisation and operating context.

Table 2 Consideration of other schemes and standards (by size-band)

Scheme or standard	Decision	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
ISO 27001	Taken up	**23%**	10%	25%	36%	26%
	Considered but not taken up	**56%**	56%	50%	50%	70%
	Not heard of/not considered	**22%**	35%	25%	14%	4%
NIST Cyber Security Framework	Taken up	**6%**	5%	2%	4%	14%
	Considered but not taken up	**35%**	26%	29%	46%	51%
	Not heard of/not considered	**59%**	69%	69%	50%	35%
Other NCSC Guidance. E.g. Cloud Principles	Taken up	**16%**	13%	9%	19%	27%
	Considered but not taken up	**25%**	17%	27%	27%	36%
	Not heard of/not considered	**59%**	70%	64%	55%	37%

Service Organisational Control (SOC) 2	Taken up	**3%**	1%	-	3%	9%
	Considered but not taken up	**29%**	23%	27%	34%	40%
	Not heard of/not considered	**68%**	76%	73%	64%	51%

In comparing responses to the same question between current and lapsed Cyber Essentials users, the most notable difference between the two groups is that more than double the proportion of current users (24%) to lapsed users (11%) report having taken up ISO 27001 – a significant difference (Table 3).[6] However, it should be noted when looking at these results that there is no evidence that lapsed users are any more or less likely to have taken up other schemes or standards.

With the exception of ISO 27001, the majority within both groups had not heard of any of the other specified schemes, standards and principles before completing the survey. With respect to organisations that no longer hold Cyber Essentials, this could mean, for example, an increased exposure to cyber threats, or that they might have implemented the controls once and no longer feel that certification is necessary. The government, NCSC and IASME could potentially do more to help current users understand why a certain baseline level of cyber security is important.

Table 3 Consideration of other schemes and standards (by current and lapsed users)

Scheme or standard	Decision	All	Current Cyber Essentials users	Lapsed Cyber Essentials users
ISO 27001	Taken up	**23%**	24%	11%
	Considered but not taken up	**56%**	56%	57%
	Not heard of/not considered	**22%**	21%	33%
NIST Cyber Security Framework	Taken up	**6%**	6%	5%
	Considered but not taken up	**35%**	36%	32%
	Not heard of/not considered	**59%**	59%	64%
Other NCSC Guidance. E.g. Cloud Principles	Taken up	**16%**	15%	21%
	Considered but not taken up	**25%**	26%	21%
	Not heard of/not considered	**59%**	59%	59%
Service Organisational Control (SOC) 2	Taken up	**3%**	2%	5%
	Considered but not taken up	**29%**	30%	27%
	Not heard of/not considered	**68%**	68%	68%

Views on how Cyber Essentials compares with other schemes or standards

Cyber Essentials is broadly regarded by users as a basic and accessible security standard compared to others. For example, many smaller organisations recognise that Cyber Essentials is cost-effective and sufficiently easy to obtain when balanced alongside the scale of their operations.

[6] It should be kept in mind that the base number of lapsed users is substantially lower at 47 respondents, so these findings should be treated with extra caution.

“Unlike ISO 27001, [Cyber Essentials] sets an actual security standard (pass or fail) which is important. It is achievable for most organisations if they have the will and it’s not too expensive.”

Current user of Cyber Essentials, small employer, private business

“[We were] pressured to become ISO 27001 [certified] but realised this was excessive. CE Plus was agreed as an acceptable alternative.”

Current user of Cyber Essentials, small employer, registered charity/trust

Opinion is more divided among large organisations. Some believe that Cyber Essentials provides a benchmark standard that companies ought to naturally strive for, even if considering other security schemes or standards such as ISO 27001. Others reflected on the differences between Cyber Essentials and alternative schemes, indicating that they each have their own place in the market.

“Cyber Essentials helps set expectations for obtaining other certifications. Some of its policies and procedures are relevant in other schemes.”

Current user of Cyber Essentials, large employer, private business

“Cyber Essentials is a well put together, functional and meaningful set of controls and helps our business develop, maintain and improve our cyber security posture.”

Current user of Cyber Essentials, large employer, private business

“[It’s] different horses for different courses: ISO 27001 is risk based, externally audited, deeply embedded into [business as usual] management systems, governing all internet security related activity on a daily basis. Cyber Essentials is a point in time, pass or fail assessment based on NCSC norms.

Current user of Cyber Essentials, large employer, private business

Where an organisation deems that it needs an alternative (for example ISO 27001) this raises the question that it could be placing an additional burden upon these organisations if they are also required to adopt Cyber Essentials as part of a procurement requirement.

Chapter 2 Summary Box

Among surveyed current and lapsed users, the standard CE certification is the most commonly held. CE Plus is more prevalent among large organisations, for which it accounts for just over half (51%) of certifications, compared to just 17% among micro organisations.

The small sample of lapsed users had held their certification for varying lengths of time, with drop-offs highest after the first year (45%) then 32% after two years and 21% after three or more years.

Among micro organisations, overall responsibility for certification is most commonly handled by the owner or manager. The larger the size-band of the organisation, the more common it

is to place overall responsibility for Cyber Essentials certification in the hands of a dedicated in-house IT or data security specialist.

With the exception of the ISO 27001 standard on Information Security and Management, which more than half (56%) of Cyber Essentials users had considered and a further 23% taken up, most had not heard of or considered other specific schemes and standards asked about in the survey.

Some organisations believe that Cyber Essentials provides a benchmark standard that companies ought to naturally strive for, even if considering other security schemes or standards such as ISO 27001. Others reflected on the differences between Cyber Essentials and other schemes, indicating that they each have their own place in the market.

Qualitative insights reveal that Cyber Essentials is broadly regarded by users as a basic and accessible security standard compared to other schemes or standards. However, large organisations in particular expressed the view that ISO 27001 is more rigorous and appropriate to their setting.

3. Factors Driving Cyber Essentials Certification

3.1 Motivations for taking up Cyber Essentials

Strategic stakeholders (representatives from government and industry) interviewed for the research view the main motivations for organisations becoming Cyber Essentials certified as:

- Being a commercial requirement (where mandated by government contracts)
- Cyber Essentials being considered a simpler, more straightforward and cheaper solution than ISO 27001 and the NIST Cyber Security Framework
- To help grow their business
- To make a big difference to their cyber resilience (for smaller organisations)

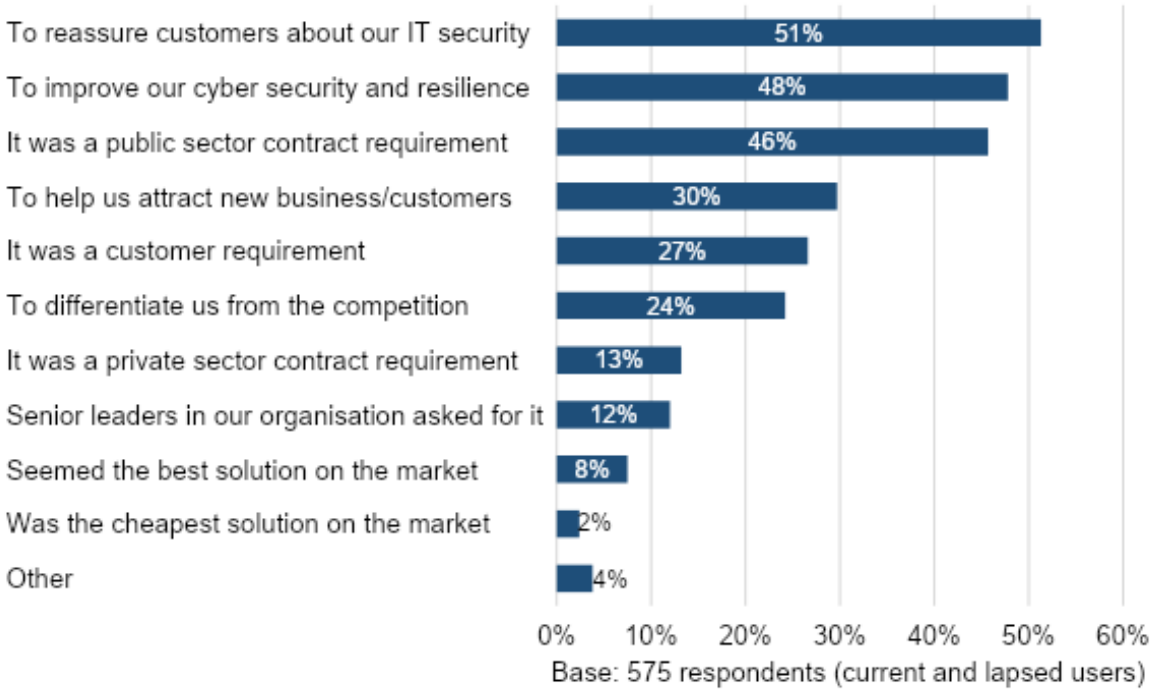
One stakeholder observed that the reputational benefit associated with having the Cyber Essentials badge on their website does not appear to be as prominent now as it was a few years ago. This could be due to Cyber Essentials take-up gaining ground, becoming more established in the market and increasingly being seen as a must-have – especially for those working on government contracts.

Reasons for first becoming Cyber Essentials certified

A range of factors are behind why surveyed organisations chose to become Cyber Essentials certified. Some of these react to the needs of other organisations, while others serve to benefit the organisation becoming certified proactively.

The three most popular responses are: to reassure customers about IT security (51%), to improve cyber security and resilience (48%) and to meet public sector contract requirements (46%). (Figure 6).

Figure 6 Reasons for first becoming Cyber Essentials-certified



The most common responses classified as 'Other' include: to meet insurance requirements, being part of a pilot programme and as a speculative or learning opportunity to see what Cyber Essentials was like.

Analysis by size-band reveals that the proportion of small, medium and large organisations motivated to take up Cyber Essentials to improve their own cyber security and resilience is significantly higher than among micro businesses (Table 4). Once again, this suggests that more could be done to help the smallest organisations understand why they should be more cyber secure, including how Cyber Essentials goes beyond off-the-shelf anti-virus software, and the risks and consequences of not having a suitable baseline level of security in place.

Table 4 Reasons for first becoming Cyber Essentials-certified (by size-band)

	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base	**575**	**179**	**159**	**133**	**104**
To reassure customers about our IT security	**51%**	42%	57%	59%	48%
To improve our cyber security and resilience	**48%**	34%	60%	50%	52%
It was a public sector contract requirement	**46%**	48%	42%	46%	49%
To help us attract new business/customers	**30%**	27%	37%	26%	28%
It was a customer requirement	**27%**	22%	31%	26%	28%
To differentiate us from the competition	**24%**	24%	30%	23%	16%
It was a private sector contract requirement	**13%**	11%	11%	15%	19%
Senior leaders in our organisation asked for it	**12%**	6%	15%	13%	18%
Seemed the best solution on the market	**8%**	5%	12%	8%	6%
Was the cheapest solution on the market	**2%**	5%	1%	2%	1%
Other	**4%**	2%	3%	8%	4%

“Cyber Essentials and Plus help to ‘open doors’ to opportunities for partnerships and research engagement.”

Current user of Cyber Essentials, large employer, academic institution

“[It’s important] to show that despite being a small business we are capable of [performing] as well as any larger business.”

Current user of Cyber Essentials, micro employer, private business

Further analysis on this question by type of organisation reveals that surveyed private sector businesses were comparatively less inclined to pursue Cyber Essentials to improve their own cyber security and resilience than other organisation types. Some 44% of private businesses selected this option compared to more than three quarters of registered charities and trusts, non-governmental organisations, and national or local government.

Two thirds of academic institutions (66%) said they were motivated to take up Cyber Essentials because it was a requirement of a public sector contract – the highest percentage across all organisation types and compared to 46% on average.

The vast majority of registered charities and trusts regard Cyber Essentials positively, irrespective of size.

“It's an achievable and recognised framework, at a reasonable cost.”

Current user of Cyber Essentials, medium employer, registered charity/trust

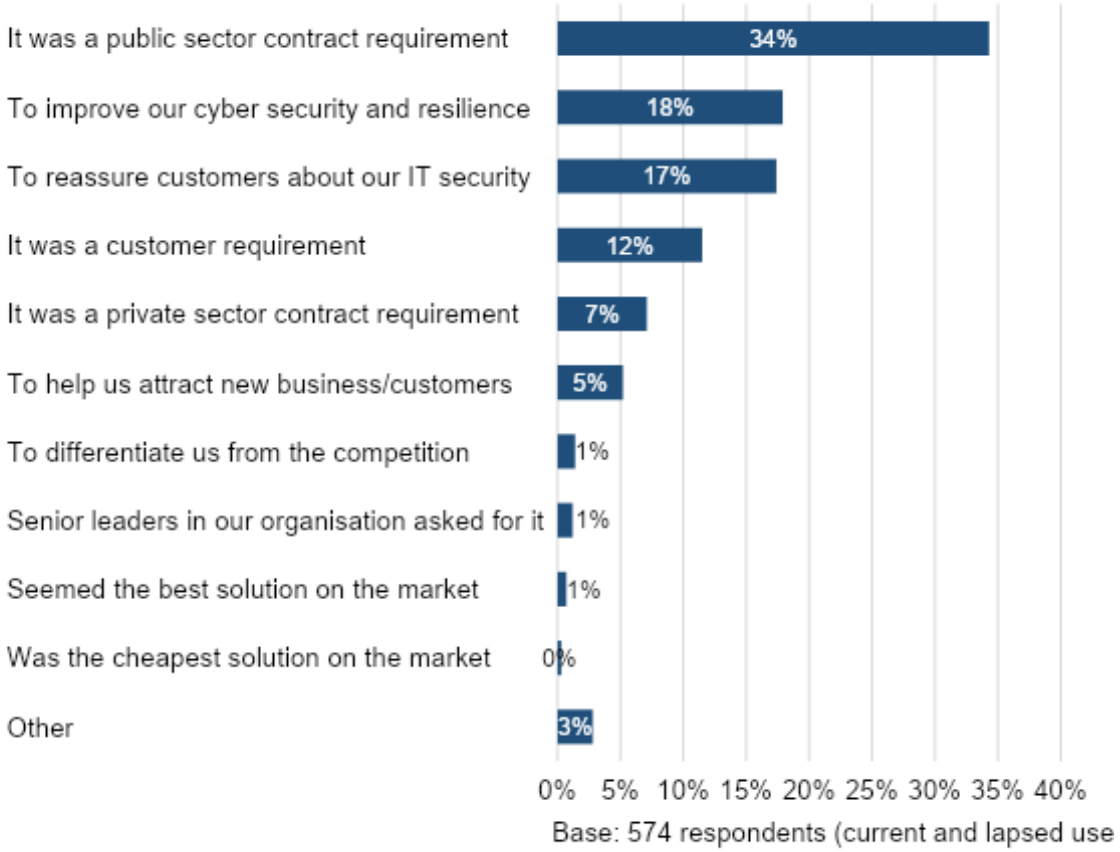
“I like Cyber Essentials due to its NCSC connections which I think give it more weight as a scheme.”

Current user of Cyber Essentials, medium employer, registered charity/trust

Single main reason for first becoming Cyber Essentials certified

All surveyed organisations were asked to narrow their choice of motivating factors down to one main reason for first becoming Cyber Essentials certified. Again, a range of reasons were given, although the most common (mentioned by just over a third, 34%) is that Cyber Essentials was a requirement of a public sector contract (Figure 7).

Figure 7 Single main reason for first becoming Cyber Essentials-certified



Looking across the size-bands, the most common reason for taking up Cyber Essentials in all cases is that it was a public sector contract requirement (Table 5). Larger organisations seem more likely to seek certification due to an internal motivation to improve their cyber security, whereas smaller organisations appear more focused on the benefit of reassuring customers. Indeed, the proportion of large, medium and small organisations motivated to take up Cyber Essentials to improve their own cyber security and resilience is significantly higher than among micro businesses.

Table 5 Single main reason for first becoming Cyber Essentials-certified (by size-band)

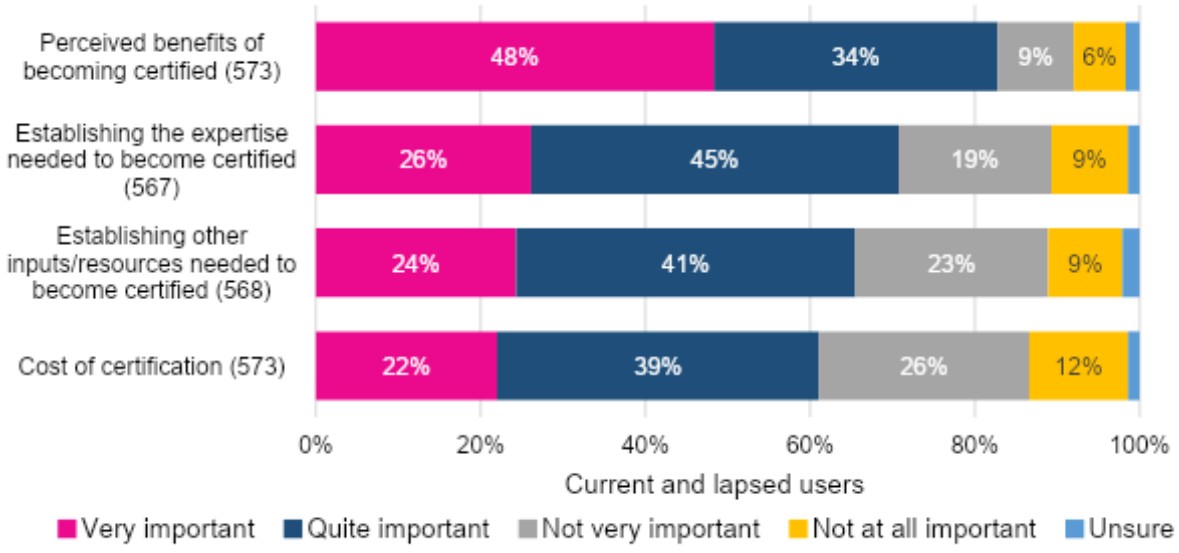
	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base	**574**	**179**	**159**	**132**	**104**
It was a public sector contract requirement	**34%**	40%	30%	33%	35%
To improve our cyber security and resilience	**18%**	10%	20%	19%	28%
To reassure customers about our IT security	**17%**	20%	20%	18%	9%
It was a customer requirement	**12%**	12%	9%	11%	14%
It was a private sector contract requirement	**7%**	6%	7%	9%	8%
To help us attract new business/customers	**5%**	8%	7%	2%	3%
Other	**3%**	2%	1%	7%	2%
To differentiate us from the competition	**1%**	2%	3%	-	-
Senior leaders in our organisation asked for it	**1%**	1%	1%	2%	2%
Seemed the best solution on the market	**1%**	-	2%	1%	-
Was the cheapest solution on the market	**0%**	1%	-	-	-

Importance of specific factors in becoming Cyber Essentials certified

Current and lapsed users were asked how important each of four particular factors were as part of their decision-making process to take up Cyber Essentials (Figure 8).

The majority considered all four factors to be very or quite important, especially understanding the 'perceived benefits of becoming Cyber Essentials certified'. Logistical inputs in terms of expertise, resources and cost are all clearly important, making it essential that organisations are clear from information and guidance what is expected of them as part of the certification process (Figure 8).

Figure 8 Importance of specific factors in decision-making process to take up Cyber Essentials



Analysis by size-band reveals that the majority of organisations per band consider each of these factors to be very or quite important (Table 6).

However, there are significant differences by size-band on the matter of cost, with smaller organisations appearing to be much more cost sensitive. For example, the proportion of micro organisations viewing cost as very important (32%) is significantly higher than small, medium and large organisations. Furthermore, the proportion of large organisations describing cost as not very or not at all important (57%) is significantly higher than the other size-bands.

Table 6 Importance of specific factors in decision-making to take up Cyber Essentials (by size-band)

Factor	Rating	All	Micro (< 10 staff)	Small (10-49)	Medium (50-249)	Large (250+)
Perceived benefits of becoming Cyber Essentials certified	Very important	**48%**	44%	54%	49%	48%
	Quite important	**34%**	34%	30%	37%	39%
	Not very important	**9%**	8%	11%	11%	8%
	Not at all important	**6%**	12%	4%	2%	4%
	Unsure	**2%**	2%	1%	2%	2%
Establishing the expertise needed to become Cyber Essentials certified	Very important	**26%**	26%	30%	24%	22%
	Quite important	**45%**	41%	43%	51%	45%
	Not very important	**19%**	17%	15%	19%	26%
	Not at all important	**9%**	14%	11%	5%	5%
	Unsure	**1%**	2%	1%	1%	2%
Establishing other inputs/resources needed to become Cyber Essentials certified	Very important	**24%**	23%	26%	20%	31%
	Quite important	**41%**	37%	47%	44%	37%
	Not very important	**23%**	23%	20%	29%	23%
	Not at all important	**9%**	14%	7%	5%	8%
	Unsure	**2%**	3%	1%	2%	2%
Cost of certification	Very important	**22%**	32%	21%	19%	11%
	Quite important	**39%**	35%	47%	43%	31%
	Not very important	**26%**	22%	22%	26%	37%
	Not at all important	**12%**	10%	9%	12%	20%
	Unsure	**1%**	2%	2%	-	2%

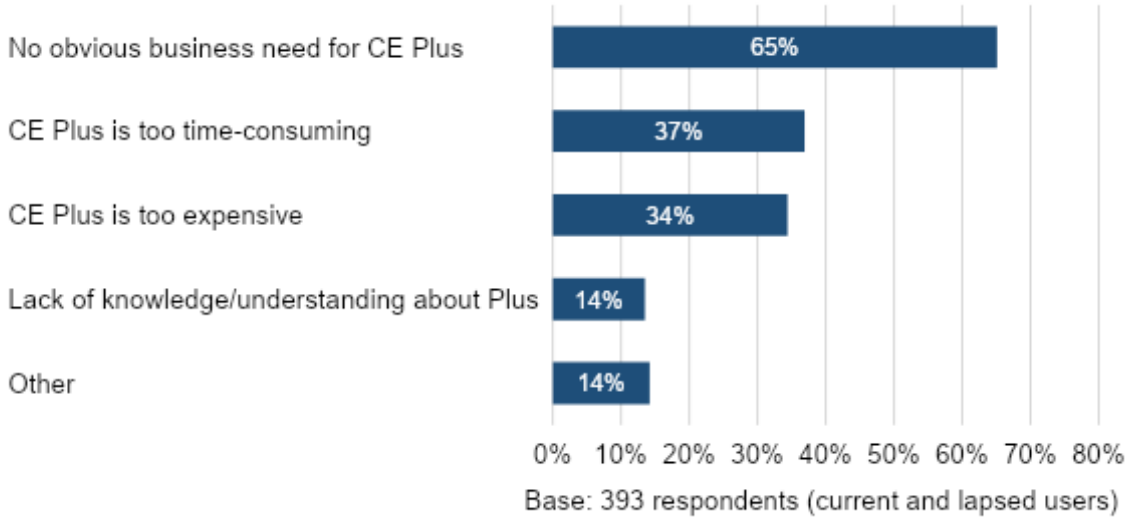
When asked what other factors (if any) played a part in their decision to take up Cyber Essentials, the majority of current and lapsed clients took the opportunity to re-emphasise the importance of meeting contractual, funding or tender requirements. Linked to this, many reiterated the point that Cyber Essentials is often a requirement for public sector work and is often listed as desirable, if not mandatory, for other types of work.

Additional factors important for organisations in deciding whether to take up Cyber Essentials include demonstrating good business practices and standards, and remaining competitive and improving security in a cost-effective way, including with low entry and maintenance requirements.

3.2 Rationale for the choice of certification level

The most prominent reason for surveyed current and lapsed users opting for CE as opposed to CE Plus was no obvious need for CE Plus (65% of respondents) followed by CE Plus being perceived as too time-consuming (37%) and too expensive (35%) (Figure 9).

Figure 9 Reasons for preferring CE over CE Plus



Responses categorised as 'Other' include: perceived challenges and difficulties around passing the audit; wanting to take Cyber Essentials one step at a time and not being ready yet for Plus (but often with the ambition to raise the level); Plus not being required by users or contractors; and not wanting to share data with a third party.

Analysis by size-band (Table 7) reveals broadly similar proportions. Almost three quarters (74%) of micro organisations said that they had no obvious business need for Plus – significantly higher than each of the other size-bands. Medium and large organisations appear more likely to find CE Plus too time-consuming than micro and small organisations, which potentially ties in with the additional resource needed to implement it (section 5.1) although this finding is not statistically significant.

Table 7 Reasons for preferring CE over CE Plus (by size-band)

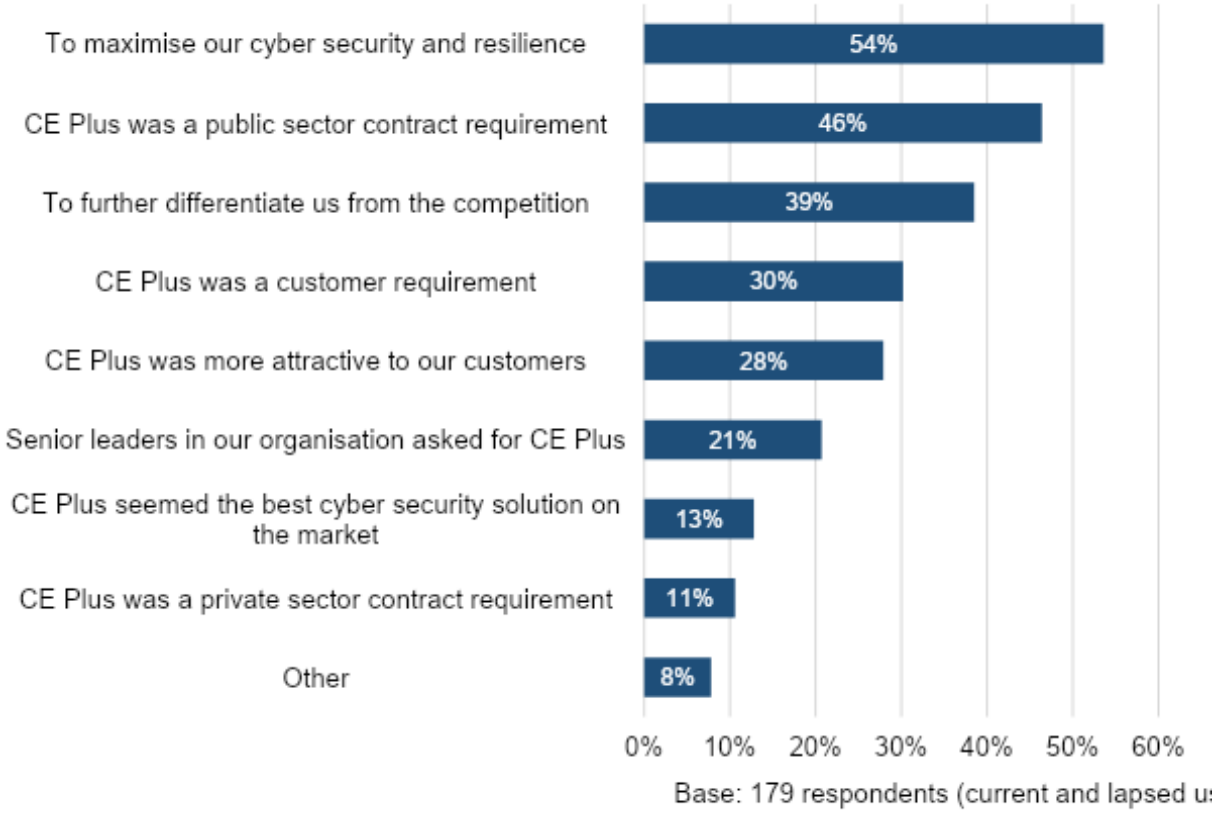
	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base	**393**	**151**	**104**	**86**	**52**
No obvious business need for Plus	**65%**	74%	64%	64%	44%
Plus is too time-consuming	**37%**	34%	32%	43%	44%
Plus is too expensive	**34%**	38%	32%	34%	29%
Lack of knowledge/understanding about Plus	**14%**	15%	16%	11%	10%
Other	**14%**	7%	16%	11%	39%

Large organisations were also more inclined to choose ‘other’, with reasons as follows from most to least mentioned:

- CE Plus is in progress or a next planned step
- Not yet ready or confident at being able to meet the technical controls
- Progressing to CE Plus proved more difficult to prioritise during the height of the COVID-19 pandemic
- CE Plus is not currently required for contracts being worked on
- Looking for a more comprehensive hands-on audit, involving running of audit tools as opposed to providing evidence of implementation
- Not sure that the extra time, resources and cost for CE Plus represents good value for money year on year
- Concerns around sharing information with a third party (i.e. Certification Body);

Current and lapsed users opting for CE Plus chose this level for a variety of reasons, with the most common being to maximise cyber security and resilience (54%), followed by CE Plus being a requirement of a public sector contract (46%) and to differentiate their organisation from the competition (39%) (Figure 10). Once again this shows that a range of reactive and proactive drivers are at play.

Figure 10 Reasons for preferring CE Plus



Responses categorised as 'Other' include: wanting independent assurance (including the 'weight' that brings), wanting to lead by example, an effective way to measure cyber security without incurring too much expense, to prepare for the Network and Information Systems Regulations, to be able to audit other companies and to become a Certification Body.

Analysis by size-band reveals similar proportions, with no significant differences in the results (Table 8).

Table 8 Reasons for preferring CE Plus (by size-band)

	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base	**179**	**28**	**54**	**46**	**51**
To maximise our cyber security and resilience	**54%**	46%	52%	63%	51%
It was a public sector contract requirement	**46%**	43%	41%	46%	55%
To further differentiate us from the competition	**39%**	43%	43%	35%	35%
CE Plus was a customer requirement	**30%**	36%	26%	26%	35%
CE Plus was more attractive to our customers	**28%**	36%	24%	33%	24%
Senior leaders in our organisation asked for Plus	**21%**	11%	24%	24%	20%
CE Plus seemed the best cyber security solution on the market	**13%**	7%	11%	20%	12%
It was a private sector contract requirement	**11%**	7%	9%	13%	12%
Other	**8%**	7%	6%	15%	4%

3.3 Reasons for certification lapsing

Strategic stakeholders interviewed for the research believe that Cyber Essentials users can allow their certification to lapse for several possible reasons – typically that they:

- No longer need it for a contract
- Do not wish to invest the cost and time needed to go through recertification
- Do not fully understand and appreciate the security impact that Cyber Essentials has
- Have another mechanism already in place such as ISO 27001 or NIST.

Organisations with lapsed Cyber Essentials certifications were subsequently asked for the reasons why that happened (Figure 11). The top three reasons, each mentioned by a minority of respondents, are as follows:

- Too difficult to keep up with changing controls (28%)
- Too expensive (23%)
- Too time-consuming (19%)

Figure 11 Reasons why Cyber Essentials certification lapsed

Just under a third (32%) of lapsed organisations gave other responses. These are listed below – each mentioned by one respondent unless otherwise stated:

- Too busy to allocate resources to renewal (three respondents)
- In the process of upgrading the server to avoid a fail and plan to renew Cyber Essentials again in the future (two respondents)
- New scope of Cyber Essentials required too great a resource injection to gather relevant information (two respondents)

- As a software company, tools and systems are determined by what users use, so it was a choice between Cyber Essentials or something else
- Other schemes and standards perceived to have greater credibility
- In the process of changing Certification Body
- Cyber Essentials did not lead to business generation
- COVID-19 pandemic led to recertification no longer being a priority
- Cyber Essentials scheme too restrictive and 'tick box' oriented rather than being based on an understanding of an organisation's security profile
- Waste of time as it seems like you are always going to pass

Despite the low base number to this question about why certification lapsed, additional analysis has been undertaken based on the length of time Cyber Essentials certification was previously held (in years).

Among those that had held certification for three or more years prior to it lapsing (just 10 respondents), four said it was too difficult to keep up with the changing requirements and controls (explored further in section 5.5) and three said they did not pass the annual recertification process. There is insufficient data to analyse the reason why Cyber Essentials certification lapsed by comparing organisations that previously only ever held the standard level and those that previously attained Plus level.

Further probing reveals that, among large organisations whose certification lapsed, a common factor was not being able to keep up with changing controls. Among small and micro organisations, a common factor was the perception of the process being too expensive and time-consuming. These issues are unpicked further in sections 5.4 and 5.5.

It should be noted that a major update to the scheme took place in January 2022 which was still potentially being felt by respondents at the time of the survey. In addition, the announcement of the 2023 update coincided with the time of the survey (and with a live date of April 2023) which may also have influenced responses in terms of the perceived burden of change.

"More information was required, much more detailed than in the previous year, which made it very difficult to complete the recertification process."

Lapsed user of Cyber Essentials, medium employer, private business

Despite the perception mentioned elsewhere that Cyber Essentials offers an affordable security baseline suitable for smaller businesses, some micro and small organisations whose certification lapsed emphasised their dissatisfaction with the cost and resources required to maintain and renew Cyber Essentials, which they regard as a barrier to business. Whilst the cost of assessment appears to form just one part of the costs involved for many organisations in becoming Cyber Essentials certified (see section 5.1), this suggests a potential need to review the scheme's pricing structure.

“The annual cost of recertification was quoted at a few pounds shy of £2,000 by our existing provider and two others I obtained quotes from. This is simply too expensive for a small business when the actual benefit was not reflected in the profit and loss account.”

Lapsed user of Cyber Essentials, micro employer, private business

Chapter 3 Summary Box

When asked why their organisation first decided to become Cyber Essentials certified, current and lapsed users mentioned a range of factors, including those which are reactive to others’ requirements and perceived needs, and those which are proactively aimed at benefiting their own organisation.

The most common single main reason (mentioned by just over a third, 34%) is that Cyber Essentials is a requirement of a public sector contract. Micro businesses in particular appear to be less strongly motivated by improving their own cyber security and resilience, and more strongly motivated by external influencers such as customer or contractual requirements. This suggests that Cyber Essentials certification is, in some cases, serving as a means to an end – a view also reflected in some of the qualitative feedback.

The majority of respondents (82%) consider it important to understand the perceived benefits of becoming Cyber Essentials, and most also place importance on planning various logistical inputs in terms of expertise, resources and costs. This makes it essential that organisations are clear from various information and guidance what the Cyber Essentials scheme expects of them.

The most prominent reason for current and lapsed users opting for CE as opposed to CE Plus was that they saw no obvious need for CE Plus (65% of respondents). Conversely, most of those opting for CE Plus did so to maximise cyber security and resilience (54%).

The top three reasons for Cyber Essentials certification lapsing, each mentioned by a minority of respondents, are that it was too difficult to keep up with changing controls (28%), too expensive (23%) and too time-consuming (19%). This points to some challenges in a scheme which by its very nature is prescriptive rather than risk-based.

4. Cyber Essentials Information and Guidance

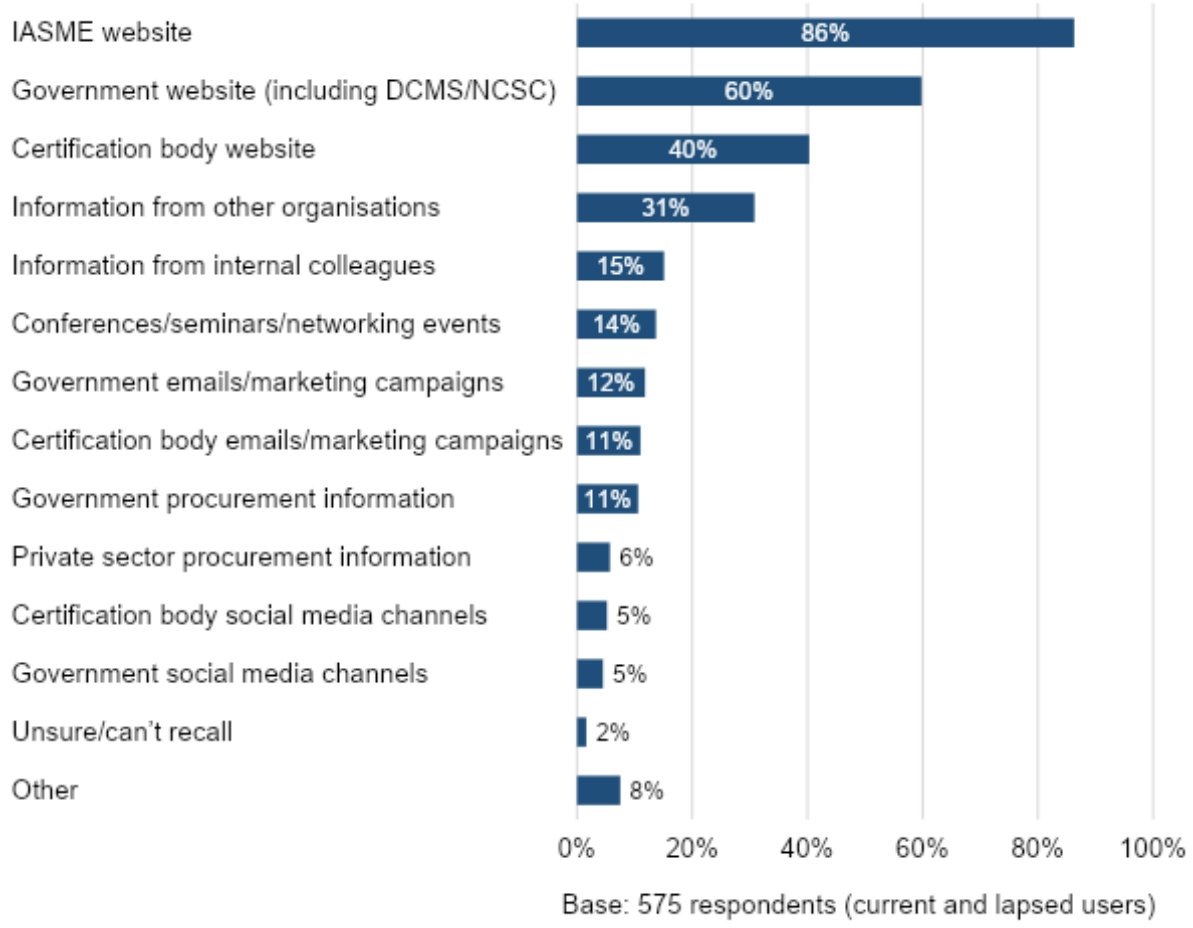
This chapter explores interactions and perceptions relating to Cyber Essentials information and guidance (including sources used), whether organisations sought support (and from where) during the process of becoming Cyber Essentials-certified, and perceptions of the quality of that support. It also sets out suggestions for how Cyber Essentials information and guidance could be improved.

4.1 Sources of information, help and support

Sources of information

Current and lapsed Cyber Essentials users were asked which, from a range of sources of Cyber Essentials information and guidance, they have ever used. The most widely accessed are those from the government and IASME, with the vast majority (86%) using the IASME website, followed by government websites such as DCMS or NCSC (60%) and Certification Body websites (40%). This suggests that organisations are generally accessing information from trusted sources. (Figure 12).

Figure 12 Sources of information and guidance accessed about Cyber Essentials



Responses classified as ‘Other’ include: Jisc, LinkedIn groups, existing knowledge, experience, industry trends, auditor and this survey questionnaire.

Analysis by size-band reveals that a significantly higher proportion of large organisations compared to micro and medium organisations are inclined to draw on government and Certification Body websites, as well as access information via conferences, seminars and networking events (Table 9). Large organisations may therefore be party to wider and deeper discussions about Cyber Essentials.

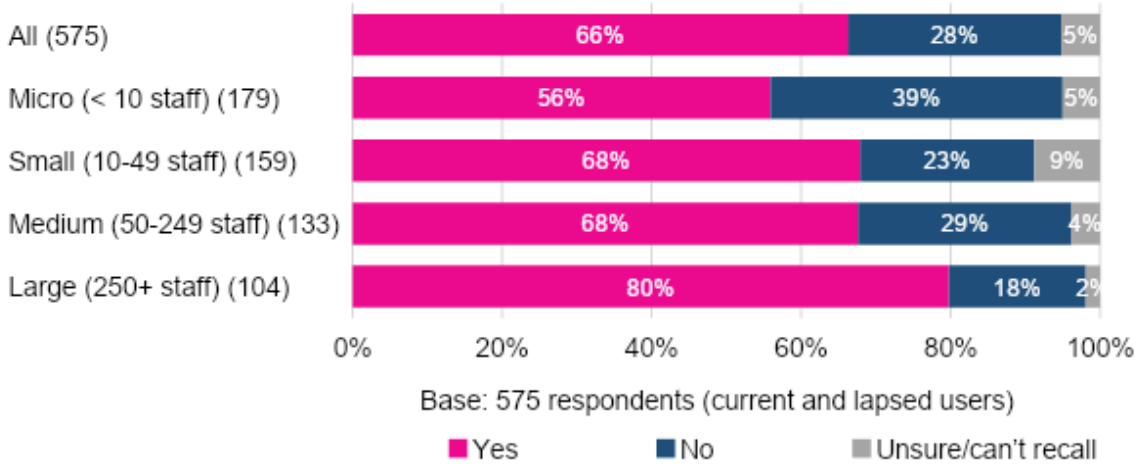
Table 9 Sources of information and guidance accessed about Cyber Essentials (by size-band)

Sources	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base	**575**	**179**	**159**	**133**	**104**
IASME website	**86%**	84%	87%	90%	85%
Government website (inc. DCMS/NCSC)	**60%**	53%	62%	57%	72%
Certification body website	**40%**	34%	41%	39%	53%
Information from other organisations	**31%**	22%	30%	36%	39%
Information from internal colleagues	**15%**	8%	21%	15%	18%
Conferences/seminars/networking events	**14%**	7%	10%	14%	31%
Government emails/marketing campaigns	**12%**	8%	11%	13%	18%
Government procurement information	**11%**	15%	8%	10%	9%
Certification body emails/marketing campaigns	**11%**	8%	11%	10%	18%
Other	**8%**	7%	5%	8%	13%
Private sector procurement information	**6%**	5%	9%	6%	2%
Government social media channels	**5%**	3%	4%	5%	8%
Certification body social media channels	**5%**	4%	6%	8%	4%
Unsure/can’t recall	**2%**	2%	1%	2%	1%

Need for help

Two thirds of current and lapsed clients (66%) reported having a need to ask questions or seek help during the certification process. This indicates the importance of easily accessible and high-quality support being in place. The proportions of small, medium and large organisations reporting that they needed help are significantly higher than micro businesses (Figure 13).

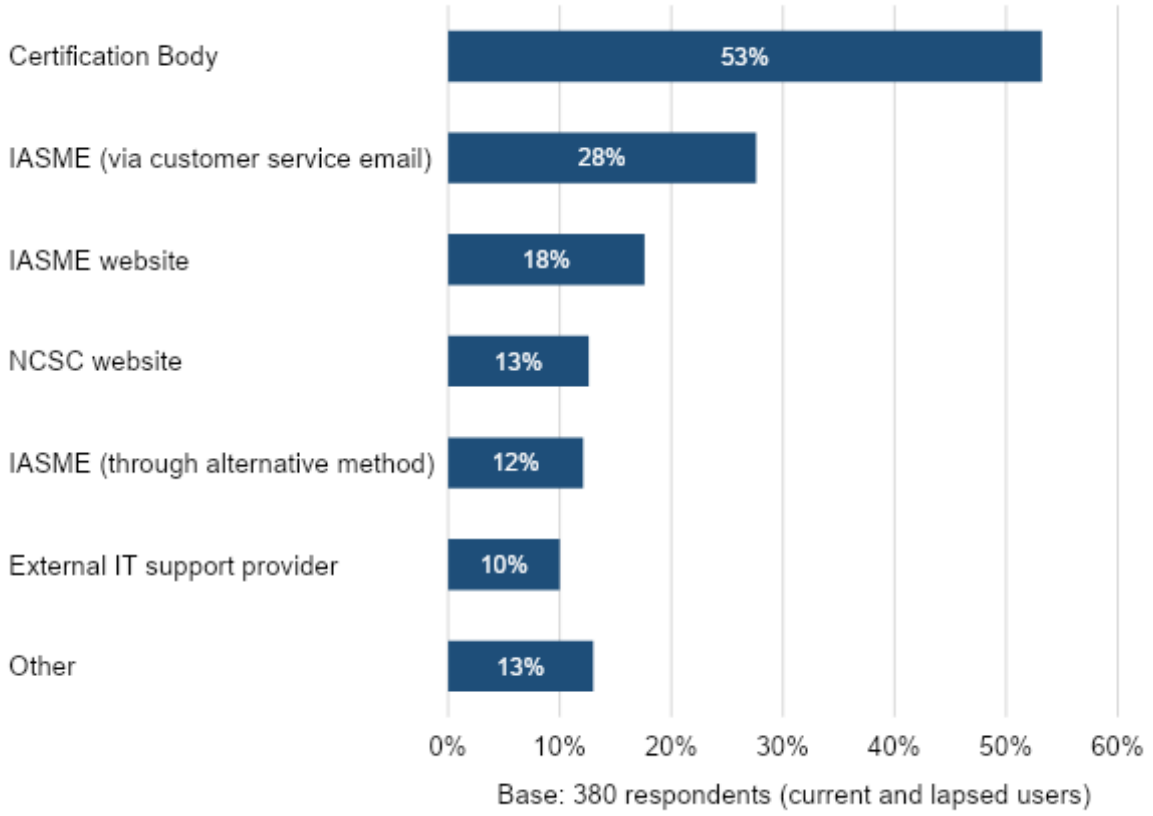
Figure 13 Need for help during the certification process (by size-band)



Sources of support

The most common places turned to for support during the certification process are the Certification Body (53%), followed by IASME either via customer service email (28%) or the IASME website (18%). This makes it important that Certification Bodies are open and willing to provide the assistance needed to help organisations achieve the ultimate end goal of becoming more cyber resilient. (Figure 14).

Figure 14 Sources of support used during the certification process



Responses classified as 'Other' include Google, colleagues (notably internal IT support), forums, professional bodies (two mentioned UCISA), auditors, partners, colleagues, peers and friends.

Looking across the size-bands, large organisations appear more predisposed to seek help from their Certification Body (significantly higher than for micro and medium organisations). It is also noteworthy that almost a fifth of micro organisations (18%) choose to look elsewhere and seek support from a variety of 'other' sources, including those mentioned above (Table 10).

Table 10 Sources of support used during the certification process (by size-band)

Sources	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base	**380**	**100**	**107**	**90**	**83**
Certification Body	**53%**	46%	58%	44%	65%
IASME (via customer service email)	**28%**	29%	28%	31%	22%
IASME website	**18%**	17%	13%	22%	19%
NCSC website	**13%**	11%	8%	16%	18%
IASME (through alternative method)	**12%**	15%	8%	12%	13%
External IT support provider	**10%**	7%	15%	12%	5%
Other	**13%**	18%	11%	12%	11%

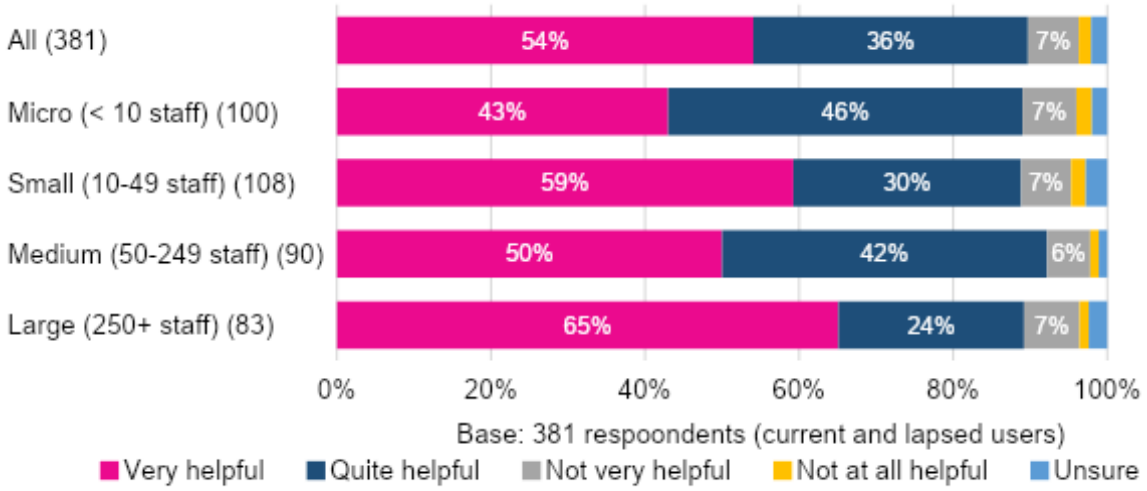
4.2 Perceptions of support received

Helpfulness of support

Support is generally considered helpful, with more than half of respondents (54%) describing it as very helpful and 36% quite helpful. The picture is similar across the size-bands, although the proportion of large organisations viewing support as very helpful is significantly higher than for micro and medium organisations (Figure 15).

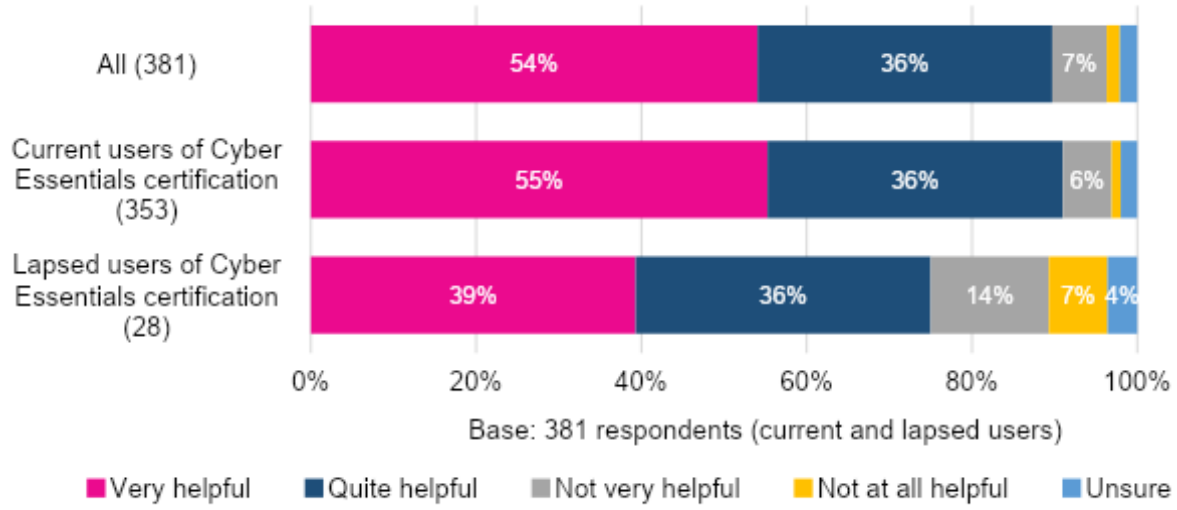
In cases where support is described as anything other than 'very helpful', this suggests a weakness in addressing organisations' specific needs and a possible case for better tailoring – an issue explored further in section 4.3.

Figure 15 Helpfulness of support during the certification process (by size-band)



Further analysis reveals that surveyed lapsed users are less complimentary about the support they received than current users. More than a fifth (21%) of lapsed users describe it as not very or not at all helpful compared to 7% of current users – a significant difference (Figure 16). This may have contributed to organisations' decisions not to pursue their annual renewal.

Figure 16 Helpfulness of support during certification (by current and lapsed users)

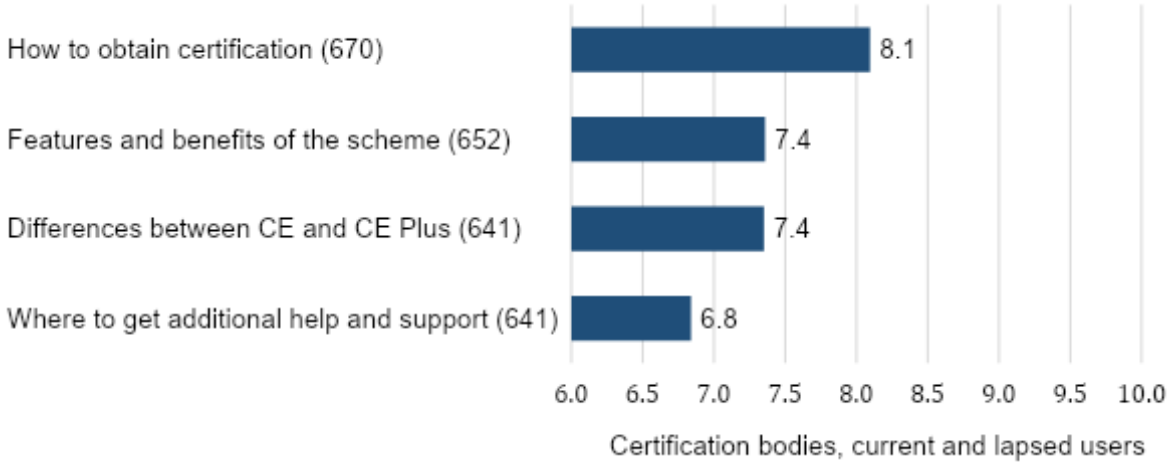


Clarity of online information and guidance

All organisations (including Certification Bodies) were asked to rate on a scale from 1 (not at all clear) to 10 (perfectly clear) how clear they consider a range of specific aspects of online information and guidance about the Cyber Essentials scheme to be.

The full range of ratings (1 to 10) was received and the mean scores for each aspect are moderate. Greatest clarity relates to how to obtain Cyber Essentials certification, averaging 8.1, while there is clarity around where to get additional help and support, averaging 6.8 (Figure 17).

Figure 17 Clarity of information and guidance about Cyber Essentials from 1 to 10



Regarding the clarity of information on where to get additional help and support, the mean ratings among large, medium and small organisations are significantly higher than for micro organisations. This indicates that micro businesses could find it difficult to access additional help to answer their questions or concerns.

With respect to clarity of differences between CE and CE Plus, the mean rating by large organisations is significantly higher than medium, small and micro businesses, suggesting that more could be done to make these differences clearer and more understandable to organisations that lack the same underpinning knowledge as large organisations (Table 11).

Table 11 Clarity of information and guidance from 1 to 10 (by size-band)

Aspects of information and guidance	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
How to obtain certification	**8.1**	7.6	8	8.2	8.6
Differences between CE and CE Plus	**7.3**	6.6	7.2	7.6	8.2
Features and benefits of the scheme	**7.2**	6.7	7.5	7.6	7.3
Where to get additional help and support	**6.7**	5.9	6.9	7	7.4

Base: 652 respondents

At this point, it is worth noting that strategic stakeholders interviewed for the research are generally complimentary about the features and benefits of published information and guidance about the Cyber Essentials scheme, but less so when asked how clear the differences are between CE and CE Plus.

One stakeholder referred to a common misconception that CE Plus provides an enhanced level of security and another said the current information and guidance does not really give organisations all the information they need to make an informed decision about whether the CE or CE Plus scheme is right for them.

Among stakeholders who raised issues about online information and guidance, the main messages are that:

- There is a lot of information which can prove hard to navigate
- The guidance probably works best for organisations that already know what they are looking for but less so for those that do not know where to start
- Published information does not give a sufficient sense of what the controls can really do for an organisation and how many attacks they can prevent.

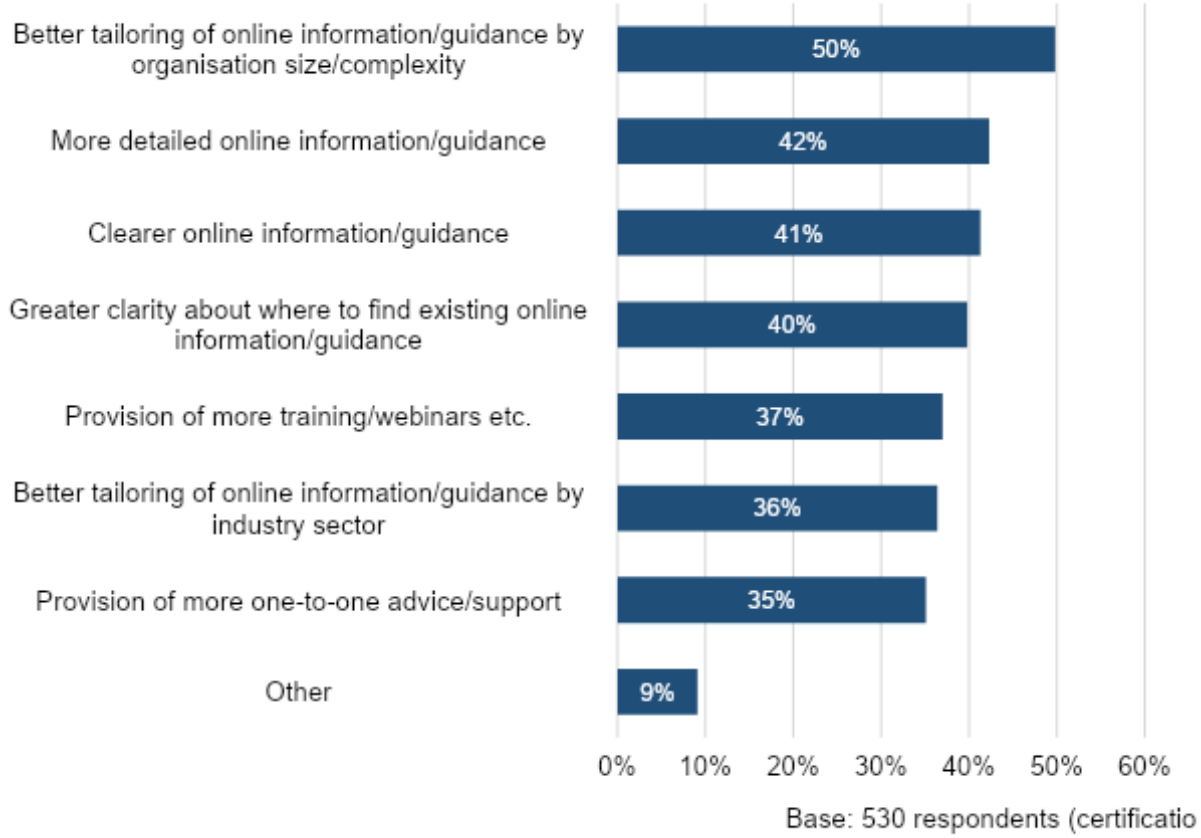
These findings indicate that online information and guidance could be made more readily accessible, useful and intuitive. Suggestions for improving information and guidance are discussed in the next section.

4.3 Improving information and guidance

All surveyed organisations – including Certification Bodies – were asked how Cyber Essentials information and guidance could be improved or made more accessible. Half (50%) would like to see better tailoring of online information and guidance by organisation size or complexity, followed by more detailed guidance (42%) and clearer guidance (41%)

(Figure 18). This corroborates some of the points made in the preceding section regarding perceptions of support already received.

Figure 18 How Cyber Essentials information and guidance could be improved



Responses classified as 'Other' largely elaborated on the existing response options, with some exceptions, including:

- Greater clarity on Bring Your Own Device (BYOD) controls and practical implementation – discussed further in section 5.6
- Vendor and product specific guidance
- Better notification of changes to certification requirements ("so we're not scrambling to introduce new controls")
- More readily understandable step by step guidance to certification
- Less technical jargon
- Making the questions clearer ("currently too many, duplicated, poorly expressed and unnecessarily complex")
- More webinar or video guidance on how to complete the Cyber Essentials assessment questions

- Interactive web chat

Proportions are similar by size-band, although an above average 60% of micro organisations believe that better tailoring of information and guidance is needed – a significant difference (Table 12). Proportions are also very similar between Certification Bodies, current and lapsed users (not displayed).

Table 12 How Cyber Essentials information and guidance could be improved (by size-band)

Improvement mechanisms	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base	**530**	**163**	**147**	**121**	**99**
Greater clarity about where to find existing online information/guidance	**40%**	37%	41%	39%	43%
More detailed online information/guidance	**42%**	40%	41%	46%	44%
Clearer online information/guidance	**41%**	41%	42%	34%	51%
Better tailoring of online information/guidance by industry sector	**36%**	39%	35%	33%	39%
Better tailoring of online information/guidance by organisation size/complexity	**50%**	60%	45%	44%	48%
Provision of more one-to-one advice/support	**35%**	37%	36%	35%	30%
Provision of more training/webinars etc.	**37%**	29%	37%	46%	37%
Other	**9%**	9%	12%	6%	9%

Building on these points, surveyed organisations, including Certification Bodies, were asked to describe in more detail how they think Cyber Essentials information and guidance could be improved or made more accessible. The majority emphasised the need for greater clarity around Cyber Essentials requirements, especially where elements can be too easily open to interpretation.

“The guidance in the questionnaire is vague in places and open to different interpretations.”

Current user of Cyber Essentials, large employer, private business

“I have to stop ‘attempts to evade the rules’ [by users] over and over... and it's always a struggle because it's my word against their interpretation.”

Cyber Essentials Certification Body

Others would like more contextual information and examples relating to the types of cyber security policies that Cyber Essentials outlines.

“There is too much ‘what’ and too little ‘how’. For most small [organisations] the advice needs to say ‘do it like this’ – not ask them lots of questions that they don't understand. A few key points on standard architectures and compliance with those is all that's needed.”

Cyber Essentials Certification Body

Some perceive Cyber Essentials guidance as a ‘one-size-fits-all’ checklist which does not adequately speak to or benefit certain types and sizes of organisation. Many smaller employers contend that current Cyber Essentials guidance does not cater for the limitations of their operation in terms of the technical understanding needed to navigate it. This is further hampered by the perceived lack of feasibility of acquiring additional staff with this technical understanding. Similar issues are raised by academic institutions.

“[Cyber Essentials guidance should provide] worked examples of compliant approaches for different company sizes, for each requirement.”

Current user of Cyber Essentials, micro employer, private business

“Cyber Essentials is challenging for education establishments and it would be better if it could be tailored per application or industry.”

Current user of Cyber Essentials, large employer, academic institution

Additionally, while Certification Bodies share many of the above views, some express the need for campaigns or promotions to raise awareness of the importance of cyber security.

“[Cyber Essentials] is not about answering a few questions and tweaking them to pass the assessment. It's about improving the overall security posture of organisations. This message needs to be sent clearly to organisations that would like to obtain the certification.”

Cyber Essentials Certification Body

Some Certification Bodies are keen to stress that information and guidance should not just encourage users to understand the scheme as a means to an end, but to understand more broadly and fully the importance of cyber security – including the potential consequences of cyber threats more generally. In this way, they feel that organisations would be encouraged to maintain their security standard not just because they have passed a certain assessment or ticked the right boxes but because of their fluency in cyber security.

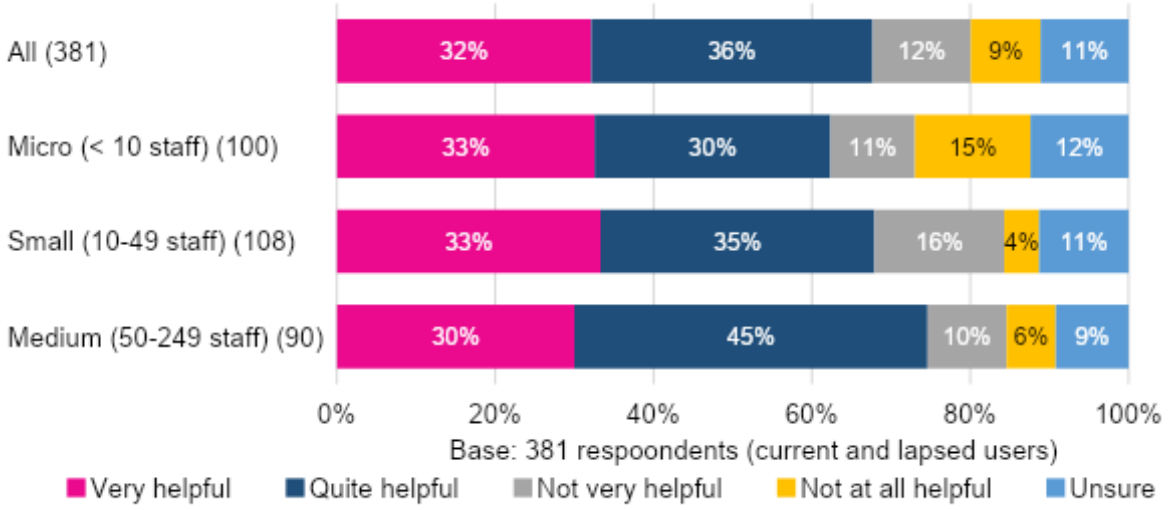
As such, there is a case for Cyber Essentials information and guidance to focus more strongly on how it goes above and beyond off-the-shelf anti-virus software, how it can help organisations, the importance of cyber security in the business world and the potential consequences of not being sufficiently protected.

Cyber Advisor Scheme

Finally, organisations classified as SMEs were asked how helpful they feel the NCSC’s new Cyber Advisor Scheme would be to their organisation. The scheme aims to offer assured cyber security consultancy services to SMEs and help them to achieve a minimum standard of security.

This provides an example of tailoring of support that organisations have said they would recommend increasing. More than two thirds (68%) believe they would find the Cyber Advisor scheme very or quite helpful (Figure 19). The proportion of medium organisations saying very or quite helpful is significantly higher than for micro organisations. This could be due to the former having comparatively more complex needs or the fact that these organisations may be more used to accessing or buying third party support and consultancy more frequently.

Figure 19 Likely helpfulness of the Cyber Advisor scheme (by size-band)



Chapter 4 Summary Box

The most widely accessed information and guidance sources about Cyber Essentials include the IASME website, followed by NCSC, DCMS and Certification Body websites. This suggests that organisations are generally accessing information from trusted sources. Large organisations are more inclined to draw on a wider range of sources including conferences, seminars and networking events.

Two thirds of current and lapsed users (66%) needed to ask questions or seek help during the certification process. The figure is 80% among large organisations, indicating a need for more bespoke support appropriate to the complexities of their organisation. The most common place to turn to is the Certification Body (53%), making it important that Certification Bodies are open and willing to provide the assistance needed to help organisations achieve the ultimate end goal of becoming more cyber resilient.

Support during the certification process is generally viewed positively, with more than half of respondents (54%) describing it as very helpful and 36% quite helpful. More than a fifth (21%) of lapsed users describe support as not very or not at all helpful – three times higher than the proportion of current users – which may have contributed to these organisations' decisions not to renew.

Some concerns raised by survey respondents are that existing scheme guidance adopts a 'one-size-fits-all' approach which does not adequately speak to or benefit certain types and sizes of organisation. Indeed, half of current and lapsed users (50%) would like to see better

tailoring of online information and guidance by organisation size or complexity, followed by more detailed guidance (42%) and clearer guidance (41%).

The majority also call for greater clarity around Cyber Essentials assessment requirements, especially where elements can be too easily open to interpretation. For their part, several Certification Bodies stressed the need to provide more foundational information to help users understand the importance of cyber security and threats in a more general sense.

5. Cyber Essentials Customer Journey

Understanding the customer journey involves assessing organisations' resource inputs when seeking to obtain Cyber Essentials certification and the relative ease or difficulty of specific aspects of the certification process. Particular attention is paid to the needs of different sizes of organisation, as well as meeting the technical control requirements and how well changes to those control arrangements are communicated.

5.1 Resource inputs

Costs involved

Current and lapsed users were asked for the approximate total cost to their organisation to attain Cyber Essentials accreditation, factoring in the cost of assessment (built into the scheme pricing structure), work needed to qualify, any new equipment needed etc.

The overall mean amount is £4,941 (base of 460 respondents).[7] The mean amounts by size-band, and between current and lapsed users, are set out below.

The figures of small, medium and large organisations are significantly higher than for micro organisations, and the figure for large organisations is significantly higher than each of the other groups.

- Micro (£1,894)
- Small (£4,741)
- Medium (£6,267)
- Large (£31,459)

- Current users (£8,360)
- Lapsed users (£9,419)

The most common (modal) answer is £1,000, mentioned by 48 respondents.

These costs are substantially over and above the cost of the assessment process. When asked to expand on the types of costs involved, surveyed firms commonly mentioned additional staff time and costs involved, notably to meet the technical controls. Quoted figures for the individual elements of the cost of certification and assessment each vary from several hundred to several thousand pounds.

To a lesser extent, organisations referred to money spent on IT consultation and support (again quoted figures vary from several hundred to several thousand pounds), as well as hardware and software upgrades and updating policies. Smaller organisations appear more inclined to consider the costs associated with meeting the technical controls as a substantial outlay in relative terms.

"[Money was spent on the] certification cost and resource time to investigate and document."

[7] An outlier response of £5m stated by a large organisation has been removed from the mean scores.

Current user of Cyber Essentials, small employer, private business

"[Money was spent on] new IT services, staff costs (technical and project management), communication plans and equipment upgrades."

Current user of Cyber Essentials, large employer, academic institution

Full-time equivalent (FTE) days involved

Current and lapsed users were also asked how many FTE days were typically involved in preparing for their organisation's Cyber Essentials certification annual renewal. This was to be left blank if an organisation had not renewed their Cyber Essentials certification at least once.

The overall average is 9 days (base of 479 respondents)[8]. The averages by size-band, and between current and lapsed users, are set out below.

As with cost, the averages for small, medium and large organisations are significantly higher than for micro organisations, and the average for large organisations is significantly higher than each of the other groups.

- Micro (4 days)
- Small (6 days)
- Medium (10 days)
- Large (23 days)

- Current users (9 days)
- Lapsed users (15 days)

Those that spent comparatively fewer FTE days organising Cyber Essentials certification mostly described completing, reviewing and checking answers to the assessment questions. Those who spent comparatively more FTE days mentioned a wider variety of activities, including updating hardware and software, learning new information in relation to changing assessment criteria, as well as audit-related activities.

"[1 day was spent] reviewing the previous certification and preparing a new submission, including finding answers to questions and revising the submission based on feedback."

Current user of Cyber Essentials, micro employer, private business

"[28 days were spent] checking software updates, [operating system] updates, firmware updates, firewall updates, open ports, mobile device and app updates, PIN numbers."

Current user of Cyber Essentials, small employer, private business

The substantially longer time spent by large organisations appears to be mainly due to the scope of operations and the increased time taken to verify necessary controls across a range of departments.

[8] An outlier response of 1,000 days has been removed from the mean scores.

"[90 days were spent on] security to review the requirements and scope the engagement, meeting with stakeholders to discuss the scope and requirements, security to conduct the assessment against the requirements, produce a gap analysis and remediation plan, remediation activity, final assessment, evidence gathering and submission."

Current user of Cyber Essentials, large employer, private business

It is worth noting that the survey did not specifically ask current users about whether the cost and time spent on obtaining certification was deemed too much or too long. While cost and time are not among the main difficulties cited in relation to the customer journey (section 5.4), reducing the costs associated with certification is a common suggestion for improvement (section 6.4). Furthermore, cost and time are both among the top three reasons why lapsed Cyber Essentials users did not renew their certification (Figure 11). For some organisations therefore, these factors are clearly an issue and could pose a risk to take-up and retention.

5.2 Rating of specific aspects of the certification experience

On the whole, most surveyed current and lapsed users have had a positive certification experience, with the majority rating various specific aspects of the customer journey to obtaining Cyber Essentials certification as very or quite good (Figure 20).

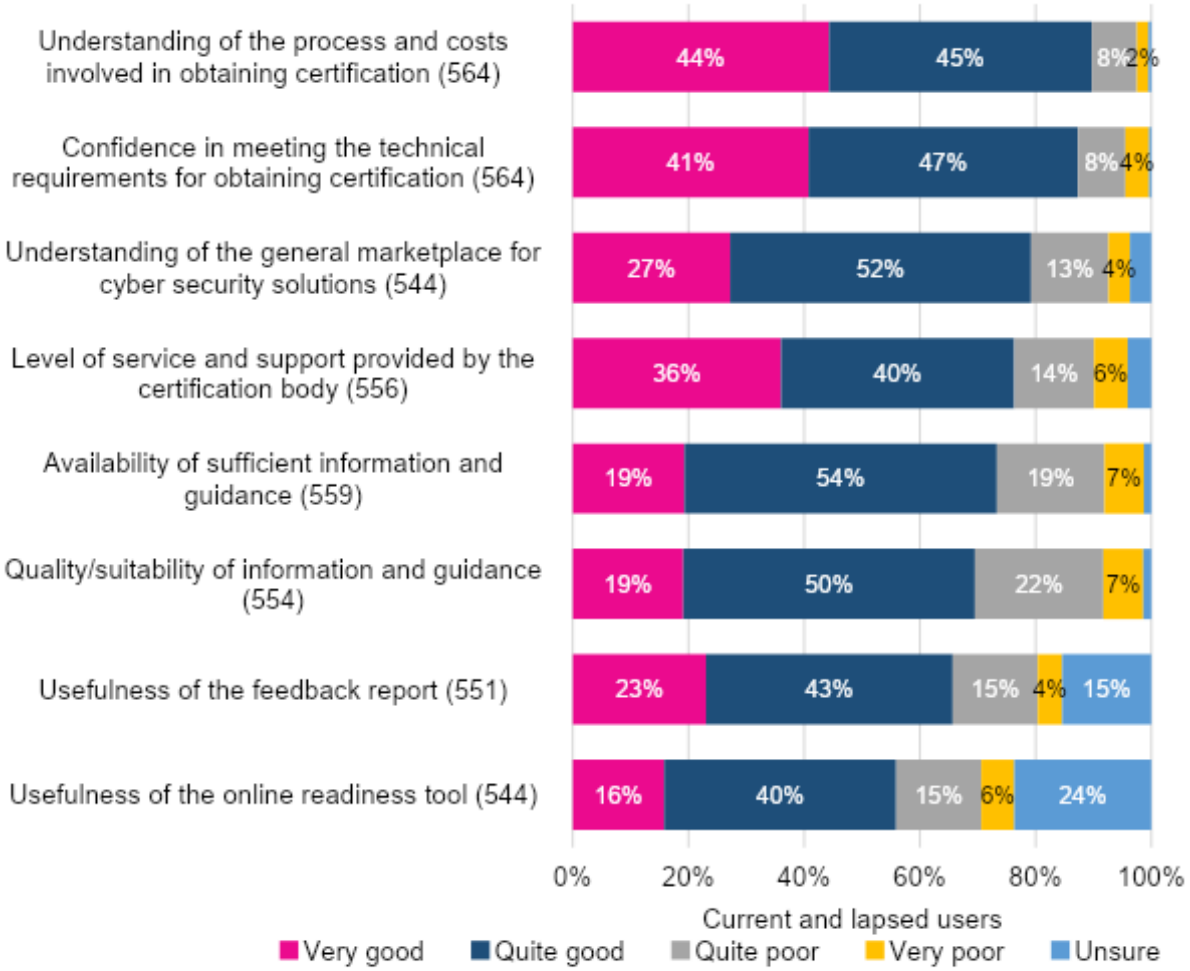
Organisations are most favourable about the following:

- Understanding the process and costs involved (89% very or quite good)
- Confidence in meeting the technical requirements for obtaining Cyber Essentials certification (88% very or quite good)
- Understanding of the general marketplace for cyber security solutions (79% very or quite good)

The weakest areas are as follows:

- Quality and suitability of information and guidance – while more than two thirds (69%) rate this as very or quite good, over a quarter (29%) consider it to be very or quite poor, which indicates room for improvement to meet users' needs
- Usefulness of the Cyber Essentials online readiness tool – more than a fifth (21%) rate this as very or quite poor and almost a quarter (24%) are unsure how to rate it, indicating many may lack familiarity
- Usefulness of the Cyber Essentials feedback report – almost a fifth (19%) rate this as very or quite poor, with a further 15% unsure

Figure 20 Rating of specific aspects of the Cyber Essentials certification experience



Analysis by size-band (not displayed here) reveals similar proportions in most cases, with more than half of micro, small, medium and large organisations giving very or quite good ratings to each specific aspect of the customer journey. Notwithstanding these generally positive views, the favourability of small, medium and large organisations is significantly higher than micro organisations with respect to two specific aspects. These include:

- Understanding of the general marketplace for cyber security solutions (71% of micro organisations said very or quite good)
- Level of service and support provided by the certification body (67% of micro organisations said very or quite good).

A comparison of current and lapsed users (also not displayed) reveals that the majority of both groups consider each aspect of their experience to have been very or quite good. However, there are some significant differences concerning the proportions describing the following aspects as very or quite poor. These include:

- Quality and suitability of information and guidance (46% of lapsed users said very or quite poor compared with 28% of current users)

- Level of service and support provided by the Certification Body (39% of lapsed users said very or quite poor compared with 18% of current users

- Usefulness of the Cyber Essentials online readiness tool (37% of lapsed users said very or quite poor compared with 19% of current users).

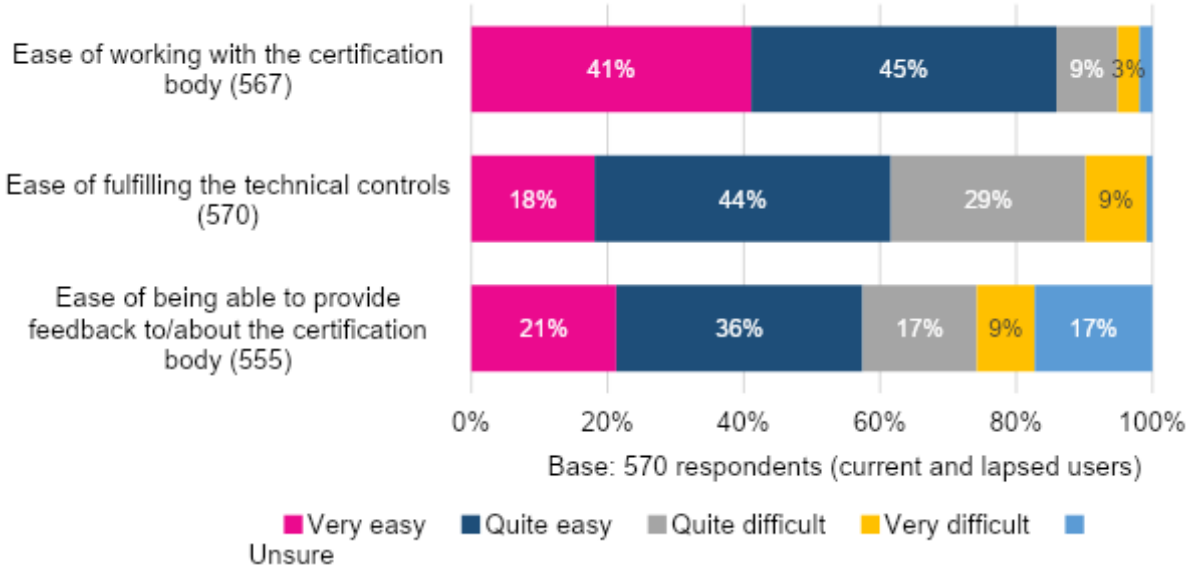
Where negative experiences materialised, these may have contributed (to greater or lesser extents) to these organisations' decisions to renew.

Working with the Certification Body

The vast majority of surveyed current and lapsed users (86%) report working with their Certification Body to have been very or quite easy, which is important given the reliance many organisations place on their Certification Body for support (covered in section 4.1).

However, views are more divided on the ease or difficulty of fulfilling the technical controls. Whilst the majority (62%) consider this very or quite easy, more than a third (38%) do not (Figure 21).

Figure 21 Ease or difficulty of specific aspects of the certification journey



Perceptions are similar across the size-bands. The proportion of large organisations saying very or quite easy is significantly higher than micro organisations with respect to ease of working with the Certification Body and ease of being able to provide feedback to or about the Certification Body (Table 13). There could be very different reasons for organisations of different sizes experiencing difficulties meeting the technical controls, as explored in the next section.

Table 13 Ease or difficulty of specific aspects of the certification journey (by size-band)

Aspect of journey	Rating	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Ease of working with the certification body	Very easy	**41%**	38%	39%	40%	50%
	Quite easy	**45%**	45%	45%	48%	41%
	Quite difficult	**9%**	10%	10%	8%	7%
	Very difficult	**3%**	4%	5%	2%	1%
	Unsure	**2%**	3%	1%	3%	1%
Ease of fulfilling the technical controls	Very easy	**18%**	22%	17%	17%	14%
	Quite easy	**44%**	38%	48%	48%	41%
	Quite difficult	**29%**	27%	29%	28%	31%
	Very difficult	**9%**	13%	5%	7%	12%
	Unsure	**1%**	1%	1%	-	3%
Ease of being able to provide feedback to/about the certification body	Very easy	**21%**	20%	24%	17%	25%
	Quite easy	**36%**	32%	36%	38%	41%
	Quite difficult	**17%**	14%	19%	21%	13%
	Very difficult	**9%**	12%	8%	6%	7%
	Unsure	**17%**	22%	13%	18%	15%

“We really didn't want to go through [Cyber Essentials] but are very glad that we did. The first time was a bit of a nightmare but the renewal was much easier as things were already in place. Going through the scheme made us look in detail at our systems and processes, showing where the danger areas were and ensuring we dealt with them.”

Current user of Cyber Essentials certification, micro employer, private business

5.3 Positive aspects of the customer journey

Current and lapsed Cyber Essentials users were asked what aspects of their organisation’s journey to becoming Cyber Essentials certified (if any) worked particularly well. Excluding those that said none, nothing or not applicable, a total of 250 responses were received to this question out of 575 organisations in scope, therefore just under half (43%) cited specific aspects that worked well.

Responses are summarised below in three broad categories from most to least prevalent. Each of these provides a starting point for DSIT, NCSC and IASME in thinking about what works well so that these can be maintained or built upon to boost awareness and encourage future take-up.

Feedback, support and guidance from Certification Bodies and assessors

Many organisations find their interactions with Certification Bodies to be constructive and practical when encountering difficulties in the Cyber Essentials certification process.

“[The] certification body [was] very helpful, [and] provided excellent feedback about gaps in assurance.”

Current user of Cyber Essentials, large employer, private business

“[The best aspect is] receiving feedback from the certification body and getting clarification of requirements.”

Current user of Cyber Essentials, medium employer, registered charity/trust

Ease of completing the process

Many feel that obtaining Cyber Essentials certification is a sufficiently simple process which is easy to learn and understand, quick to complete and intuitive on a technical level. Some drew attention to the online portal for submitting the applications as an example of this.

“It was all really quite easy. I especially liked completing the question section, having it reviewed by our auditor and amending it as required. It could have been so much harder.”

Current user of Cyber Essentials, Small employer, Private business

Improving security

A minority of respondents mentioned that being able to increase their awareness of cyber security and how to put sufficient measures in place was a key perceived benefit of seeking Cyber Essentials certification.

“It gave us a framework to follow – previously we had been serious about cyber security but lacked an understanding of what to prioritise.”

Current user of Cyber Essentials, large employer, registered charity/trust

There is little variation in views between current and lapsed users of Cyber Essentials.

5.4 Difficulties faced during the customer journey

Current and lapsed Cyber Essentials users were asked what aspects of their organisation’s journey to becoming Cyber Essentials certified (if any) proved difficult or problematic. Excluding those that said none, nothing or not applicable, a total of 326 responses were received to this question out of 575 organisations in scope of the question so more than half (57%) cited difficulties or problems.

Responses are summarised below in three broad categories from most to least prevalent. Again, each of these provides a starting point for DSIT, NCSC and IASME in thinking about some of the key barriers that need to be overcome which could boost retention of existing Cyber Essentials users.

Lack of clarity or understanding of aspects of the process

This remains a considerable problem for surveyed firms with multiple complaints about unclear terminology and jargon. Although many highlighted the ease of working with their Certification Body when seeking guidance, others are either not satisfied with or unaware of the availability of guidance. Key reported issues relate to understanding of the scheme and

the assistance available (especially among registered charities and trusts, and organisations saying that they lack specialist IT knowledge).

“Questions and answers can be open to interpretation by an assessor within the same Certification Body.”

Current user of Cyber Essentials, small employer, registered charity/trust

“[A problematic aspect was] understanding some of the technical requirement questions and pressure of only having a couple of submissions without having to pay again. Not great if you don't have IT [specialists] in house.”

Current user of Cyber Essentials, micro employer, private business

Difficulties meeting the technical controls

Several surveyed organisations have experienced difficulties implementing the technical controls and requirements necessary to progress their Cyber Essentials certification. This is generally perceived to be due to the controls not being adequately tailored to specific settings and sizes of business.

“Some of the technical controls are very narrow which doesn't always suit the type of work we carry out.”

Current user of Cyber Essentials, medium employer, private business

One organisation would like to see more time between feedback during the assessment process and being able to add more information, stating that “a 48-hour window to update our answers is not enough.”

Keeping up with changes

This is chiefly a concern among SME private businesses. Several find having to keep up with information on changes on a yearly basis to maintain Cyber Essentials certification to be burdensome.

“[The main issue is] just knowing when changes have happened – especially significant ones.”

Current user of Cyber Essentials, small employer, private business

“The question set changes every year, making us obtain yearly input on new issues from our IT suppliers. It feels like every year the goal posts are moved.”

Current user of Cyber Essentials, micro employer, private business

Of the above difficulties, the final two themes – difficulties meeting the technical controls and keeping up with changes, are discussed in more detail in the next section.

5.5 Meeting technical control requirements

Perceptions of stakeholders

A commonly reported conceptual challenge raised by stakeholders relates to very different issues faced by the largest and smallest organisations seeking to become Cyber Essentials certified.

For large organisations, whilst the controls might seem quite straightforward in themselves, they might not be easy to implement at scale. Main reasons include having a large and expansive suite of hardware and legacy versions of software across the organisation, which makes the planning and resource investment needed to make changes extremely difficult. Conversely, for micro organisations, meeting the technical control requirements can be a particular challenge given the perceived cost, time and expertise required to do so – especially where these organisations lack a dedicated IT resource or do not have a third party IT consultancy in place.

An issue raised several times is security update management (patching) which is seen by stakeholders as potentially problematic. For larger organisations, it could have negative knock-on effects elsewhere across their network. For micro organisations, the main perceived issues in the eyes of stakeholders are cost and lack of expertise to meet the controls.

Some organisations appear to lack understanding about the broader value of having greater cyber security in place and the implications of not doing so. In some cases this can result in the perception of Cyber Essentials as a form of 'tax' – as highlighted by one stakeholder in the following quotation:

“Some feel disenfranchised because they think the government is putting an unfair tax on them. It’s being handled in quite a blunt way by government. Those that sail through are happy and those that don’t achieve Cyber Essentials are unhappy, but mainly because it means they can’t get government contracts.”

Stakeholder

Looking across the sectors, one stakeholder said that while charities have embraced Cyber Essentials (where they have sufficient expertise), universities have genuine problems meeting the controls and Cyber Essentials is “not the right thing for schools” so is not heavily pushed. In the private sector, construction is seen as facing particular challenges due to many firms having “old or complex estates.”

Despite these challenges, there is a recognition by some stakeholders that Cyber Essentials straddles a difficult path largely successfully. One remarked that “the balance is about right because all organisations are being challenged” and that once they’ve completed the process there’s “far more positive feedback than negative which suggests it’s about right.”

Stakeholders are strongly of the view that awareness-raising and marketing of Cyber Essentials needs to be strengthened, although the signs are encouraging; one stakeholder observed that “trade bodies are asking for presentations from IASME”.

Perceptions of surveyed organisations

All surveyed organisations were asked on a scale from 1 (not at all appropriate) to 10 (completely appropriate) how appropriate they consider the current requirements and technical controls to attaining Cyber Essentials certification to be.

The overall mean rating is 7.1 (base of 655 respondents). The ratings show some variations between groups – significantly higher among Certification Bodies compared with current and lapsed users, and significantly higher among small and medium sized organisations compared to large and micro organisations.

- Certification Bodies (7.8)
- Current users (7.1)
- Lapsed users (5.6)
- Micro (6.5)
- Small (7.4)
- Medium (7.4)
- Large (6.6)

When asked to explain the reasons for their rating, the vast majority giving higher ratings mentioned the adaptability of the controls and requirements, and their role in helping to maintain a general and universal standard. They tend to believe that the controls and requirements should be broadly applicable to most organisations.

(9/10) “These are simple controls that can be implemented by anyone, in any organisation and help to protect against common cyberattacks.”

Cyber Essentials Certification Body

(8/10) “Most [requirements and controls] are appropriate but some are inflexible and others may be outdated by latest technology practices (e.g. password expiry is now not recommended by Microsoft), local admin for users can be controlled by Intune/Azure and should not be entirely ruled-out.”

Current user of Cyber Essentials, medium employer, private business

It should be noted from the above quotation that password expiry has not been part of Cyber Essentials since 2018, indicating a potential misconception which could be usefully addressed.

Those who gave lower ratings generally referred to the perceived inflexibility of Cyber Essentials controls and requirements for their own organisation. Academic institutions tended to be more critical, for reasons previously discussed.

(2/10) “Requirements do not scale for educational institutions.”

Current user of Cyber Essentials, large employer, academic institution

Several smaller private businesses that gave lower ratings view the Cyber Essentials controls and requirements as being more appropriate to larger businesses, primarily due to the perceived cost and resource requirement to meet them. Conversely, some larger organisations think the controls are better suited to smaller organisations, pointing to a lack

of depth in the controls and requirements, which they argue do not cater for a wide variety of business settings and contexts. Some Certification Bodies in their responses acknowledged both sides of the problem.

(6/10) “The controls meet the certification but the binary nature of the questions [is] more suited to smaller organisations. As organisations get larger, it becomes more difficult to give the correct answers to meet the certification requirements.”

Current user of Cyber Essentials, large employer, private business

(4/10) “The controls are a foreign language to most smaller businesses, or are not technical or detailed enough for larger organisations with dedicated security staff in place. Larger organisations tend to misunderstand the controls or attempt to over-engineer the solutions.”

Cyber Essentials Certification Body

The views of surveyed organisations supports a point made by strategic stakeholders – namely that Cyber Essentials faces a conceptual challenge in providing a solution that meets all types and sizes of organisation. It raises questions as to whether the scheme’s prescriptive rather than risk-based approach to setting and implementing controls is correct. This will largely come down to where the scheme considers itself to be situated in the market and the degree to which certain additional flexibilities can be built in.

Communications about changes to control arrangements

It is understood that control arrangements are subject to a 12-month rolling review by IASME and NCSC. On the one hand, strategic stakeholders interviewed for the research acknowledge that the Cyber Essentials scheme has to be sufficiently agile to respond to changing threats whilst on the other hand that these changes have resource and cost implications for organisations seeking to maintain certification.

Certain stakeholder feedback refers to a “big communications problem” and that organisations are not being made aware in sufficient time about changes to control arrangements. This is partly attributed to the need for more joined-up working between IASME, NCSC and DSIT.

Whilst some stakeholders praise the information about changes to controls communicated online by NCSC and IASME, they also criticise the fact that users seem to be left to find this information for themselves and state that it would be more helpful if cascaded down to them in a more structured way. They argue that the technical work on the controls and updates works well but that more needs to be done to translate that into a strategic conversation and rolled out via a clear communications plan to Cyber Essentials users.

“When experienced cyber security professionals in large organisations say something is difficult, it’s essential not to dismiss those opinions… goalposts are being moved… things need to be communicated better.”

Stakeholder

“There’s an issue at the moment where Cyber Essentials users are hearing about technical controls coming into force this month that were communicated via NCSC’s website over a

year ago. If it's been public for a year then it either hasn't filtered through the Certification Bodies properly or it's not in the right forums."

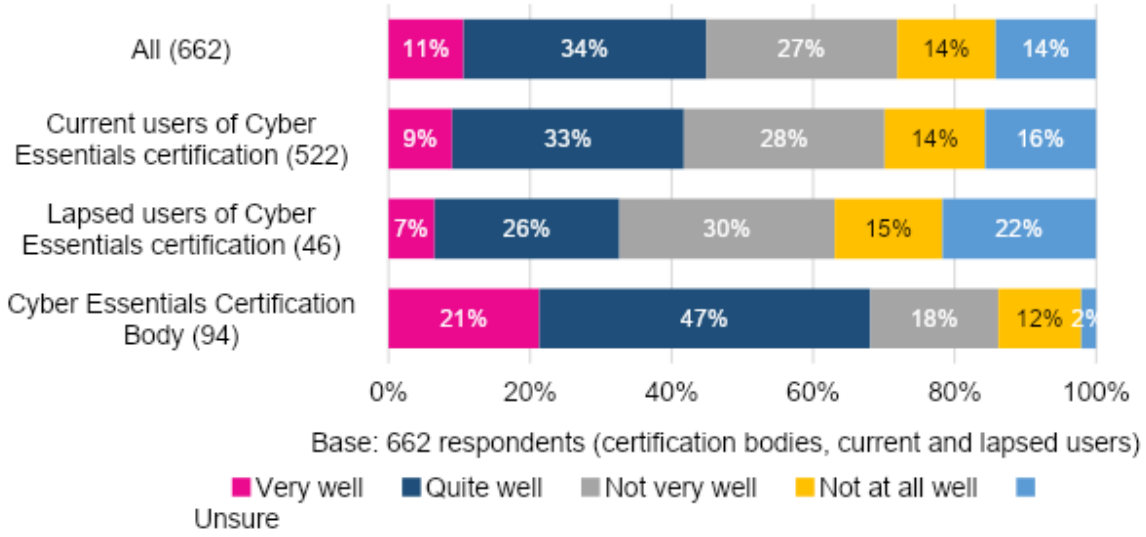
Stakeholder

These views point to a need for a more structured and timeous approach to communicating and disseminating changes through Certification Bodies – especially where there are major updates in the future.

All surveyed organisations (including current and lapsed users, as well as Certification Bodies) were asked how well they think changes and interim updates to control arrangements are communicated and put in place. Certification Bodies are significantly more positive than current and lapsed users, with more than two thirds (68%) saying very or quite well (Figure 22).

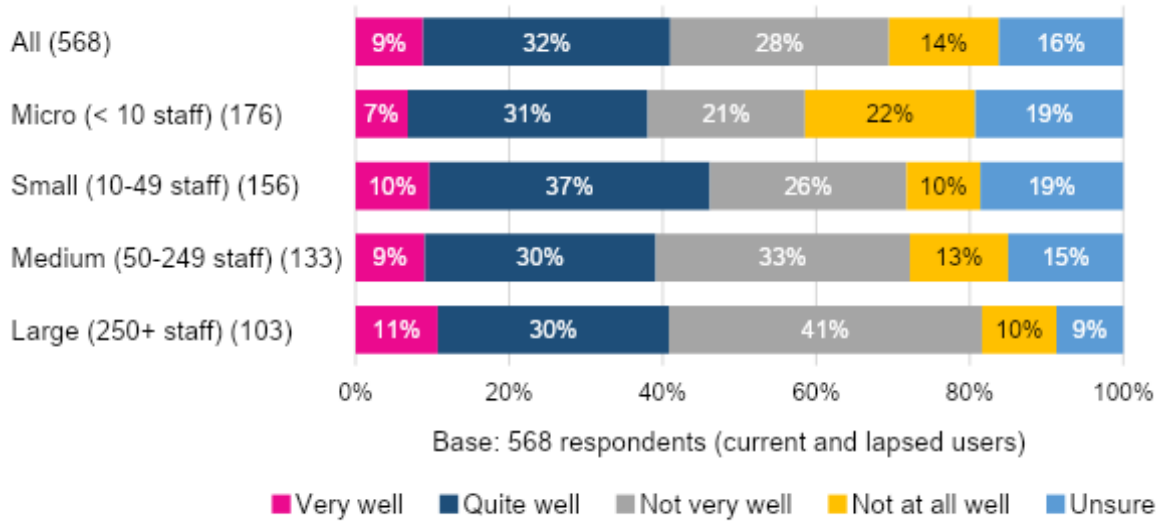
The difference in perspectives between Certification Bodies and users points to a possible disconnect between how well Certification Bodies believe communications have been deployed compared with the user base, and that this needs to be given greater attention with lessons learned for future updates – especially major changes.

Figure 22 How well changes to controls are communicated (by current and lapsed users)



Analysis of the same question by size-band with respect to current and lapsed users reveals similar patterns. Almost a fifth (19%) of both micro and small organisations were unsure how to answer this question, which could mean that they lack knowledge of where to find information about changes or do not know what the changes are (Figure 23).

Figure 23 How well changes to control arrangements are communicated (by size-band)



Reasons for saying 'quite well'

Reasons given for describing the communication of control arrangements as 'quite well' varies. Some of these organisations believe that communications about changes are readily available. Many, though, say that information can be accessed, but only with an awareness of how to find it.

(Quite well) "I tend to use Google or the NCSC website to find out this information, rather than expecting to be contacted."

Current user of Cyber Essentials, medium employer, registered charity/trust

(Quite well) "Information is available if you know where to look or who to ask. Could a newsletter be sent to all current certificate holders about these changes?"

Current user of Cyber Essentials, medium employer, private business

The majority of Certification Bodies expressed similar views. Some have no major concerns relating to the efficacy of the communication of changes and updates and believe IASME performs well in this regard. Others stress the need to improve – that information is out there but needs to be better conveyed.

(Quite well) "Once you know where to look [it's] okay and IASME's help is very, very good."

Cyber Essentials Certification Body

Reasons for saying 'not very well' or 'not at all well'

The vast majority of those who answered 'not very or not at all well' said that they had not received any update about the changes. This is especially true of micro employers and academic institutions.

(Not at all well) “I don't appear to receive any communication about changes to the standard as they occur. It's [a] surprise each year as to what new measures are required.”

Current user of Cyber Essentials, micro employer, private business

(Not very well) “[We] had no communication from anybody apart from correspondence relating to the success of any given application.”

Current user of Cyber Essentials, medium employer, academic institution

Several Certification Bodies share the concerns of users, adding that there are often inconsistencies in the way information about changes is circulated to them and, in turn, to users.

(Not at all well) “[Communication is] very scrappy and there’s lots of ambiguity. The objectives, impacts and explanations of changes need to be crystal clear. This would assist the [Certification Body] and applicants to understand the purpose.”

Cyber Essentials Certification Body

Other users who answered ‘not very or not at all well’ said that they had become aware of updates and changes through liaison with Certification Bodies and assessors but still feel that changes should be communicated in more accessible and coherent ways.

(Not very well) “I only [knew] about the new version of the certification this year because the assessor company we use notified us in plenty of time. I feel that the changes were not published sufficiently.”

Current user of Cyber Essentials, medium employer, private business

5.6 Barriers faced by academic institutions

There is evidence that some surveyed organisations, especially academic institutions, feel that Cyber Essentials does not suit the scale of their operation, with a minority of the view that Cyber Essentials feels like a “tick-box exercise”. The fact that surveyed academic institutions are more commonly driven (than other organisation types) to take up Cyber Essentials to meet public sector procurement requirements (section 3.1) risks exacerbating this barrier and warrants a more focused look on the views of these organisations.

“[Cyber Essentials] is a tick box exercise. We do it because we are mandated to do so but it doesn't take account of how things work in the real world. It’s not suited to big businesses. Its place is for small organisations with no in-house IT department who are using it as a way to show they have something.”

Current user of Cyber Essentials large employer, academic institution

“[Cyber Essentials] does not understand the issues that face [further education]. It’s easier to comply with ISO 27001 than Cyber Essentials in an educational setting.”

Current user of Cyber Essentials, large employer, academic institution

Another issue emerging from the survey – particularly among academic institutions – relates to the use of BYOD.

"[We were] intending to [renew Cyber Essentials], but the BYOD requirement [is] burdensome and requires major changes in operations – we have large numbers of hybrid and casual workers."

Lapsed user of Cyber Essentials, large employer, academic institution

In a 2022 blog article, Jisc notes that BYOD offers a good fit with education environments, supporting flexible access from a range of different locations and devices. More recently, personally owned devices have been essential to the enforced shift to home working during the pandemic and to the new hybrid ways of working that are a legacy of COVID-19.

In January 2022, the NCSC made clear in a threat report that "due to the increased number of personal devices connected to enterprise networks, it is likely these devices will be targeted to gain access to the enterprise network". Whilst there are several options open to colleges and universities to meet BYOD criteria, some survey respondents to this evaluation have expressed their concern regarding the feasibility of implementing those.

DSIT, NCSC and IASME are currently engaging with the Universities and Colleges Information Systems Association to address certain challenges relative to universities specifically. Furthermore, in 2023 IASME introduced changes to the requirements for information about BYOD specifically on the feedback from universities to allow them to manage devices more easily.

Other large organisations responding to the survey acknowledge what they see as different strengths and limitations of Cyber Essentials compared with other, similar, certifications.

Chapter 5 Summary Box

The overall cost and time involved for organisations to obtain certification varies considerably between organisations and especially between size-bands. The overall mean spend (excluding outliers) is estimated at £4,941. This factors in resources needed to meet the technical controls such as consultancy support and changes to hardware, software and updated policy implementation.

Whilst cost and time were not among the main difficulties cited by users in their customer journey, the fact that these featured among the top three reasons for certification lapsing suggests that cost and time stresses are almost certainly being felt by some organisations. This points to a potential case to review the pricing structure for Cyber Essentials.

On the whole, most surveyed current and lapsed users have had a positive certification experience, with the majority rating various specific aspects of the customer journey as very or quite good. However, and building on the previous section, the quality and suitability of information and guidance is considered by more than a quarter (29%) to be very or quite poor.

The vast majority of surveyed current and lapsed users (86%) report working with their Certification Body to have been very or quite easy, which is important given the reliance

many organisations place on their Certification Body for support. However, views are more divided on the ease of fulfilling the technical controls. Whilst the majority (62%) consider this very or quite easy, more than a third (38%) do not.

Qualitative insights reveal that the most positive aspects of the customer journey relate to: i) feedback, support and guidance from Certification Bodies and assessors; ii) ease of completing the process; and iii) improving security. The most difficult aspects relate to: i) lack of clarity or understanding of aspects of the process; ii) difficulties meeting the technical controls; and iii) keeping up with changes.

On a perceptual scale from 1 (not at all appropriate) to 10 (completely appropriate) organisations rate the technical controls at a moderate 7.1. Among micro and large organisations, the means are lower (6.6 and 6.5 respectively) – a significant difference. There appear to be distinct issues facing the largest and smallest organisations. For large organisations, the controls can be difficult to implement at scale due to IT infrastructure complexities. For micro organisations, the main challenge lies in the perceived cost, time and expertise required to implement them, especially where they lack access to an expert IT resource.

Academic institutions also appear to face unique barriers, as evidenced from this and other research. The prevalence of Bring Your Own Device (BYOD) practices in these settings has led to some of these organisations expressing concern about their perceived ability to meet the requirements of Cyber Essentials.

There is a significant difference between the perspectives of Certification Bodies and of current and lapsed users in how well changes to control arrangements are communicated. Only a minority of current and lapsed users consider changes to have been communicated very or quite well, which points to a possible disconnect in how well Certification Bodies believe certain communications have been deployed compared with the user base.

6. Cyber Essentials Scheme Effectiveness and Improvement

This chapter offers a more thorough look at the effectiveness of the Cyber Essentials scheme, spanning governance, implementation, influence on organisational behaviours and how the scheme could be improved. Insights are provided in turn from strategic stakeholders, current and lapsed Cyber Essentials users, as well as Certification Bodies.

6.1 Stakeholder perceptions of effectiveness

Governance

Strategic stakeholders interviewed for the research generally seem content with the way the Cyber Essentials scheme has been managed and delivered between (former) DCMS, NCSC and IASME. There is a sense that partnership working has increased and could be strengthened by a greater commitment to transparency, sharing information that would benefit all parties, and taking on board feedback with a view to making changes that would serve the greater good.

A minority expressed concerns that the three-way governance arrangement can cause confusion about where current and potential users should turn for information and advice. One stakeholder remarked that IASME's website does not make its affiliation with the government as clear as it could be and that doing so could help to establish trust and confidence in the Cyber Essentials scheme more quickly.

"The branding seems a bit weird. Cyber Essentials is advertised as an NCSC assured programme, but the readiness tool points to IASME. Talking to organisations, they find that a bit strange. It needs to look more like a government scheme."

Stakeholder

Stakeholders largely feel that the move to consolidate five Accreditation Bodies to one in 2020 (under IASME) proved to be the right thing, although the end result is not yet perfect. Anecdotal evidence points to past inconsistencies between the former Accreditation Bodies and – in turn – the Certification Bodies that each Accreditation Body was responsible for. For example, where one Accreditation Body might advocate a risk-based approach to implementing the controls, another might take a more black-and-white approach, with the latter being what was originally intended.

One stakeholder remarked that the 2020 consolidation caused some "pain" for users, partly because the change came in during the onset of the COVID-19 pandemic and partly because organisations that had gained certification by doing things one way discovered that their existing approaches were no longer being accepted.

Implementation

Based on the views of stakeholders, the current Cyber Essentials certification process offers the following key strengths in addition to its value in helping users to secure contracts that depend on it. These include helping organisations to:

- Meet minimum cyber security baselines
- Better understand how things can go wrong if a cyber attack were to happen
- Mitigate risks from common ways businesses are cyber attacked and help take the pressure away
- Be better equipped to put in place formal response plans in the event of a cyber attack
- Help to raise the profile of cyber security with more prominent positioning on boardroom agendas
- Encourage smaller businesses to think more seriously about cyber security where they might not have done so before
- Improve knowledge transfer within the organisation

However, stakeholders were also keen to stress the challenge of a 'one-size-fits-all' approach, especially where there are quite different challenges to implementing cyber security measures for organisations of different types, sizes and sectors. There are calls from a minority of stakeholders (and some survey respondents) for the assessment process to be less binary and to adopt a more risk-focused approach that takes into account different business settings and challenges. The Pathways pilot project (cf. section 1.2) is one example of this.

Several referred to a particular nuance of the scheme that they see as problematic. On the one hand, a key driver of Cyber Essentials uptake is where it is mandated in government contracts. However, too much focus on this route to building certification levels would risk cultivating the perception of Cyber Essentials as "a means to an end" or a "hoop to jump through" rather than for the cyber security benefits at its core.

This makes it important to promote more strongly how Cyber Essentials can contribute to improving organisations' understanding of cyber security in general and the consequences of inadequate cyber security.

Consistency between Certification Bodies

Stakeholders largely feel that coordination, consistency and communications have changed for the better with a single Accreditation Body. However, one stakeholder was keen to stress that there are still differences in the assessment processes between Certification Bodies, as touched on above, with some more rigorous than others, as well as differences in the level of support and consultancy they provide to their users.

This leads to the question of what role the Certification Bodies should ultimately have, with a minority of stakeholders questioning the appropriateness of Certification Bodies fulfilling the dual roles of assessor and advisor to organisations seeking certification. One said that the assessor should not have responsibility for "fixing the user's problem." This argument clearly needs to be balanced against the importance that users place on the support they get from Certification Bodies (section 4.2) and the fact that Cyber Essentials is ultimately about ensuring that long-term cyber security controls are in place.

There are some concerns among stakeholders about the competence of certain assessors within some Certification Bodies. One stakeholder remarked that there is not much profit margin in being a Certification Body, especially where they are paid on certification, creating the risk of driving a “race to the bottom” and the potential for “perverse behaviours” where it is in the Certification Body’s interests for an organisation to pass. The extent to which such practice occurs cannot be validated within the context of this evaluation but could be further investigated in terms of the extent to which it occurs, its influence on Certification Body behaviours and what, if anything, could be done differently.

6.2 Users’ perceptions of effectiveness

Current and lapsed users were asked what changes in cyber behaviours they have observed in their organisation since attaining Cyber Essentials certification (Figure 24). The findings indicate a range of positive outcomes that could make a lasting difference to each organisation if nurtured and maintained. The most prominent are:

- Improved cyber security awareness and understanding (71%)
- Being better able to mitigate cyber security risks in their own organisation (52%)
- Applying further technical controls beyond what is required for Cyber Essentials (42%)

Figure 24 Changes in cyber behaviours

Responses classified as ‘Other’ include:

- Forcing the organisation to make changes that it had not wanted to make but which are necessary for data security
- Aligning with other policies and procedures such as GDPR etc.
- Ensuring controls are applied in a standardised baselined approach across the organisation
- Raising the profile and awareness of cyber security in the organisation and its culture
- Discounts on business insurance
- Encouraging suppliers to comply

Proportions are similar by size of organisation, although it is noteworthy that 56% of large organisations say they have applied further technical controls beyond what is required for Cyber Essentials, which is significantly higher than 31% of micro organisations and 41% of small organisations (Table 14). This indicates that Cyber Essentials is providing a baseline level of security which many organisations are using as a launchpad to go further.

Table 14 Changes in cyber behaviours (by size-band)

Changes	All	Micro (< 10 staff)	Small (10-49 staff)	Medium (50-249 staff)	Large (250+ staff)
Base	**526**	**153**	**149**	**128**	**96**
Improved cyber security awareness/understanding	**71%**	65%	77%	75%	64%
Better able to mitigate cyber security risks in our own organisation	**52%**	53%	54%	54%	46%
Applying further technical controls beyond what is required for Cyber Essentials	**42%**	31%	41%	48%	56%
Having a monitoring strategy in place	**33%**	34%	34%	34%	28%
Using Cyber Essentials as a cyber risk assurance tool in the supply chain	**31%**	25%	32%	34%	35%
Having formal incident response plans in place	**26%**	25%	33%	24%	22%
Better able to manage cyber security risks in our supply chain	**21%**	19%	22%	20%	25%
Other	**12%**	14%	6%	9%	22%

Advocacy

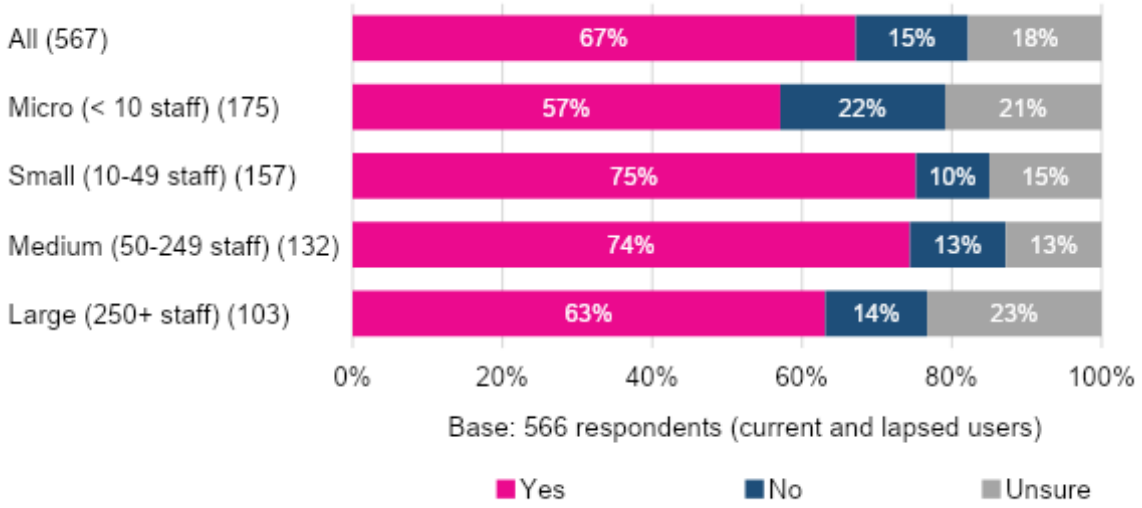
Just over two thirds (67%) of current and lapsed users would recommend Cyber Essentials to others (Figure 25). Whilst an encouraging picture, there is room to strengthen the customer experience to improve lasting impressions.

Advocacy among small and medium organisations is significantly higher than micro organisations and somewhat higher than large organisations. This pattern is perhaps

unsurprising given evidence to date on the unique challenges faced by these organisations in implementing the technical control.

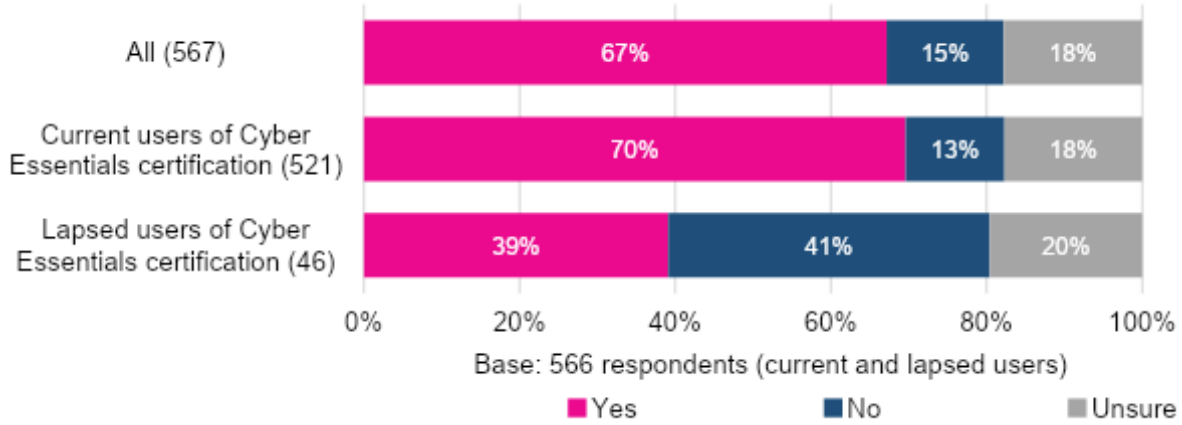
The fact that almost a fifth of organisations are unsure about whether they would recommend Cyber Essentials suggests that these organisations are less able to identify with the benefits that the scheme offers.

Figure 25 Willingness to recommend Cyber Essentials to others (by size-band)



Advocacy among current users of Cyber Essentials certification (70%) is significantly higher than lapsed users (39%) (Figure 26). However, the fact that almost four in ten lapsed users would still recommend Cyber Essentials indicates that whilst Cyber Essentials may not have been right for them, the scheme is still a sufficiently strong product.

Figure 26 Willingness to recommend Cyber Essentials to others (by current and lapsed users)



Why users would recommend Cyber Essentials to others

Those that would recommend Cyber Essentials are generally of the view that increasing awareness about an acceptable standard of cyber security is crucial in the modern business environment. They view the Cyber Essentials scheme as cost-effective and accessible – especially among registered charities and trusts.

“The Cyber Essentials scheme provides good value for money compared to other, similar certifications. I would recommend others, who don't already have the certification, to have it [because] of the benefits it brought us.”

Current user of Cyber Essentials, medium employer, registered charity/trust

Smaller private businesses in some cases recommend Cyber Essentials over the more extensive and expensive ISO 27001.

“As a strong believer and advocate for cyber security in the SME space, I both recommend Cyber Essentials and believe it's the only certification that's affordable and easily attainable for small businesses. E.g. the work to obtain ISO 27001 is beyond most small and micro businesses in the UK.”

Current user of Cyber Essentials, micro employer, private business

Large organisations that would recommend Cyber Essentials share the view that certification is worthwhile because it provides a good baseline for security. While they acknowledge that other, more extensive, security schemes are available, they make the point that Cyber Essentials certification allows firms of all kinds to accord with the minimum acceptable standard and would encourage others to do the same.

“It just makes sense. It drives improvement [and] proves that ‘security’ doesn't get in the way of the business – unless the business is irresponsible, incompetent or inept.”

Current user of Cyber Essentials, large employer, academic institution

Why users would not recommend Cyber Essentials to others

Those that would not recommend Cyber Essentials to others do not typically believe that Cyber Essentials controls are applicable or relevant to the workings of their own organisation.

“I don’t think it represents the reality of complex organisations. It’s too rigid and doesn't provide any flexibility for a risk-based approach.”

Current user of Cyber Essentials certification, large employer, NHS organisation

Lapsed users that would not recommend Cyber Essentials are commonly of the view that most of the scheme’s value lies in certification being required by their clients, which is the only reason why they would otherwise recommend it.

“It is not relevant for ALL businesses and asks far too much of micro businesses.”

Lapsed user of Cyber Essentials certification, micro employer, private business

These differing perceptions point to a need to promote Cyber Essentials scheme benefits more strongly. Doing so with more and better tailored information for different types and sizes of organisation would potentially help them make fully informed decisions. There is

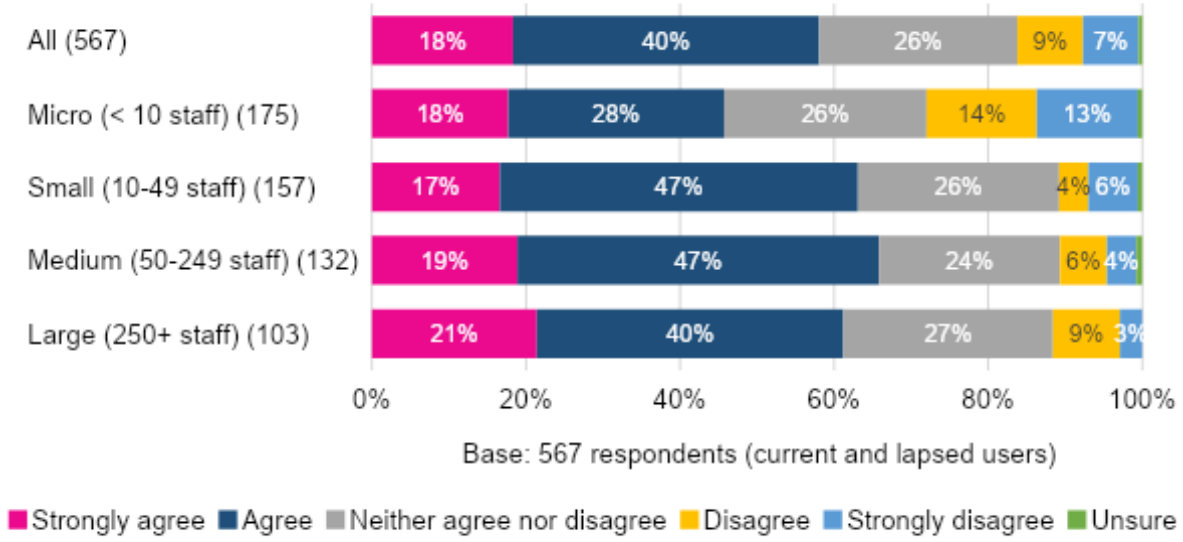
also a case to consider how, if at all, controls could be more flexible or adaptable. These points therefore tie in closely with those raised in section 5.5.

Overall value for money

Current and lapsed users were asked to what extent they agree that the Cyber Essentials scheme overall represents good value for money. The emerging picture is mixed. While the majority (58%) strongly agree or agree, just over a quarter (26%) are ambivalent and a minority (16%) disagree or strongly disagree. This offers a clear opportunity to help organisations better understand what they are getting in return for their investment.

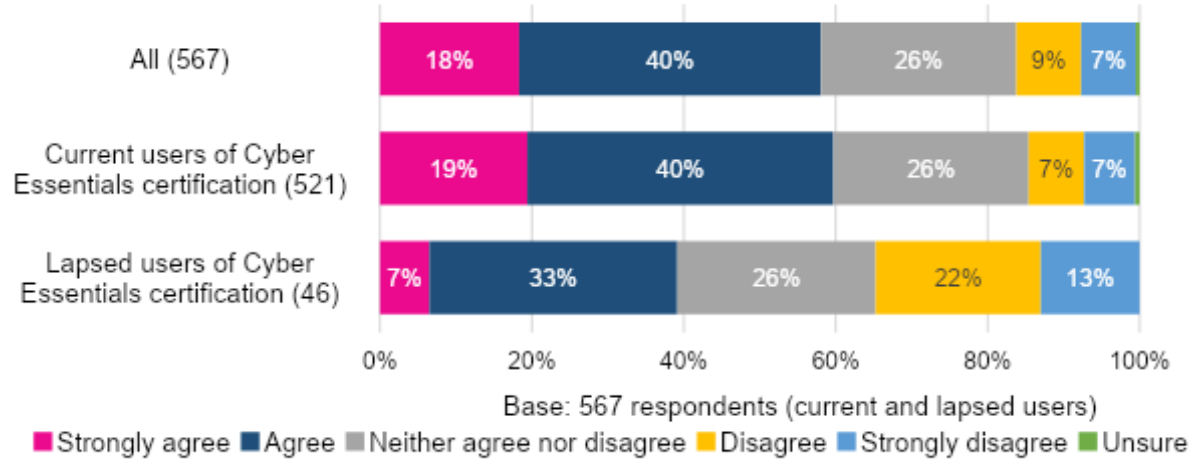
Looking across the size-bands, the proportion of large organisations in agreement (61%) is significantly higher than micro organisations (46%) (Figure 27). This reinforces the need for more to be done to help micro organisations understand the benefits of being cyber secure.

Figure 27 Perceived value for money of Cyber Essentials (by size-band)



Comparisons between current and lapsed users reveal a marked difference in views. The proportion of current users strongly agreeing or agreeing that Cyber Essentials represents good value for money (59%) is significantly higher than 40% of lapsed users (Figure 28).

Figure 28 Perceived value for money of Cyber Essentials (by current and lapsed users)

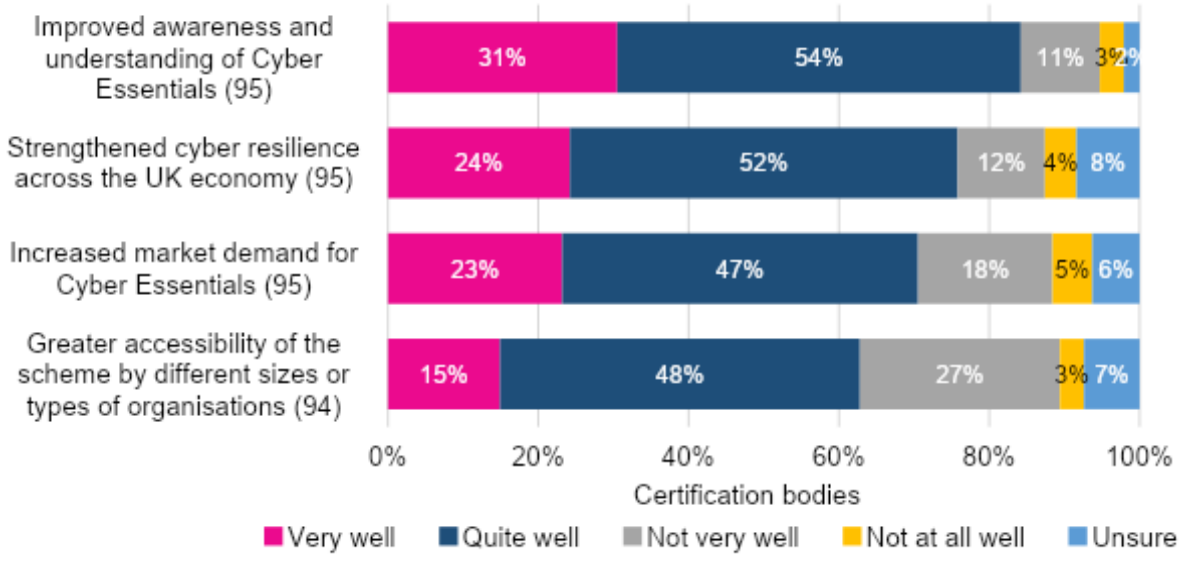


How organisations came to these views is likely to be a blend of the positives and difficulties raised and discussed in the preceding sections

6.3 Certification bodies' perceptions of effectiveness

Certification Bodies were asked how well they think Cyber Essentials scheme processes are helping to achieve specific outcomes. Most are favourable in relation to each outcome, although it is noteworthy that almost a third (30%) answered either not very well or not at all well in relation to the intended outcome of 'greater accessibility of the scheme by different sizes of types of organisation' (Figure 29). This comparatively weaker area aligns with earlier findings.

Figure 29 How Cyber Essentials is helping to achieve specific outcomes



Aspects of delivery that work well

Certification Bodies were asked what aspects of Cyber Essentials scheme implementation and delivery (if any) work particularly well. A common message is that Cyber Essentials provides an effective and accessible security baseline for certified organisations. Some note the ease with which smaller businesses in particular are able to develop an effective standard of cyber security, while others underscore that Cyber Essentials certification compels a company-wide awareness of cyber security and its importance.

Several are also complimentary about IASME, referring to its liaison and support as dependable, friendly and supportive. They also feel that a single Accreditation Body offers consistency in messaging and delivery.

"[Cyber Essentials is] especially good for small to medium sized businesses which have never considered their cyber security previously and which are engaged in the process (and not doing it begrudgingly because of third-party pressure)."

Cyber Essentials Certification Body

"We find that it gives users the opportunity to evaluate their current cyber security to identify and address internal and external risks. We generally find users are far more educated on keeping their organisation safer after going through the certification process."

Cyber Essentials Certification Body

"We find a lot of users presume their IT are doing a lot of this work already but the vulnerability assessment highlights where they are not doing things which is really useful."

Cyber Essentials Certification Body

Other factors of the Cyber Essentials scheme that are deemed by Certification Bodies to work particularly well are as follows:

- All of it is appropriate and proportionate
- Consistency of questions and guidance
- Easy to complete self-assessment
- Having a distributed model using Certification Bodies under IASME which ensures reach to a wide spread of companies and their users using multiple marketing channels
- Notable improvements in awareness and marketing
- The Pervade online assessment platform and Cyber Essentials Plus test portal are working well
- Unintrusive tests

Challenges affecting delivery

Certification Bodies were asked for their view on the current challenges affecting Cyber Essentials scheme implementation and delivery. One of the biggest is the perception that many users and potential users lack a sufficiently detailed understanding about cyber security, thus lacking the incentive to make the most of it. As a result, they say that some Cyber Essentials users go through with certification as a means to an end without paying sufficient attention to the importance of cyber security more generally. Furthermore, it is felt that some companies may rush the assessment with the aim of 'ticking the right boxes', while others may incorrectly believe that they are at no or minimal risk.

"Most applicants apply reluctantly because they are told they need it by a customer. Few strive to get it."

Cyber Essentials Certification Body

"[There is an] ongoing [challenge] of 'convincing' organisations that Cyber Essentials is good for them against their belief that a cyber attack 'will never happen to them'."

Cyber Essentials Certification Body

In order to overcome this challenge, some Certification Bodies set out their ideas for improving awareness of cyber security and encouraging the "right" motivation for completing Cyber Essentials certification. Of importance are improvements to advertising and marketing, and diversifying the control requirements and assessment criteria rationally to suit a variety of business contexts.

"[Cyber Essentials needs] stronger funding from [government] with regard to marketing Cyber Essentials across industry sectors, including to SMEs."

Cyber Essentials Certification Body

"Having a one-size-fits-all approach presents some challenges. For some micro companies without growth plans, some of the process and policy questions seem tedious and unnecessary."

Cyber Essentials Certification Body

Other challenges raised include:

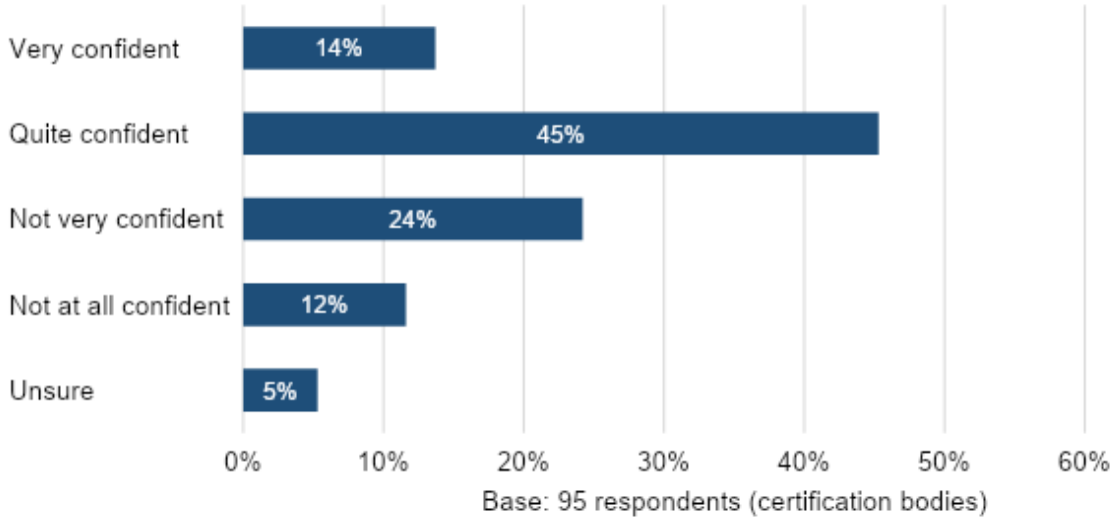
- Lack of awareness about Cyber Essentials, especially among businesses working outside of government circles, and that more could be done to get the message out there
- Cost, particularly to SMEs
- Implementation of controls should be completely independent, commenting that "you cannot mark your own homework"
- Issues surrounding BYOD and remote working
- The potential for users taking the assessment to embellish their answers

These findings emphasise the importance of more effectively conveying to current and prospective users the importance of cyber security, why they should take it seriously and how Cyber Essentials provides a cost-effective solution to starting that journey.

Confidence in consistent delivery

Finally in this section, the majority of Certification Bodies (59%) are very or quite confident that the Cyber Essentials scheme is being delivered consistently by different Certification Bodies, although 36% are not very or not at all confident (Figure 30).

Figure 30 Confidence in consistent Cyber Essentials delivery



Certification Bodies answering anything other than ‘very confident’ were asked to elaborate on current consistency issues and the reasons why they exist. Most mentioned differing requirements, standards and capabilities between Certification Bodies. Some feel that certain assessors lack sufficient technical expertise to carry out the assessment and that the criteria are too open to interpretation.

(Quite confident in consistency of Cyber Essentials delivery) “Some of the questions asked by 'some' assessors during update sessions seem to show a fundamental lack of understanding of information security and the scheme requirements. It is absolutely better than it was with multiple [Accreditation Bodies] but there is still more work to be done.”

Cyber Essentials Certification Body

(Not very confident in consistency of Cyber Essentials delivery) “As an auditor, I have insight into [Cyber Essentials] assessment and I see frequent inconsistencies. The amalgamation of [Accreditation Bodies] has brought together a varying degree of standards and interpretations.”

Cyber Essentials Certification Body

Some Certification Bodies who were quite confident nevertheless flagged assessor training as an area for improvement.

(Quite confident) “[The reasons for inconsistency include] the lack of a proper training function for assessors, the lack of a proper knowledge base for assessors to ask questions [and] much of the guidance does not help.”

Cyber Essentials Certification Body

Additionally, a minority of Certification Bodies questioned the motives of assessors, reinforcing an issue raised by stakeholders.

(Not very confident) “Some Certification Bodies have vested interests in passing applicants e.g. making sure customers they service are as secure as possible. This is ideal. Other Certification Bodies however, who purely transact for gaining Cyber Essentials accreditation, have no vested interest to ensure the customer is telling the truth on the application. This then leads to customers going down the ‘easy route’ of going to a Certification Body that will simply pass the customer, rather than engaging with the scheme correctly and ensuring all controls are being met.”

Cyber Essentials Certification Body

6.4 Suggestions for improvement

All surveyed organisations were asked in what ways they think the Cyber Essentials scheme could be improved in the future. Suggestions are grouped into the following five main themes – ordered from most to least discussed though the survey responses.

1. Better tailoring and scalability

Many organisations feel Cyber Essentials could be better tailored to a wider variety of sectors and size-bands. Academic institutions commonly assert that Cyber Essentials has limited applicability to educational settings and view it more as a ‘tick box’ exercise as a result. Larger organisations often mention that the scale of their operations necessitates a risk-based approach in addition to the general standard Cyber Essentials enforces. Some smaller organisations feel that the process could be simplified.

“[Cyber Essentials should be] more flexible [and] address how larger and global organisations manage risk etc.”

Current user of Cyber Essentials, large employer, private business

“[Cyber Essentials should be] simpler, easier to understand, cheaper, tailored more specifically to the size of the organisation and the nature of their work, and the number of employees. We are a very small charity with one employee and do not have an office or tech support. I work from home.”

Current user of Cyber Essentials, small employer, registered charity/trust

2. Improvements in communication, guidance and support

Organisations of all sizes feel that Cyber Essentials guidance could be made clearer to enhance understanding of the controls, requirements and questions.

This includes communicating changes more overtly and in advance, simplification of language and terminology such as in explanatory notes, clarity on which controls apply to desktop and mobile operating systems, and clarity on how controls should be applied to user-owned devices. Several smaller organisations say this is important due to lacking sufficient existing IT expertise which they believe hinders their understanding of the necessary controls – a point also echoed by several Certification Bodies.

Respondents also suggest more workshops, webinars and videos, including case studies, to support this process.

“Clarity needs to be given when a business has an external IT provider that deals with cyber security.”

Current user of Cyber Essentials certification, small employer, private business

“[Cyber Essentials could be improved with] easy access to better support. I think the new Cyber Advisor scheme will help with this. I think it would be good to have video guides also.”

Cyber Essentials Certification Body

3. Reduced cost

Some respondents – notably small organisations and lapsed users of Cyber Essentials – expressed dissatisfaction with the costs associated with Cyber Essentials certification. It was not always clear which costs respondents were referring to (for example costs to implement the technical controls) but some specifically mentioned the cost of assessment and re assessment. Several suggested some form of tiered approach to the assessment cost, such as a special rate for startups, and others felt that reassessment costs ought to be lower.

“Renewal costs are prohibitive to small businesses.”

Lapsed user of Cyber Essentials, medium employer, private business

4. Quality and scrutiny of assessments

Several Certification Bodies and some Cyber Essentials users believe that assessments and audits are not up to standard, and that action should be taken to guard against the risk of false passes.

“There needs to be formal sampled audits of all submissions and a far more robust process to investigate when a Certification Body reports suspicious activity.”

Cyber Essentials Certification Body

5. Synergy with other security schemes

A small number of organisations feel that Cyber Essentials should have greater links with other security schemes, either by standardising criteria between them or accepting the implementation of other security schemes as an acceptable standard. One organisation gave the example of ISO 27001 certification being valid for three years, against which the Cyber Essentials scheme’s annual renewal requirement compared negatively.

"[Cyber Essentials should] automatically qualify for relevant aspects of other certifications through harmonisation e.g. ISO 27001 and by doing this provide a stepping stone to other internationally recognised standards."

Current user of Cyber Essentials, micro employer, private business

Chapter 6 Summary Box

With respect to Cyber Essentials scheme governance, strategic stakeholders say partnership working has increased. They suggest that it could be strengthened by a greater commitment to transparency, sharing information that would benefit all parties, and taking on board feedback with a view to making changes that would serve the greater good.

In terms of scheme implementation, strategic stakeholders (representatives from government and industry) stressed the challenge of the current 'one-size-fits-all' approach where there are quite different challenges to implementing cyber security measures by organisations of different types, sizes and sectors. As such they advocate more in-built flexibilities where this would be possible. The Pathways pilot project (cf. section 1.2) is one example of this.

In relation to consistency of work between Certification Bodies, a minority of stakeholders questioned the appropriateness of Certification Bodies fulfilling the dual roles of assessor and advisor to organisations seeking certification. However, this argument needs to be balanced against the importance users place on the support they get from Certification Bodies and the ultimate goal, which is about building organisations' protection against threats.

The majority of current and lapsed users believe that going through the Cyber Essentials process has improved their cyber security awareness and understanding (71%) and, as a result, they are better able to mitigate cyber security risks in their own organisation (52%).

Just over two thirds (67%) would recommend Cyber Essentials to others. These users, especially registered charities and trusts, view the scheme as cost-effective and accessible. Users that would not recommend Cyber Essentials to others do not typically believe that the controls are applicable or relevant to the workings of their own organisation. This points to a need to consider how, if at all, the controls could be more flexible or adaptable.

Current and lapsed users were asked to what extent they agree that the Cyber Essentials scheme overall represents good value for money. The emerging picture is mixed. While the majority (58%) strongly agree or agree, just over a quarter (26%) are ambivalent and a minority (16%) disagree or strongly disagree. This offers an opportunity to help organisations better understand what they are getting in return for their investment.

Certification Bodies, which were also asked about the scheme's effectiveness and improvement, compliment it for providing an effective and accessible security baseline for certified organisations. However, a key perceived challenge is that users and potential users lack a sufficiently detailed understanding about cyber security. These findings emphasise the importance of more effectively conveying to current and prospective users the importance of cyber security, why they should take it seriously and how Cyber Essentials provides a cost-effective solution to starting that journey.

The majority of Certification Bodies (59%) are very or quite confident that the Cyber Essentials scheme is being delivered consistently by different Certification Bodies, although 36% are not very or not at all confident. Most mentioned differing requirements, standards and capabilities between Certification Bodies as being potential reasons for lack of consistency.

All surveyed organisations were asked in what ways they think the Cyber Essentials scheme could be improved in the future. Suggestions fall into the following five main themes: i) better tailoring and scalability; ii) improvements in communication, guidance and support; iii) reduced cost; iv) quality and scrutiny of assessments; and v) synergy with other security schemes.

7. Non-Users of Cyber Essentials

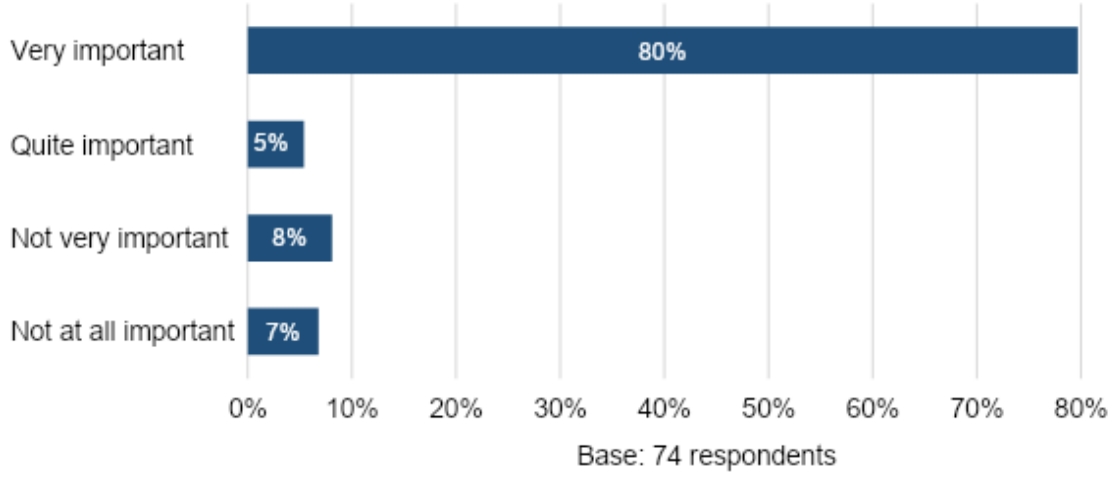
This chapter summarises the findings from a separate small-scale phone survey of users that have never held Cyber Essentials. It explores such factors as the perceived importance of cyber security, as well as awareness and consideration given to taking up Cyber Essentials vis-à-vis other schemes and standards.

Whilst the base numbers are small and findings should therefore be treated with caution, they do offer a valuable insight into whether there is a potentially untapped market for Cyber Essentials. The profile of non-Cyber Essentials survey respondents can be found in Appendix 2 (section A2.2).

7.1 Attitudes and knowledge

Among 74 surveyed organisations that have never held Cyber Essentials, eight in ten consider cyber security very important to their organisation. Of the 15% answering not very or not at all important, all are micro organisations (Figure 31). These businesses could therefore be the hardest to engage in terms of future take-up.

Figure 31 Perceived importance of cyber security (non-Cyber Essentials organisations)



Respondents were asked to provide reasons for their answer. Those stating ‘very or quite important’ are conscious that a cyber attack could cause serious problems for their business. They are committed to keeping their systems safe, secure and up to date, protecting information including user and other personal data, protecting system users and guarding against the possibility of being hacked.

(Very important) “As a website and developmental designer we take IT security very seriously and employ a third party provider to manage all our IT.”

Lapsed user of Cyber Essentials, small employer, private business

“As a manufacturer and wholesaler, we have to secure business and customer accounts from cyber-crime.”

Lapsed user of Cyber Essentials, micro employer, private business

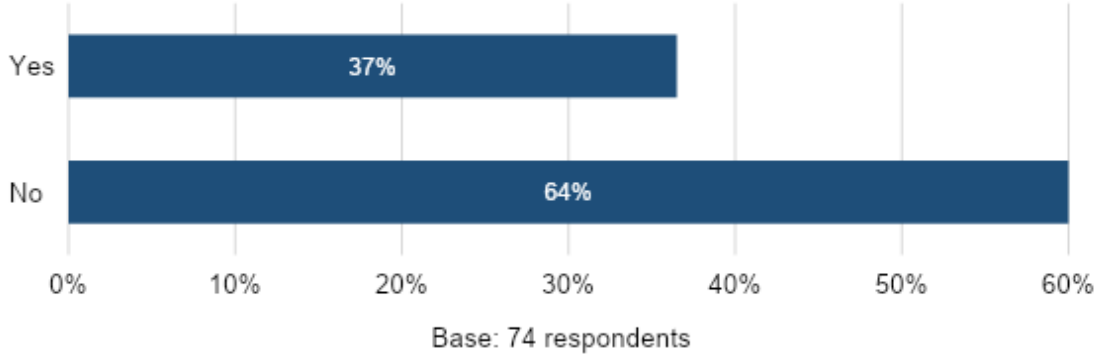
The minority stating ‘not very or not at all important’ mentioned mainly doing business on their phone, doing little business online, using paper-based records, being content to use free internet security software (AVG was specifically referenced) and in one case not trusting the government. These reasons suggest that they either do not feel particularly exposed to an attack or do not consider an attack to be especially consequential for their organisation.

“There are only two people working in the business so we don't need to spend money on advanced cyber security.”

Non-holder of Cyber Essentials, micro employer, private business

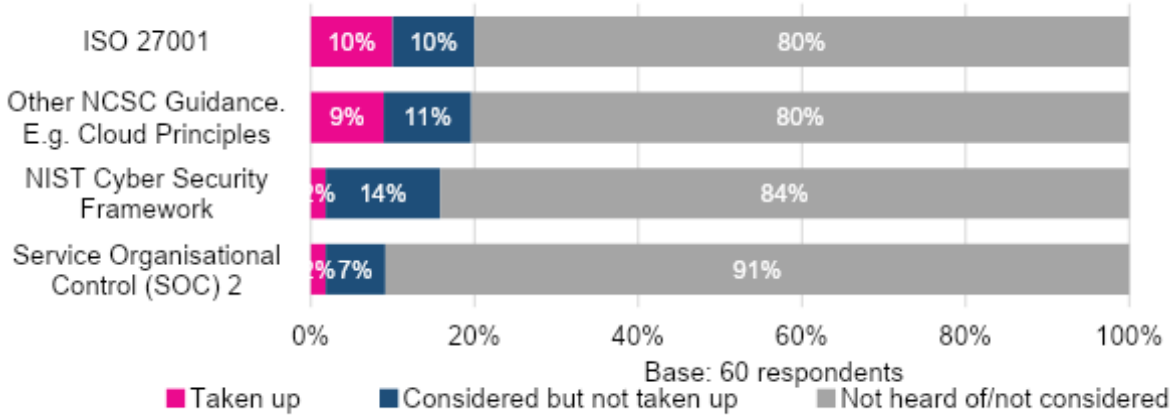
Almost two thirds (64%) of the 74 surveyed organisations that have never held Cyber Essentials had not heard of it prior to taking part in the survey (Figure 32). The result suggests that there could be a viable gap to fill depending on what other arrangements they already have in place (examined further below).

Figure 32 Whether heard of Cyber Essentials (non-Cyber Essentials organisations)



The vast majority of surveyed organisations that have never held Cyber Essentials also report not having heard of other cyber security schemes or standards (Figure 33). This points to a potential target market for Cyber Essentials that may lack cyber security and an understanding of the importance of becoming more cyber secure.

Figure 33 Consideration of other schemes and standards (non-Cyber Essentials organisations)



Respondents that had considered or taken up at least one other scheme or standard were asked for their views on how it compares to Cyber Essentials. Most found this hard to answer and responses did not address the question directly. Other comments showed mixed opinions between respondents, as follows:

- Cyber Essentials is viewed positively as an accepted industry standard
- Cyber Essentials is too costly
- IT is outsourced so others outside the organisation decide what action to take
- Cyber Essentials certification criteria are not compatible with volunteers' ways of working, including BYOD

7.2 Consideration given to Cyber Essentials certification

A small subset of 11 organisations had both heard of and considered taking up Cyber Essentials. Their three most common reasons for doing so are:

- To reassure customers about IT security (11 respondents)
- To improve cyber security and resilience (nine respondents)
- That it was a requirement of their organisation (four respondents)

Specific factors considered **very important** by the majority of these 11 respondents are:

- Establishing the expertise needed to become Cyber Essentials certified (ten respondents)
- Establishing the necessary resources and inputs needed to become Cyber Essentials certified (seven respondents)
- Understanding the benefits of becoming Cyber Essentials certified (seven respondents)

Seven out of these 11 respondents consider the cost of certification to be either very or quite important, with the remaining four saying not very important.

When asked what other factors (if any) were important to their organisation when considering taking up Cyber Essentials, unprompted answers are:

- Cost and time involved
- Ensuring compatibility with volunteer workers and their personal devices
- Meeting user and patient needs
- Password authentication
- Safeguarding the business
- Working to an industry accepted standard

The main reasons for these 11 organisations not taking up Cyber Essentials are that they consider it potentially too time-consuming or lacking compatibility with different devices. These are issues that marketing, information and guidance could help to address where there are misconceptions.

7.3 Guidance and support

The 11 surveyed organisations that have never held Cyber Essentials certification but had considered taking it up were asked which, from a range of sources of Cyber Essentials information and guidance, they had come across or used. The top three answers point to trusted sources being used and are:

- Government website, including DCMS and NCSC (eight respondents)
- Certification body website (four respondents)
- Certification body social media channels (four respondents)

As to whether these 11 organisations had reasons to ask questions or seek help when considering becoming Cyber Essentials certified, responses are divided between those saying yes (four), those saying no (four) and those unable to recall (three).

Among the four saying that they sought help or asked questions, channels of interaction included the Certification Body, IASME (customer service email and website) and NCSC website.

Two of those four organisations found that support very helpful, one quite helpful and one was unsure whether it was helpful or not. Either way, these organisations were evidently not convinced that Cyber Essentials was right for their organisation based on the information they had initially accessed or the help they had obtained.

Eight non-Cyber Essentials organisations rated on a scale from 1 (not at all clear) to 10 (perfectly clear) how clear they considered specific aspects of online information and guidance about the Cyber Essentials scheme. The mean scores are moderate, as follows:

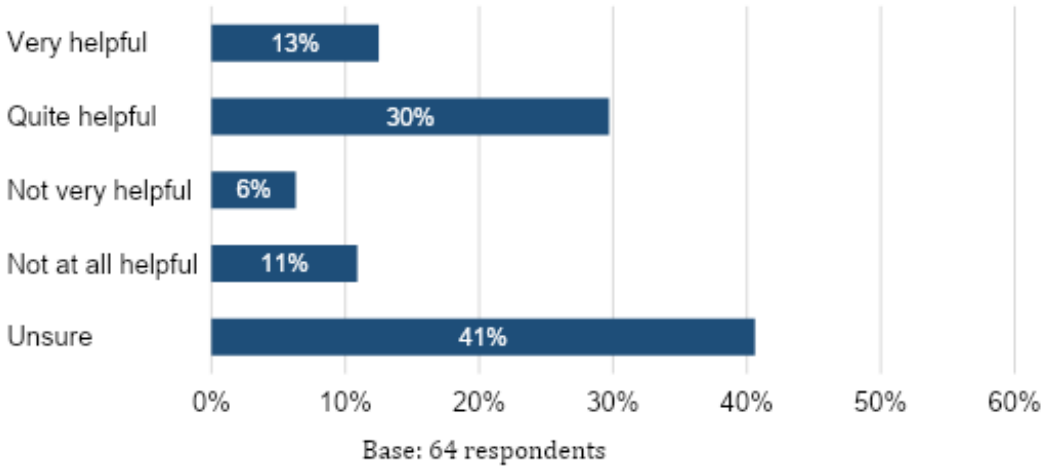
- Features and benefits of the Cyber Essentials scheme (7)
- How to obtain Cyber Essentials certification (7)
- Differences between Cyber Essentials and Cyber Essentials Plus (6)
- Where to get additional help and support about Cyber Essentials (6)

Eleven non-Cyber Essentials organisations that had heard of or considered taking up Cyber Essentials were asked how the information and guidance could be improved or made more accessible.

The majority (six) feel it could be clearer and four were unsure where to find existing online information and guidance. This could be due to several issues, such as insufficient detail contained in the information they have been able to find or not knowing which, from a range of sources, to trust or where to start.

With reference to NCSC's preparation to roll out a new Cyber Advisor Scheme offering assured cyber security consultancy services to SMEs and helping them to achieve a minimum standard of security, non-Cyber Essentials SMEs were asked how helpful they feel this would be to their organisation. More than four in ten (43%) believe this would be very or quite helpful, although a similar proportion are unsure, suggesting that awareness and understanding is currently low (Figure 34).

Figure 34 Likely helpfulness of the Cyber Advisor scheme



All non-Cyber Essentials organisations were asked what would be needed for their organisation to consider obtaining Cyber Essentials certification in the future (Figure 35). A range of answers were given, with the most common – all of which are reactive drivers – being:

- If it is required by a contract we want to work on (58%)

- If it is a requirement of our customer(s) (47%)
- If senior leaders in our organisation asked for it (35%)

Figure 35 What would be needed to make Cyber Essentials attractive (non-Cyber Essentials organisations)

Finally, when asked if they had any final comments, many non-Cyber Essentials users indicated that they would be interested in finding out more about Cyber Essentials, had an open mind about it, would be willing to discuss it with their third-party IT providers (as appropriate) and in some cases are considering reviewing their cyber security needs in the near future. These responses indicate potential opportunities to improve awareness and understanding of Cyber Essentials in the market, including its value.

Chapter 7 Summary Box

Among 74 surveyed organisations that have never held Cyber Essentials, eight in ten consider cyber security very important to their organisation. However, of the 15% answering not very or not at all important, all are micro organisations. These businesses could therefore be the hardest to engage in terms of future take-up.

The minority stating ‘not very or not at all important’ mentioned mainly doing business on their phone, doing little business online, using paper-based records, being content to use free internet security software and in one case not trusting the government.

Almost two thirds (64%) of the 74 surveyed organisations that have never held Cyber Essentials had not heard of it prior to taking part in the survey. The vast majority had also not heard of other specified cyber security schemes or standards, which points to a potential target market for Cyber Essentials that may lack cyber security and an understanding of the importance of becoming more cyber secure.

Among 11 of these organisations that had hitherto heard of and considered taking up Cyber Essentials, their main reasons for not taking it up were that they considered it too time-consuming or lacking compatibility with different devices. These are issues that marketing, information and guidance could potentially help to address where there are misconceptions.

All 74 organisations were asked what would be needed for their organisation to consider obtaining Cyber Essentials certification in the future. The top three answers are primarily reactive, including: if it is required by a contract we want to work on (58%), if it is a requirement of our customer(s) (47%) and if senior leaders in our organisation asked for it (35%).

Many non-Cyber Essentials users indicated that they would be interested in finding out more about the scheme, had an open mind about it, would be willing to discuss it with their third-party IT providers (as appropriate) and, in some cases, are considering reviewing their cyber security needs in the near future. These responses indicate potential opportunities to improve awareness and understanding of Cyber Essentials in the market, including its value.

8. Conclusions and Recommendations

8.1 Conclusions

Role and purpose of Cyber Essentials

1. **The most common reasons for adopting Cyber Essentials are reactive rather than proactive, risking the scheme being perceived as a "hoop to jump through" in order to fulfil contract requirements.**

   While surveyed organisations take up Cyber Essentials for a variety of reasons (Figure 6), four of the five main drivers are external and only one is focused on the value that being more cyber resilient can bring to the user's organisation (Figure 7). The scheme has built prominence in recent years through being a mandatory condition of certain government contracts; indeed, 34% of surveyed users cite public sector contract requirements as their single main reason for first becoming Cyber Essentials certified. Ideally, a greater proportion of organisations would adopt Cyber Essentials for its intrinsic value in building cyber resilience.

   Furthermore, in cases where organisations hold more than one solution, e.g. Cyber Essentials in tandem with ISO 27001 (Figure 5), this could mean that Cyber Essentials is complementary to other products, or it could mean – in some cases – that organisations have no choice but to adopt both, especially where Cyber Essentials is mandated in government contracts.

   These issues are leading to some organisations perceiving Cyber Essentials as a means to an end, over and above its function as mitigating potentially organisation-damaging cyber threats.

2. **Stronger focus should be placed on promoting the dangers and threats associated with conducting business online, so organisations can appreciate why a cyber security solution such as Cyber Essentials is important.**

   There is a case for DSIT, IASME and NCSC to do more to help organisations understand the dangers and threats that the Cyber Essentials scheme is designed to mitigate. This is backed up by the fact that more than eight in ten surveyed users consider understanding the benefits of becoming Cyber Essentials certified to be important to their organisation (Figure 8).

   Where organisations can more fully appreciate the consequences of not being cyber secure, and buy into the value that Cyber Essentials offers besides being a stepping-stone to winning a contract, this has the potential to stimulate growth in uptake, reduce attrition and help boost the UK's cyber resilience.

   At the same time, it is important that organisations are equipped with sufficient knowledge to make an informed decision about which cyber security solution is right for them. Almost half (46%) of lapsed users rated the quality and suitability of information and guidance to be poor (section 5.2), suggesting that many organisations are struggling to see why they should justify the cost and time to maintain certification.

User experiences

3. **There is evidence that the certification process is making a positive difference to users' cyber behaviours, although there is a mixed picture concerning perceived value for money.**

   There is evidence that the scheme is making a positive difference to users' cyber security behaviours. The majority of surveyed users (71%), including organisations across all size-bands, report improved cyber security awareness and understanding as a result of the certification process. Furthermore, a small majority (52%) say they feel better able to mitigate cyber security risks in their own organisation (Table 14).

   Other key strengths of the scheme as perceived by stakeholders and users are that it is affordable, easily attainable, cost-effective, accessible and offers a good baseline for security (Chapter 5).

   However, the picture is mixed in terms of perceptions of overall value for money. While the majority (58%) strongly agree or agree that the scheme offers value for money, there is a significant difference between the proportion of large organisations in agreement (61%) and the proportion of micro organisations in agreement (less than half – 46%). Whilst the cost, time and resources associated with implementing Cyber Essentials go beyond the basic assessment cost, this suggests a need to review the scheme's pricing structure.

4. **The cost and time inputs needed to go through the Cyber Essentials certification process can vary widely between organisations, with high costs (including, but not limited to, scheme pricing) potentially affecting take-up and retention of Cyber Essentials certification.**

   The evaluation has been able to estimate the average cost and FTE days for different sizes of organisation to go through the certification process, which for micro businesses stands at £1,894 and four days, and for large businesses stands at £31,459 and 23 days once outliers are removed from the data. High numbers of days are accounted for through activities such as planning and subsequent updating of hardware and software, conducting gap analyses and remediation plans, remediation activity, final assessment, evidence gathering etc. (section 5.1).

   While cost and time are not among the main difficulties cited in relation to the customer journey (section 5.4), reducing the costs associated with certification is a common suggestion for improvement (section 6.4). Furthermore, cost and time are both among the top three reasons why lapsed Cyber Essentials users did not renew their certification (Figure 11). For some organisations therefore, these factors are clearly an issue and could pose a risk to take-up and retention.

Meeting the technical controls

5. **Some of the largest and smallest organisations face substantial yet quite different obstacles to meeting the technical controls, indicating inherent challenges to the scheme's prescriptive (rather than risk-based) and one-size-fits-all concept.**

For the largest organisations, the controls can prove difficult to implement across a large network, especially where legacy hardware and software is prevalent. This takes time, considerable expense and the will to instigate changes.

For the smallest, meeting the technical control requirements of the Cyber Essentials scheme can be a particular challenge given the perceived cost, time and expertise required to do so – especially where these organisations lack a dedicated IT resource or do not have a third party IT consultancy in place (section 5.5).

The Cyber Essentials scheme therefore walks a difficult path in terms of meeting the needs of different organisational types, sizes and settings. However, trying to change course could also be problematic for a number of reasons.

Firstly, there is evidence that Cyber Essentials is valued by organisations of different sizes and that the scheme is already challenging organisations in different ways (Chapter 6). There could also be a reduction to future uptake if Cyber Essentials were to align itself overtly with certain types or sizes of organisations over others.

Secondly, some evaluation participants suggest that the scheme needs to move away from a 'one-size-fits-all' approach in favour of becoming more risk-based or flexible. This is considered especially important for settings such as academia where there is a high prevalence of BYOD and a perception that meeting control requirements will not be manageable (section 5.6). However, a risk-based approach would be difficult as the scheme is fundamentally a prescriptive rather than risk-based product.

The solution would therefore seem to lie in developing more flexible approaches, which are already being tested and could provide a viable way forward. IASME's current work with NCSC as part of a Pathways pilot project (due to conclude in the second quarter of 2023) is one step towards tackling this issue based on testing outcomes rather than specific controls and using a simulated attack scenario (section 1.2).

Alongside this, there is a case for DSIT, NCSC and IASME to continue to work closely with partners that actively promote the benefits of academic organisations taking steps to becoming more cyber resilient. This would help to convey that message more clearly and introduce a shift in behavioural change.

6. **Updates to the technical control requirements are clearly important but communications about changes – especially major updates – appear to be inadequate and are not sufficiently timely for organisations to plan ahead.**

Firstly, evidence is convincing that the Cyber Essentials scheme needs to remain agile and responsive to ever-changing threats in order to maintain credibility and trust (section 5.5). However, there are concerns about how updates and changes to control arrangements are communicated, suggesting that messaging needs to be more proactive and timeous (section 5.5 and Figure 22).

A more coordinated communications plan should therefore be considered since giving organisations the time to plan for changes is important for ensuring they feel able to meet recertification requirements. This could be supplemented by a clearer mechanism or central web page for publishing updates with notifications sent to all users.

The case for some sort of action here is further evidenced by the fact that 'difficulty keeping up with changing controls' was mentioned by almost a third (32%) of users as at least one reason why their Cyber Essentials certification lapsed (Figure 11).

Information, guidance and marketing

7. Existing information and guidance could be improved with better tailoring and simplification for different types and sizes of organisation.

Cyber Essentials users access information about the scheme from a range of trusted sources, most prominently IASME, the government (including NCSC and former DCMS) as well as their Certification Body (section 4.1). Two thirds of users also said that they needed some form of help and support and the vast majority (90%) found this support helpful (section 4.2).

However, current information and guidance to aid the certification process could be better tailored (50% of respondents), more detailed (42%) and clearer (41%) (Figure 18). This would help different types and sizes of organisation to make a more informed decision as to whether Cyber Essentials is in their best interests. Stakeholders also emphasised that there should be greater clarity around the difference between the CE and CE Plus schemes, especially to eliminate the risk of misconceptions that CE Plus offers a stronger level of security once obtained.

It should be noted that IASME has already taken steps to address this, including through recent and further planned updates to the assessment questions.

8. There is a clear market opportunity for Cyber Essentials among organisations that have never been certified under the scheme and which consider cyber security very important.

Four in five surveyed organisations that have never held Cyber Essentials consider cyber security to be very important to their organisation (Figure 31) but almost two thirds (64%) had not heard of the scheme prior to taking part in the survey (Figure 32). Many of these, including organisations of all sizes, had also not heard of or considered schemes and standards such as ISO 27001 and NIST (Figure 33).

The research has also identified that Cyber Essentials is increasingly becoming a talking point among trade bodies and large organisations through blog articles, published reports and interactions between different bodies and IASME (desk research and section 5.5).

Given the identified need to educate organisations more prominently about the importance of having cyber security arrangements in place, there could be an opportunity for TV, radio and social media adverts with harder hitting messages about the risks and potential consequences of not taking action. There is also an opportunity to engage more directly with intermediaries such as IT support sector businesses.

Scheme robustness

9. Anecdotal evidence points to pockets of weakness in the rigour of the Cyber Essentials assessment process. This could be overcome through education and

guidance aimed at users in relation to cyber threats, risks and potential consequences, as well as the benefits of becoming more cyber resilient.

There are some concerns from stakeholders that the motivation of Certification Bodies to pass users in return for the resulting fee risks creating pockets of 'perverse behaviours'. There are also some concerns raised by Certification Bodies that some users are making false statements in order to pass certification (sections 5.1 and 5.4).

The extent of such practice is unknown and raises the question as to whether the scheme ought to be strengthened in some way, for example through additional spot checks or audits. That said, there is a risk that such an approach may be perceived as draconian, especially as there is a strong argument to say that Cyber Essentials is there to help organisations and that it is in organisations' own interests to complete the assessment as intended. Instead, there is a stronger case to provide more education around cyber threats, risks and potential consequences, and the benefits of becoming more cyber resilient. Arguably a mindset change is needed and this can take time.

8.2 Recommendations

The following recommendations are aimed at DSIT, IASME and NCSC to consider as part of a coordinated approach. Not all components of these recommendations may be appropriate or desirable depending on feasibility but they have been developed to respond to the main issues raised through the research.

1. **Increase basic awareness and understanding about security threats and provide users with an informed choice about the most appropriate solution for them**

    a. Help to build a more foundational awareness among organisations of the importance of being cyber secure, the potential impact and consequences of a cyber security breach, and the need to take action to mitigate that risk. This applies to current users and non-users.

    b. Develop more and better information about the features and benefits of the Cyber Essentials scheme. Consider providing comparison tables to show how the scheme compares with off-the-shelf anti-virus software, as well as other schemes and standards such as ISO 27001. This will help potential users to make a fully informed decision as to whether Cyber Essentials is appropriate to their organisation.

    c. Consider not mandating Cyber Essentials in public sector procurement contracts where suitable alternatives are already held.

2. **Improve information, tools and guidance aimed at current and potential users**

    a. Provide more and better information to articulate the differences between the standard and Plus schemes in order to:

        - Reduce the risk of misconceptions that Plus offers a stronger level of security

        - Help organisations to determine (e.g. through an interactive question flowchart) which would be the best solution for their organisation

b. Produce more information and training resources via webinars, videos and infographics to help convey key aspects of the Cyber Essentials scheme, including:

   - Features and benefits
   - How the process works in practice
   - Examples of the likely resource inputs and time that could be involved for different types and sizes of organisation

c. Improve the clarity of information and guidance in several key areas, notably:

   - Simplifying language and terminology (such as in explanatory notes)
   - Being clearer about which controls apply to different types of devices, including BYOD

d. Produce best practice case studies to show how organisations of different types and sizes have progressed through the customer journey, overcome challenges and achieved particular outcomes. This could extend to include these organisations' top tips.

e. Consider introducing an online chat interface to help users with frequently asked questions.

f. Deploy user testing to help improve the clarity of assessment questions by checking for and reducing instances of duplication and any unnecessary complexity.

3. Provide more tailored information to different types and sizes of organisation, and consider more targeted and high-profile marketing and communications

a. Develop and roll out more tailored and nuanced information and marketing to different types and sizes of business to explain the benefits of becoming Cyber Essentials certified. This could include tools to help organisations self-assess whether Cyber Essentials is right for their organisation and to manage their expectations from the outset.

b. Consider a targeted marketing campaign to other key enablers in the cyber security space, such as IT support sector businesses. With their buy-in, these organisations are well placed to promote it further to the organisations they work with. Other avenues of promotion could include trade bodies and online or offline forums aimed at directors and IT specialists.

c. Building on the existing Cyber Aware campaign, consider producing and running hard-hitting media adverts about the risks of a cyber breach – via television, radio or social media depending on the costs involved. These could be similar in style to past drink driving campaigns, pointing to the Cyber Essentials scheme as a solution to the main threats.

4. **Consider the feasibility of adapting aspects of the Cyber Essentials scheme to be more responsive to current user needs.**

    a. Build in flexibilities to the Cyber Essentials scheme where possible, especially those which would help large organisations and academic institutions to meet the technical controls. The Pathways pilot project may prove one suitable way forward depending on outcomes due in the second quarter of 2023.

    b. Put in place a coordinated communications plan to more frequently and timeously distil information through Certification Bodies about changes and updates to control arrangements. This is especially the case for major (rather than minor) updates, noting of course that they tend to be less frequent. This will give Cyber Essentials users time to prepare and plan in advance.

    c. Explore further the relative merits of increasing the length of certification to three years, albeit with annual audits comparable to ISO 27001. A key argument in favour is that it could help to alleviate the issue of annual cost and resource input but a key argument against is how organisations would ensure they meet the latest control updates.

    d. Allow more time for organisations to provide additional information in response to requests during the assessment process. This follows feedback that the current 48-hour window is too short.

    e. Based on evidence that smaller organisations are more cost sensitive, and that cost is a key reason why Cyber Essentials certification lapsed, review the scheme's pricing structure. This could involve exploring further whether the fee for assessment is a barrier to certification, or considering a more nuanced approach to assessment fees, such as a special rate for startups or lower reassessment costs at annual renewal.

5. **Commit to strengthening scheme robustness and transparency**

    a. Consider how the scheme is positioned in relation to other NCSC schemes to ensure there is no risk of competing narratives.

    b. Actively encourage organisations to provide regular feedback to IASME and NCSC on how the scheme could be improved.

    c. Continue to work collaboratively with Certification Bodies towards greater consistency, for example by providing clarity on how they are expected to undertake assessments, the degree of flexibility allowed and the level of advice and support they are expected to provide alongside their assessment role.

    d. Consider an education campaign, potentially combined with more robust protocols to guard against organisations potentially providing false information in order to gain Cyber Essentials certification. This could be undertaken through a more regular system of spot checks, audits or penalties.

Appendix 1. Feasibility of a Future Impact Evaluation

An impact evaluation of the Cyber Essentials scheme is eminently feasible in principle given the length of time the scheme has been running, including three years since the last major structural change to delivery with IASME as the sole Accreditation Body.

This time factor is an important consideration since it allows outcomes and more lasting impact to have already been felt, including those which may not be tangible or easily quantifiable but that an impact evaluation could tease out.

Steps and considerations for conducting an impact evaluation of the Cyber Essentials scheme are set out below.

Establishing an evaluation steering group

A collaborative approach will be valuable for establishing the scope and parameters of an impact evaluation. This should draw together organisations with: i) a strategic and vested interest in framing the evaluation questions; ii) access to necessary secondary data sources; and iii) the ability to unlock and help broker access to key audiences for primary data collection.

Developing an evaluation framework

The starting point for a robust impact evaluation is the development of an evaluation framework based on 'theory of change' methodology. This should draw on the principles and concepts set out in HM Treasury's Green Book and Magenta Book and tailored to the specific context and nature of the scheme.

The framework should set out a plan for measuring impact, including a proposed methodology to collect, analyse and report on available data. It should help the government to: i) reflect in a structured and logical way on the difference the scheme has made; and ii) be capable of articulating a baseline along with desired outcomes and impact.

The framework should articulate:

- The problem that the Cyber Essentials scheme seeks to solve
- What the Cyber Essentials scheme seeks to achieve
- Existing evidence base available (to inform the baseline)
- Evaluation timeframe (including for data collection)
- Measures upon which to base the evaluation
- Indicators against which the measures should be assessed (which could include quantifiable and direction of travel indicators)
- Evidence needed to provide an assessment against the indicators

- Which audiences to involve
- Most appropriate data collection methods for the respective indicators
- How the results should be analysed and reported

A logic model would be a well-suited approach to constructing the theory of change that seeks to establish inputs, processes, outputs (shorter-term and more tangible), outcomes (over time, including less tangible elements) and impact (lasting and aligned with strategic objectives).

It is noted that a theory of change and logic framework has already been developed for Cyber Essentials, as part of a collaborative effort between (former) DCMS, IASME and NCSC. This should be reviewed and refined (as appropriate) in light of the above and with due consideration to suggested measures and associated considerations as set out below.

In order to assess the difference that the Cyber Essentials scheme has made, a counterfactual should be established. This involves comparing observed outcomes to those that would have been expected if the Cyber Essentials scheme had not been implemented. This could be achieved using one of several optional approaches:

1. **Using a comparison group** – to compare quantitative and qualitative data between Cyber Essentials and non-Cyber Essentials certified organisations, or organisations that have and have not implemented the technical controls

2. **Establishing a baseline counterfactual** – gathering data from organisations prior to them becoming Cyber Essentials certified and revisiting these organisations after becoming Cyber Essentials-certified (this would ideally involve waiting at least 12 months, and ideally longer, for impact to be felt)

3. **Constructing a quasi-experimental approach, involving developing a logically constructed counterfactual** – using baseline statistics and perspectives to develop a reasonable estimate of what would have happened without Cyber Essentials having been implemented

Option 1 would appear to be the most reasonable in this case given that it would allow an impact evaluation to be conducted in a relatively short timescale and given that the Cyber Essentials scheme has already been running for many years.

Establishing contribution and attribution

Determining complete causality is extremely difficult through evaluation logic models. Instead, a robust view of contribution and attribution should ideally be assessed by distinguishing between gross and net outcomes. The former looks at observable changes as outputs that are easily measurable through specific indicators, e.g. relating to tangible outcome measures.

Net outcomes or effects, i.e. that may be solely attributable to the Cyber Essentials scheme, should ideally be isolated from wider contextual variables. These might include how well Cyber Essentials contributes to productivity, business resilience and cyber maturity through

the use of technical controls, and what a direct positive impact would look like (discussed further below).

Eliminating or controlling confounding variables would best be achieved in this case through detailed qualitative primary data collection. Examples of confounding variables have already been identified as part of the existing Cyber Essentials theory of change, using as a set of assumptions – summarised below:

- That outcomes are caused only by gaining the Cyber Essentials certificate, rather than other sources (e.g. ISO 207001, NIST etc.)
- That no other security improvements are made beyond those needed to achieve Cyber Essentials
- That Cyber Essentials measures make organisations more secure

Possible criteria for impact measures

It is important to identify how positive or negative outcomes of the Cyber Essentials scheme can be defined and measured. This could involve looking at quantitative or more qualitative measures, or both. The process evaluation involved scoping with strategic stakeholders how the scheme's impact could be assessed, as well as critically reviewing existing theory of change measures for the Cyber Essentials scheme. Examples of quantitative measures are set out below, including associated considerations:

Quantitative measures – suggestions	**Additional considerations**
Comparison of the number of reported cyber security breaches between businesses which have and have not implemented technical controls	This would require self-reported data on cyber breaches from Cyber Essentials users and non-Cyber Essentials organisations. However, some may be reluctant to provide this and it could be difficult to obtain at scale for a robust assessment. Another option would be to obtain breach data from a higher level source that collects attacks, but this could be problematic if breaches are under-reported.
Whether there has been a reduction in the number of successful attacks over a given period	A difficulty here is that attacks may be infrequent or may never have previously been experienced by an organisation. Added to that, an organisation may not want to disclose details of a cyber attack. A wider conceptual challenge as noted in the Review of Cyber Essentials influence on cyber security attitudes and behaviours in UK organisations, is that improved cyber security awareness (for example through obtaining Cyber Essentials certification) can mean that organisations have a greater awareness of breaches and attacks, which in turn can have the effect of making it appear that the situation is worsening (i.e. attack frequency has increased) when in fact it may mean that

	previously attacks were undetected and organisations have since improved their awareness.
Number of successful and unsuccessful cyber attacks over a given period Where an attack has happened, assessing whether the Cyber Essentials technical controls would have prevented the attack	These may be difficult to measure at an organisation level and would likely require specialist technical input, expertise and access to technical data.
Analysis of claims data from cyber insurance, comparing data relating to organisations with and without Cyber Essentials	Some organisations who achieve Cyber Essentials are provided with the offer of cyber liability insurance as part of their certification through IASME. Where Cyber Essentials certification status is used by providers in determining policy premiums, the data may be a usable source. However, the viability of this approach would depend on factors such as: i) the proportion of Cyber Essentials users that take out the insurance; ii) the number of valid claims; and iii) insurers being able and willing to provide the anonymised data.

Below are examples of qualitative impact measures (based on gathering perceptions) that could be used to inform primary research with Cyber Essentials organisations. Some of these could be adapted to compare the perceptions of Cyber Essentials-certified and non-Cyber Essentials organisations. It would also be useful for the evaluation to include all sizes of organisation, including those new to Cyber Essentials and those renewing – capturing the length of time certified since this may influence the extent to which impacts are likely to have been felt.

- Perceived likelihood of a cyber security breach occurring in the organisation
- Where Cyber Essentials technical controls have been implemented, perceived confidence in the controls at preventing a cyber security breach from occurring
- Perceived difference that Cyber Essentials makes to an organisation's financial turnover by enabling it to enter into contracts for which Cyber Essentials is a mandatory requirement
- Perceived financial impact of a hypothetical breach - would likely need to be measured in broad terms (e.g. high/medium/low) rather than in monetary terms, which would be very difficult to estimate since attacks can vary in severity
- Perceived reputational impact of a hypothetical breach if the details were to be made public (would likely need to be measured as a Likert-scale question in terms of significance of impact)

- Perceived impact of Cyber Essentials on the confidence of user customers and investors (may be difficult to gauge accurately)
- Extent of agreement that the technical controls are helping to mitigate cyber security risks in their organisation and (where applicable) their supply chain
- Extent to which Cyber Essentials has increased organisations' awareness, knowledge and attitudes regarding cyber security
- Extent of confidence in the cyber resilience of the organisation as a result of becoming Cyber Essentials certified
- Extent and nature of organisational behavioural changes as a result of implementing Cyber Essentials
- Whether or not organisations apply technical controls beyond what is required for Cyber Essentials
- Other actions taken such as development and implementation of local policies, procedures and incident response arrangements

It should be noted that comparing perceptions of Cyber Essentials and non-Cyber Essentials organisations would require disentangling confounding variables in order to determine net outcomes as mentioned above. For example, it will be important to determine whether or not each non-Cyber Essentials organisation has already implemented the technical controls through other routes or has other cyber security schemes in place.

Identifying sources and methods of data collection

Consideration should be given to what sources are available to use against the indicators, what the limitations and gaps are within those sources, and what evidence should be gathered through new primary approaches.

For an impact evaluation of the Cyber Essentials scheme, it is recommended that a combination of approaches are used – namely drawing on existing secondary sources and deploying primary research methods.

Firstly, this process evaluation has already established that there is a limited body of academic literature and evaluative reports which could be combined with survey data to inform an impact evaluation.

Secondly, statistically robust primary data collection via surveys of current Cyber Essentials users and non-Cyber Essentials certified organisations could be carried out using questions aligned to the precise evaluation questions and indicators. If desired, in-depth qualitative research via online or offline workshops, or in-depth interviews could supplement or replace a survey. This might depend on budget, timescales, the types of questions being asked and their focus.

This process evaluation has already established that mechanisms exist for reaching Cyber Essentials users (online via IASME and Certification Bodies) and non-Cyber Essentials

organisations (undertaken via online or phone methods by using a suitable commercially available sample frame compliant with relevant data protection legislation).

Accessing data on Cyber Essentials users is of course dependent on relationship building with the relevant data controllers, as well as ensuring that the timing of the proposed data collection does not conflict with other routinely scheduled research and evaluation activity. This is important to avoid over-burdening the target audience such that it might cause reputational damage or lead to a lower than desired response rate. IASME, for example, conducts annual surveys of Cyber Essentials users usually in the first quarter of each year, which should be factored into planning and design.

Potential costs

At this stage it is difficult to estimate the potential cost of an impact evaluation since this will largely depend on which components should be included for any contractor, for example:

- Framework development
- Logic model review and redevelopment, including associated indicators
- Question design
- Secondary research
- Primary research (including audiences such as stakeholders, Cyber Essentials users and a comparison group of non-users)
- Target number of responses needed from each group (a minimum of 400-500 per group would be recommended for a robust survey)
- Nature and frequency of analysis, reporting and updates required

Phone-based survey work is much more costly than online survey work and would undoubtedly be required for independently sourcing and interviewing organisations that are not Cyber Essentials-certified.

An online survey (cheaper than a phone survey) could be utilised for reaching out to Cyber Essentials-certified organisations, assuming IASME and the Certification Bodies are willing to be involved as conduits for distributing the survey link to their users. It would be helpful if advance buy-in and approximate timings could be agreed with IASME to be sure this approach would be feasible.

There is also the question of the extent and potential reach of desk research and associated analysis, including whether this should be limited to statistical datasets or a wide range of reports and academic sources, and whether some or all of these would be supplied to the contractor and whether independent sourcing is required.

The matter of scope and costing would therefore be subject to further discussion to help refine this further. Factoring in all of the above and in the interests of ensuring a robust study, we would advise not setting a budget for any future impact evaluation below £120K.

Appendix 2. Survey respondent profiling data

A2.1 Certification bodies, current and lapsed users

The tables below set out survey respondent numbers by cohort that took part in this evaluation.

Relationship to the Cyber Essentials scheme

Current user of Cyber Essentials certification	528
Lapsed user of Cyber Essentials certification (but not currently)	47
Cyber Essentials Certification Body (Certification Body)	95

Size-band (excludes Certification Bodies)

Micro (< 10 staff)	179
Small (10-49 staff)	159
Medium (50-249 staff)	133
Large (250+ staff)	104

Region where organisation based

East of England	48
East Midlands	39
London	110
North-East	26
North-West	50
South-East	122
South-West	89
West Midlands	67
Yorkshire and The Humber	50
Scotland	36
Wales	26
Northern Ireland	7

Type of organisation (excludes Certification Bodies)

National or local government (including department/body/agency)	6
Academic institution	44
Private business	475
Non-governmental organisation (NGO)	5
Registered charity/trust	37
Other	8

Industry sector (excludes Certification Bodies)

Agriculture, forestry and fishing	2
Mining and quarrying	0
Manufacturing	28
Utilities	7
Construction	21
Wholesale and Retail Trade	14
Transportation and Storage	11
Accommodation and Food Service	1
Information and Communication	142
Financial and Insurance	19
Real Estate	10
Professional, Scientific and Technical	132
Administrative and Support Service	13
Public Administration and Defence	12
Education	77
Human Health and Social Work	33
Arts, Entertainment and Recreation	6
Other Service Activities	31
Activities of Households as Employers	0
Other	16

Responses classified as ‘other’ include: advice agency, multi-sector, charity, children and family work, community sector, defence and retail, environmental, healthcare, project management and security.

Financial turnover (excludes Certification Bodies)

Less than £250,000	91
£250,000 to £499,999	49
£500,000 to £999,999	65
£1m to £2.9m	135
£3m to £4.9m	49
£5m+	186

Job function of respondent (excludes Certification Bodies)

Owner/manager	248
IT/information security specialist	258
HR representative	4
Legal/compliance representative	16
Administrative representative	21
Third-party IT or information security support provider	8
Other	20

Job roles classified as ‘other’ include: associate, compliance, data manager, director (industry solutions), director (operations), finance controller, marketing manager, chartered engineer, quality manager, service delivery manager, technical director.

A2.2 Organisations that have never held Cyber Essentials

Size-band

Micro (< 10 staff)	19
Small (10-49 staff)	24
Medium (50-249 staff)	21
Large (250+ staff)	10

NUTS1 region where organisation based

East of England	9
East Midlands	9
London	13
North-East	1
North-West	7
South-East	8
South-West	6
West Midlands	5
Yorkshire and The Humber	5
Scotland	3
Wales	7
Northern Ireland	1

Type of organisation (excludes Certification Bodies)

National or local government (including department/body/agency)	0
Academic institution	6
Private business	66
Non-governmental organisation (NGO)	0
Registered charity/trust	2
Other	0

Industry sector (excludes Certification Bodies)

Agriculture, forestry and fishing	1
Mining and quarrying	0
Manufacturing	16
Utilities	4
Construction	8
Wholesale and Retail Trade	10
Transportation and Storage	1
Accommodation and Food Service	1
Information and Communication	10
Financial and Insurance	4
Real Estate	1
Professional, Scientific and Technical	6
Administrative and Support Service	1
Public Administration and Defence	0
Education	6

Human Health and Social Work	2
Arts, Entertainment and Recreation	2
Other Service Activities	1
Activities of Households as Employers	0
Other	0

Financial turnover (excludes Certification Bodies)

Less than £250,000	12
£250,000 to £499,999	4
£500,000 to £999,999	6
£1m to £2.9m	12
£3m to £4.9m	17
£5m+	23

Job function of respondent (excludes Certification Bodies)

Owner/manager	21
IT/information security specialist	49
HR representative	0
Legal/compliance representative	2
Administrative representative	2
Third-party IT or information security support provider	0
Other	0