Cabinet Office

Procurement Policy Note: Updates to the Cyber Essentials Scheme

Action Note 09/23 September 2023

Issue

1. Cyber Essentials is a Government backed scheme to help businesses of any size protect themselves against a range of the most common cyber attacks and to demonstrate their commitment to cyber security. To ensure appropriate cyber security controls are in place and reduce cyber security risks in supply chains, since 2014 the government has required suppliers bidding for certain types of public contracts to hold Cyber Essentials or Cyber Essentials Plus certification (or demonstrate that equivalent controls are in place).

2. This Procurement Policy Note (PPN) sets out the actions In-scope organisations should take to identify and mitigate cyber threats for certain types of contracts, along with resources to support implementation.

Dissemination and Scope

3. The contents of this PPN apply to all Central Government Departments, their Executive Agencies and Non-Departmental Public Bodies, and NHS bodies, and are referred to in this PPN as 'In-scope organisations'.

4. This PPN replaces PPN 09/14.

5. Please circulate this PPN within your organisation, particularly to those with a commercial, procurement and/or contract management role. This PPN should also be of interest to those working in Cyber Security, Information Security and the Digital, Data and Technology Profession. Other public sector bodies may wish to apply the approach set out in this PPN.

Timing

6. In-scope organisations should implement this PPN within three months of its publication date.

Action

7. In-scope organisations must ensure that effective and proportionate cyber security controls are applied to contracts to mitigate supply chain risks.

8. There are key characteristics associated with contracts considered to be at a higher risk of cyber security threats. In-scope organisations must ensure that all suppliers demonstrate that they meet certain technical requirements for contracts or services that include the following characteristics:

- where personal information of citizens, such as home addresses, bank details, or payment information is handled by a supplier;

- where personal information of Government employees, Ministers and Special Advisors is handled by a supplier (such as payroll, travel booking or expenses information);
- where ICT systems and services are supplied which are designed to store, or process data at the OFFICIAL level of the Government Security Classifications Policy[1]; and/or
- where contracts deal with information related to the day-to-day business of Government, service delivery and public finances[2].

Examples of contracts likely to meet these characteristics are set out in Annex A, however this is not an exhaustive list.

9. The quickest and most effective means of mitigating risks associated with such contracts, is for the technical requirements to include either **Cyber Essentials** or **Cyber Essentials Plus** certification[3]. Where Cyber Essentials certification is required, it must be renewed annually by the supplier for the duration of the contract.

10. Where a supplier does not hold Cyber Essentials or Cyber Essentials Plus they must be able to demonstrate equivalent controls are in place through other means.

11. Suppliers and In-scope organisations should note that evidence of holding a Cyber Essentials certificate (or equivalent) is essential at the point when data is to be passed to the supplier.

Limitations

12. In-scope organisations should note that the Cyber Essentials Scheme does not assure specific products or services being supplied. Where specific assurance of products or services is required, further relevant standards should be applied.

13. In some cases, the potential cyber risks associated with a contract, and the control measures required to mitigate them, may exceed the parameters of the Cyber Essentials Scheme. In these instances security teams or experts should be consulted to ensure proportionate additional measures are put in place. Examples of the types of contracts relevant here are provided at Annex A.

14. The Cyber Essentials Scheme does not negate risk and it is not designed to address more advanced, targeted attacks. Such risks will require significantly more sophisticated additional measures to tackle them. In-scope organisations facing these types of threats should develop a strategic approach as part of a wider organisational security strategy.

15. The Cyber Essentials Scheme should not be applied to all contracts as a matter of course. In-scope organisations must not take a blanket approach. Not all contracts will require suppliers to be certified under a Cyber Essentials Scheme, or to demonstrate equivalent controls.

16. Security controls must be relevant and proportionate to the product, goods or services being procured. In-scope organisations should take care to only require Cyber Essentials certification where it is relevant to the subject matter of the contract, proportionate and necessary to manage cyber security risks. It is important not to over-burden suppliers or deter Small and Medium-Sized Enterprises (SMEs) and Voluntary,

---

[1] For information marked SECRET or TOP SECRET, the use of designated secure IT systems is necessary. More information on security classifications can be found here.

[2] For example, contracts that deal with routine international relations and diplomatic activities, public safety, criminal justice and enforcement activities, many aspects of defence, security and resilience and commercial interests, including information provided in confidence, intellectual property and the contract itself.

[3] A summary of the key features of Cyber Essentials and Cyber Essential Plus can be found at Annex B.

Community and Social Enterprises (VCSEs) from bidding for public contracts.

17. Cyber Essentials is self assessment, with organisations completing a questionnaire. The questionnaire is then verified by an independent Certification Body to assess whether the appropriate standard has been achieved, and certification can be awarded. This option offers a basic level of assurance

18. In-scope organisations should ensure decisions relating to appropriate cyber security controls are recorded in the audit trail, including circumstances where cyber security risks are assessed as very low, not relevant, or where no measures are required.

19. A more comprehensive update on the application of the Cyber Essentials scheme will be published in line with National Cyber Security Centre's redevelopment of the CE scheme.

Suppliers on G-Cloud Framework Agreements

20. In-scope organisations accessing Cloud services through the Crown Commercial Service (CCS) G-Cloud Commercial Agreements should note that suppliers on these Agreements are required to demonstrate they comply with the Government's Cloud Security Principles.

21. Suppliers are encouraged to state if they have Cyber Essentials or Cyber Essentials Plus certification as part of their service offer, but it is not a requirement of the Commercial Agreement for suppliers to hold this certification.

22. When awarding call-off contracts via G-Cloud, In-scope organisations should assure themselves that the supplier(s) are managing relevant cyber risks effectively before making a contract award.

Background

23. The Cyber Essentials Scheme provides a sound foundation of basic hygiene measures that all types of organisations can implement, and build upon, and can significantly reduce an organisation's vulnerability. It was developed by Government and Industry to fulfil two functions:

- to provide a clear statement of the fundamental controls all organisations should implement in order to increase their cyber security, aiming to mitigate the risks from many common internet based threats, within the context of the Government's 10 Steps to Cyber Security; and
- to offer a mechanism for organisations to demonstrate to customers, investors, insurers, and others, that they have taken these essential precautions.

24. The full requirements of the Cyber Essentials Scheme can be found at: https://www.ncsc.gov.uk/cyberessentials/overview.

Contact and Sources of Further Information

25. Enquiries about this PPN should be directed to the Helpdesk (telephone 0345 410 2222; email info@crowncommercial.gov.uk).

26. Frequently asked questions (FAQs) are set out in Annex C.

27. Further information is available on the following websites:

- NCSC Cyber Essentials website: https://www.ncsc.gov.uk/cyberessentials/overview
- Cyber Essentials Scheme Partner: IASME:https://iasme.co.uk/cyber-essentials/
- Cyber Essentials readiness toolkit: https://getreadyforcyberessentials.iasme.co.uk/questions/

- Details of certification bodies: https://iasme.co.uk/certification-bodies
- Cyber Essentials Advice and Guidance: https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=Cyber%20Essentials&sort=date%2Bdesc
- Cloud security principles: https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles
- NCSC Supply Chain Risk Assessment Guidance: https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security
- National Protective Security Authority Supply Chain Guidance: https://www.npsa.gov.uk/protected-procurement
- The Digital, Data and Technology Playbook: https://www.gov.uk/government/publications/the-digital-data-and-technology-playbook

Cabinet Office

Annex A – Examples

1. The following are contract examples[4] which would be considered to meet the characteristics for the inclusion of Cyber Essentials requirements:

- Curriculum vitae (CV) writing services to support individuals back into the labour market. Data held by the supplier will include citizens' personal information; such as name, address, telephone number, date of birth, email address and National Insurance number.
- Car hire services for members of staff. Data held by the supplier will include personal information of Civil Servants including name, work address, work email, home address and driving licence number.
- Contact centre services for advice, guidance and signposting for individuals. Data held by the supplier will include citizens' personal information; such as name, address, telephone number, date of birth, email address and National Insurance number.

2. Other types of contracts where Cyber Essentials, Cyber Essentials Plus, or equivalent controls, may be relevant, include:

- where data is held or accessed outside of the UK/EC;
- where data is subject to the EU-US Data Privacy Framework;
- where data is regularly held in a separate Disaster Recovery location;
- escrow and disaster recovery suppliers with access to customer data.

3. Additional control measures are likely to be required when letting contracts in the following categories:

- Professional services suppliers, where the data being handled is classified as higher than "Official"– this may include commercial, financial, legal, HR and business services.
- ICT– IT Managed, Outsourced and ICT Services Providers (running systems that store data).

4. Examples where the Scheme would not be relevant in contracts includes:

- Communications and marketing planning services for a specific departmental product or service, which would not require access to personal data. In such instances, the supplier would have access to some OFFICIAL level communications and personal information of civil servants as points of contact that are necessary to administer the delivery of the service; but this may not meet the required security thresholds for the application of Cyber Essentials controls.
- Driving instructor services for 10 individuals with very limited access to personal data involved and delivered by a sole trader whose use of IT is limited and incidental to the service being delivered.
- Contract to deliver ICT support services which includes an element of Legacy IT provision. Effective cyber security controls would need to be implemented

[4] These examples are illustrative and are not an exhaustive list.

for all aspects of the service delivery, however Legacy systems cannot meet the requirements of Cyber Essentials. In such cases overarching Cyber Essentials requirements could be required for relevant areas, and effective alternative controls for those unable to be assured by Cyber Essentials controls.

Annex B – Key Features of Cyber Essentials and Cyber Essential Plus

Full details on the requirements of Cyber Essentials and Cyber Essentials Plus can be found at: https://www.ncsc.gov.uk/cyberessentials/overview.

The key features are summarised below:

Cyber Essentials

- Cyber Essentials assesses how an organisation has implemented five technical controls which protect from the vast majority of common (internet based) cyber attacks.
- This is important because vulnerability to basic attacks can mark out an organisation as a target for more in-depth unwanted attention from cyber criminals and others.
- Cyber Essentials is a self assessment option, with organisations completing a questionnaire. The questionnaire is then verified by an independent Certification Body to assess whether the appropriate standard has been achieved, and certification can be awarded. This option offers a basic level of assurance
- Certification gives you peace of mind that your defences will protect against the vast majority of common cyber attacks simply because these attacks are looking for targets which do not have the Cyber Essentials technical controls in place.
- When certified, organisations can demonstrate that they are meeting the minimum baseline of technical cyber security standards/controls that are prescribed by Government and Industry.

Cyber Essentials Plus

- Cyber Essentials Plus assesses the same technical controls as Cyber Essentials, but also comprises remote and on-site vulnerability testing.
- This checks whether the controls the supplier has put in place actually provides a defence against basic hacking and phishing attacks, using commodity tools that are widely available online.
- It is a more rigorous assessment and should be used when there is a higher risk of cyber security threats.

Annex C – Frequently Asked Questions (FAQs)

Q1 Why should Cyber Essentials / Cyber Essentials Plus be used in the Government's supply chain?

- To manage cyber security risk in Government's supply chain; and
- to allow Government's suppliers to use a recognisable scheme to demonstrate to other potential customers that they take cyber security seriously.

Q2 Which technical areas does Cyber Essentials cover?

- Boundary firewalls and internet gateways
- Secure configuration
- Access control
- Malware protection
- Security update management

Full details on the requirements of Cyber Essentials and Cyber Essentials Plus can be found at: https://www.ncsc.gov.uk/cyberessentials/overview.

Q3 When should I notify suppliers of any applicable Cyber Essentials requirements?

Ideally this should be discussed with potential suppliers in the pre-procurement stage where you are shaping your overall project requirements. Any applicable Cyber Essentials requirements must be specified in the Contract Notice under the Open procedure, and consideration should be given to highlighting any Cyber Essentials requirements in Contract Notices for other procedures to provide bidders with the longest possible time to seek certification.

Q4 How do suppliers undertake the certification process?

This service is provided by Government approved certification bodies which are currently accredited by Information Assurance for Small and Medium Enterprises (IASME).

Further details can be found at https://iasme.co.uk/certification-bodies.

Q5 At which point in the procurement is the supplier required to demonstrate Cyber Essentials certification?

Evidence of holding a Cyber Essentials certificate (whether basic level or Plus level), or equivalent, is required before contract award.

Under exceptional circumstances, In-scope organisations may wish to make a risk-based decision and allow a contract to commence if Cyber Essentials certification of a supplier is not current i.e. it has expired and is in the process of being renewed. However, the supplier must be able to demonstrate that they hold the appropriate certification, or equivalent, at the point when data is to be passed to the supplier.

Q6 How much will it cost a supplier to become Cyber Essentials certified?

The cost for smaller companies to be Cyber Essentials certified is currently expected to range between £300 and £500+ VAT at basic level. The cost of a Cyber Essentials Plus

assessment will depend on the size and complexity of your network. Please contact IASME with any questions and for further advice and guidance. It is possible that costs may change in the future. Up-to-date information on costs can be found here: https://www.ncsc.gov.uk/cyberessentials/overview.

Q7 How often will Cyber Essentials certification need to be renewed?

Organisations must recertify every 12 months in order to maintain a valid certificate. Failure to do so renders the organisation uncertified. As Cyber Essentials provides assurance of compliance only at the time of testing; certified organisations failing to regularly patch their ICT or control secure configuration may become non-compliant in substantially less than one year. The requirement to certify at more regular intervals should be risk based and determined on a case-by-case basis, subject to the requirements of the contract.

Q8 What does the scope of Cyber Essentials cover?

By default, Cyber Essentials applies to the legal entity providing the goods/services rather than any wider corporate entity of which the supplier may be a part. However, organisations can restrict the scope of certification to only part of the legal entity.

In-scope organisations should be aware that a supplier may share a client's information with a third party such as a cloud service provider. Cyber Essentials does not ensure that the security of the third party is in scope of certification. In-scope organisations are therefore advised to check the scope of a Cyber Essentials certificate and consider whether the risks of information sharing justify requiring Cyber Essentials certification with any third party.

Q9 How does Cyber Essentials fit in with/complement existing security requirements?

There is an existing set of information assurance and cyber security requirements that the Government has in place for suppliers. In some circumstances, Cyber Essentials will be used in areas not covered by these requirements or it will be used alongside these requirements, or used as part of them.

- The **Model Services Contract** (MSC) is a standard contract used across Government to ensure consistency of terms and conditions for complex services contracts, particularly those with ICT and Business Process Outsourcing providers exceeding £20 million in value. The MSC addresses security management in the 'Security Management' schedule. This schedule requires that the supplier and relevant subcontractors have Cyber Essentials or Cyber Essentials Plus certifications (or equivalent), alongside other ongoing security requirements.
- The **Government Functional Standard GovS 007: Security** describes the mandatory security outcomes that all Government organisations and third parties handling Government information must achieve covering physical, personnel and cyber security domains. The Cyber Essentials Scheme covers some of the cyber security measures outlined in the standard and in the Cyber Security Standard.
- The ISO27001 standard is widely used but companies that attain this standard **will not** automatically conform to Cyber Essentials. This is because it is not usual for all of the five technical controls in Cyber Essentials to be included in the scope for ISO27001 implementation. It is also unlikely that any of these

controls will be tested for ISO27001. Therefore most businesses with ISO27001 will have to adopt Cyber Essentials in addition to ISO27001 or demonstrate equivalent controls are in place.

Q10 Are there alternatives to demonstrating compliance with Cyber Essentials technical requirements other than through gaining the certificate?

Yes. To comply with the EU Public Contracts Regulations 2015 (PCR2015) for above threshold procurements, In-scope organisations must accept equivalents and suppliers need only demonstrate to the satisfaction of the In-scope organisation that they meet Cyber Essentials requirements. Normally, this should be verified by a technically competent and independent third party.

To demonstrate that Cyber Essentials Plus requirements have been met, it is required in all cases that verification is provided by a technically competent and independent third party.

The quickest and most effective means of ensuring risks associated with contracts displaying these characteristics is through the application of Cyber Essentials to the organisation.