National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

Cyber Essentials

Supply Chain Playbook

This guide will help you protect your business from cyber attacks by supporting you to embed Cyber Essentials in your supply chain

National Cyber Security Centre
a part of GCHQ

CYBER ESSENTIALS

CONTENTS

Ministerial foreword

“There have been too many occasions where we’ve seen first-hand the impact that cyber attacks can have on businesses. Supply chains can provide numerous points that attackers look to exploit, but only 14% of firms are on top of the potential risks faced by their immediate suppliers.

“That's why we wrote to the UK’s leading companies, to set out steps to bolster their cyber security – including a specific action on securing supply chains using the Cyber Essentials scheme – which should be a priority for every company.

“The Cyber Essentials Supply Chain Playbook we have developed with the NCSC is designed to help organisations manage their supply chains more effectively, ensuring their operations are protected every step of the way.”

Liz Lloyd
Cyber Security Minister

Ministerial letter on cyber security

Executive summary

Cyber threats are an immediate and escalating danger to the UK's economy, our businesses and our national security. Attacks are becoming more frequent and more damaging, with recent high-profile incidents showing how quickly operations can be disrupted and profitability eroded.

And it's not just your own systems at risk: vulnerabilities in your supply chain can have a devastating impact on your organisation.

As the National Technical Authority for cyber security, the NCSC is calling on industry to build the cyber resilience of UK supply chains by championing the Cyber Essentials scheme and making it a standard requirement for suppliers.

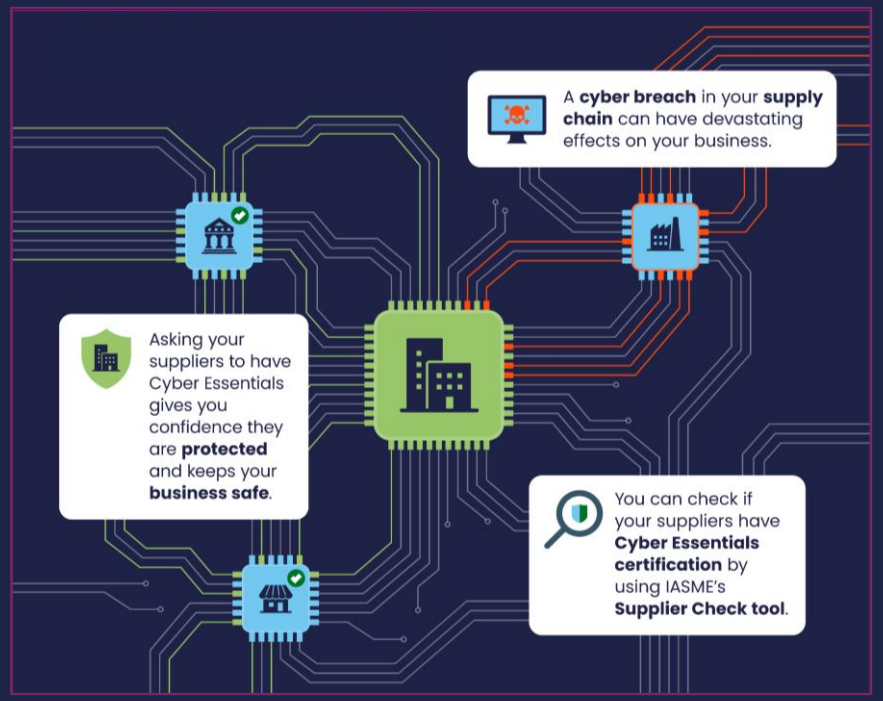
We know we cannot succeed alone. Protecting the UK's economic future requires leadership from the nation's most influential companies.

Your commitment will set the tone for the entire economy. By acting now, you will not only protect your organisation but also strengthen the UK's position as a secure, trusted environment for investment and innovation.

This Playbook is designed to give you the resources and guidance to help you embed Cyber Essentials into your supply chain.

We are asking senior leaders to direct your procurement and information security teams to:

- Embed Cyber Essentials across your supply chain. This government-backed scheme provides a proven baseline of protection against common attacks.
- Implement Cyber Essentials technical controls within your own systems as part of a strategic approach to managing cyber risk.



Time to act

The following resources in this playbook are designed to help your security and procurement professionals reduce the cyber risk to the UK and minimise the impact of the commodity cyber threat on your supply chain.

We are calling on organisations to:

- **Audit your supply chain** by using the IASME Supplier Check tool.
- Scope whether all of your supply chain, or certain supplier security profiles will **require Cyber Essentials as a Minimum Security Requirement.**
- Take forward the **most effective intervention option** to embed Cyber Essentials within your supply chain, which could include:
    - **Requiring in contracts***
    - **Influencing procurement decisions**
    - **Incentivising adoption**
    - **Awareness raising**
- Provide feedback and tell us what you're doing to implement Cyber Essentials in your supply chain at sectorresilience@ncsc.gov.uk.

***In our experience, if you want to see significant improvements in your supply chain security through Cyber Essentials, you need to require it. If you promote it among a small scope of suppliers, your impact will be limited.**

Businesses are not managing cyber risk effectively

High-profile, damaging cyber attacks have demonstrated attackers' intent and ability to exploit security vulnerabilities in supply chains across the UK. Without basic cyber hygiene, suppliers will continue to be vulnerable as threat actors hone their focus on unprotected businesses.

Despite this, relatively few organisations take steps to formally review the risks posed by their immediate suppliers and wider supply chain.

This is often attributed to a lack of capacity, capability and tools within buying organisations.

Cyber Essentials can help.

Cyber Essentials provides a clear, efficient way for organisations to gain assurance that their suppliers, or other third parties, have good cyber security in place and that they are protected against most common cyber attacks.

Cyber Essentials can help secure your business

Almost half (43%) of all UK businesses suffered a cyber attack over the last year.

In today's digital world, cyber attacks are inevitable, and the consequences can be costly. That's where Cyber Essentials comes in.

- Cyber Essentials is a UK government-backed certification that demonstrates that your organisation has implemented the essential security controls that protect against most common cyber threats. It is the minimum standard of security that the NCSC would advise *every* organisation to achieve.
- The scheme is delivered by the NCSC - in partnership with DSIT - through the IASME Consortium, who manage a network of over 400 Cyber Essentials Certification Bodies.
- Implementing just five key controls **reduces risk**, **strengthens resilience**, and gives stakeholders **verified assurance** that your organisation prioritises cyber security and meets recognised baseline standards.

Firewalls	Secure configuration	Security update management	User access control	Malware protection

There are two levels of certification:

- Cyber Essentials: a combination of self-assessment and independent audit
- Cyber Essentials Plus: the same protections, but with rigorous, independent technical testing

Lock your door against common cyber attacks

Cyber attacks come in many different forms, but the majority are basic in nature - the digital equivalent of a thief trying your front door to see if it's unlocked...

Cyber Essentials locks the door shut on these attacks.

How you can use Cyber Essentials to secure your supply chain

- Cyber Essentials has been proven effective against common cyber attacks, including supply chain threats.
- Cyber Essentials can play a significant role as an **assurance tool** and help address the challenges that many organisations face in securing and effectively managing supply chains.
- A new Supplier Check tool provides a view across your supply chain, to **quickly verify** whether your suppliers have been certified (and to what level - CE or CE Plus).
- Provide a tangible way for organisations to **gain confidence** that their suppliers, or other third parties, have effectively implemented fundamental technical controls and that they are protected from the majority of untargeted, commodity attacks.
- **Save time and reduce complexity** on cyber security due diligence. Suppliers can also use Cyber Essentials as evidence across their customer base, reducing the time spent filling out duplicative questionnaires.
- UK organisations with turnover <£20m that achieve Cyber Essentials - and certify their whole organisation - are entitled to free Cyber Liability Insurance, giving suppliers access to **a professional incident response capability** during an incident.

Case study: With the financial services sector facing an evolving cyber threat, one the UK's largest pensions & life companies asked its partnership network of over 2,800 independent businesses to certify to Cyber Essentials Plus.

In such a large supply chain this had its challenges, but the decision is already showing a positive impact.

"Security incident numbers have significantly reduced... we have seen around 80% reduction in cyber security incidents, which directly correlates to controls and best practice implemented through Cyber Essentials."

"We recognise the position we have within the supply chain in the UK, and the positive impact we have experienced with Cyber Essentials."

Matthew Smith, Divisional Director of Cyber Security, St James's Place

Steps to embed Cyber Essentials in your supply chain

We have highlighted how Cyber Essentials can address the challenges that many organisations face in securing and managing the cyber security of their supply chain.

Next, we outlined the actions you can take to embed Cyber Essentials into your supply chain.

Compiled as a series of actionable steps, we will recommend the activity you should consider and point to the tools and resources that can help you achieve each step.

1. **Assess your risks**
2. **Profile your suppliers**
3. **Set requirements**
4. **Communicate expectations**
5. **Incentivise adoption**
6. **Embed into procurement processes**
7. **Monitor adoption**

Understanding your supply chain risk

1. Assess your risks

Effectively securing the supply chain can be hard because vulnerabilities can be inherent or introduced and exploited at any point in the supply chain.

Before looking to mitigate, you should use the NCSC's Supply Chain Principles to **check you understand the risks** including:

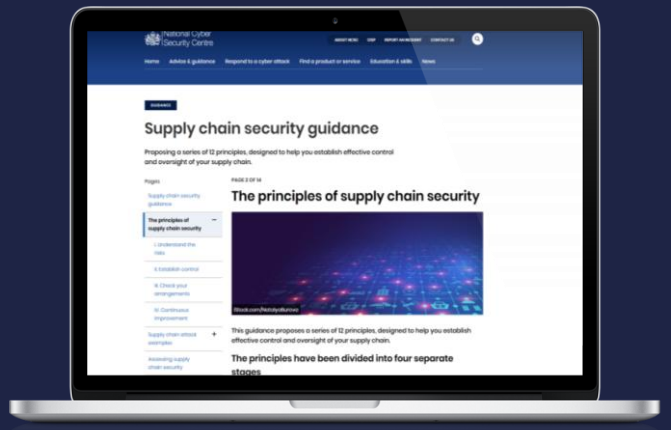
- understand what needs to be protected and why
- know who your suppliers are and build an understanding of what their security looks like
- understand the security risk posed by your supply chain

Also consider if the effects of a breach via the supplier would:

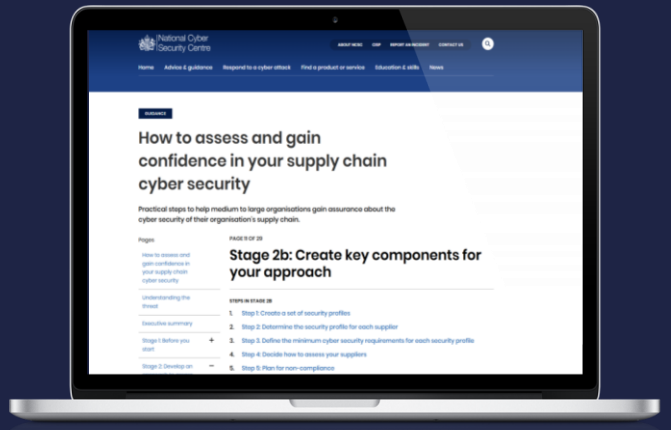
- adversely impact the organisation's business operations or processes
- adversely impact the organisation's reputation
- cause significant financial or legal, regulatory or contractual consequences
- affect the safety of your staff or customers

2. Profile your suppliers

Once this is done, you should **define a set of supplier security profiles;** consider creating different sets of requirements for different supplier sizes and types to ensure your requests are realistic, pragmatic and proportionate to the risk.



Use the NCSC's Supply Chain Principles to check you understand the risks



Use NCSC guidance to help create a set of cyber security profiles

Define your approach to increasing Cyber Essentials adoption

3. Set requirements

Once supplier security profiles have been developed, you should start to consider **minimum security requirements** for each security profile (which could include a minimum requirement for all suppliers) and consider whether Cyber Essentials is well-placed to reduce any risk and increase supply chain assurance efficiency.

Based on your business context, you could consider for each profile:

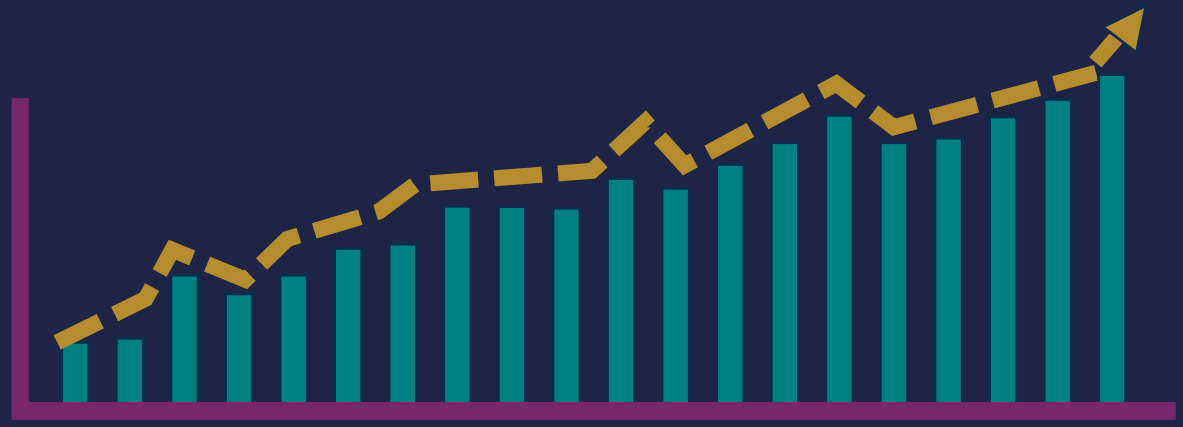
- Setting **Cyber Essentials Certifications as a minimum-security requirement**; and/or
- Aligning **Supply Chain Assurance questionnaires** to include Cyber Essentials controls and accepting a Certification as validation of these.

4. Communicate expectations

Once minimum-security requirements have been set you should consider how you communicate and enforce these with your suppliers.

In the next few pages, intervention options are explained in detail and include:

1. **Raising awareness** by signalling your intent through supplier letters and at supplier conferences.
2. **Incentivising** Cyber Essentials adoption through Funded Vouchers, or the IASME Cyber Advisor Supply Chain Package.
3. **Ensuring these criteria influence procurement decisions,** particularly in Request for Pricing (RfP) and Request for Quotation (RfQ) exercises.
4. **Requiring** Cyber Essentials during contract renewals



Tools to raise awareness with your supply chain

4.1 Communications resources: We have developed the following supporting resources to raise your supply chain's awareness of Cyber Essentials:

Account Manager
A dedicated point of contact to provide ongoing support and guidance throughout the process — you can request this via supplychain@iasme.co.uk.

Supplier Letters
We have developed a draft supplier letter template which can be used to signal your intent and also talk about the wider government and sector efforts.

Supplier event materials
We have developed a slide deck template, and a pre-recorded webinar that can be used to demonstrate to suppliers what Cyber Essentials is, why it's important and how to achieve it. Bespoke supplier webinars are available upon request.

Social Media Assets
Social media assets are also available to signal your intent to your supply chain and demonstrate your security posture to customers. Including Cyber Essentials in supply chains YouTube video

Cyber Essentials Knowledge Hub
The Cyber Essentials Knowledge Hub is a central source of trusted, up-to-date information about the Cyber Essentials scheme, including latest updates, sector specific guidance and resources to help you through certification.

Cyber Essentials Readiness Tool
The Cyber Essentials Readiness Tool is the first step in the journey towards becoming Cyber Essentials certified. It is designed to support and educate organisations by creating a tailored pathway for organisations to follow.

How to incentivise Cyber Essentials adoption

5. Incentivise adoption

Based on your business context, you may decide to incentivise Cyber Essentials adoption across the relevant supplier security profiles.

Incentivising options include:

Free Cyber Advisor Support
Through the NCSC-assured Cyber Advisor scheme, a Cyber Advisor can provide cyber security advice tailored to small and medium-sized organisations' needs. Suppliers can access 30 minutes of advice completely free.

Included Cyber Insurance
Eligible UK organisations that achieve Cyber Essentials certification receive £25,000 in cyber insurance, including 24/7 incident response support with technical, legal, and crisis management services.

Extended Cyber Advisor Support
The procuring organisation can pay for additional Cyber Advisor time for SMEs in their supply chain, available at £120 per hour.

Funded Cyber Essentials Package
A scheme where procuring organisations pay for a full package of 20 hours of remote support with a Cyber Advisor to guide organisations through Cyber Essentials Plus, including hands-on technical verification that controls have been put in place.

Cyber Essentials Vouchers
A paid-for voucher scheme where the procuring organisation can redeem an amount chosen by the customer towards the cost of Cyber Essentials certification.

You can get in touch with supplychain@iasme.co.uk to find out more or visit http://iasme.co.uk/cyber-essentials/

Influencing procurement decisions and stipulating in contracts

6. Embed into procurement processes

Based on the level of operational, financial, reputational or data risk associated with a given supplier, you may choose that certain vendors must have a Cyber Essentials certificate (or demonstrate they have implemented these controls through other means) to win your business and ask for these in Standard Contractual Clauses.

Alternatively, you may also choose to introduce **weighted criteria** that assess a supplier's cybersecurity credentials as part of a Request for Proposal or Request for Quotation.

In all these scenarios, you will need to work closely with your procurement (or third-party risk) teams to document and mitigate risk, and consider:

- when you will introduce these requirements
- how you build the 'right to audit' into contracts and exercise these
- penalties for non-compliance (e.g. no longer Cyber Essentials certified mid-contract)
- whether suppliers need to include the same requirements for any contracts they sub-let
- key performance indicators to measure the performance of your supply chain security management practices

Check Cyber Essentials adoption in your supply chain

7. Monitor adoption

To help organisations understand which suppliers are Cyber Essentials certified, IASME has developed the **Supplier Check Tool**.

The tool enables you to drop a large list of suppliers (up to 5,000) into a bespoke search function and find out which suppliers are certified to either Cyber Essentials or Cyber Essentials Plus.

This makes it significantly easier for you to check which suppliers are certified.

A completed CSV spreadsheet may be retained for up to 6 months to avoid creating a database each time.

The results may be viewed to screen or exported to Excel.

Visit the IASME Supplier Check Tool website to find out more.

https://supplier.iasme.co.uk

Frequently Asked Questions

Is Cyber Essentials risk-based?	The NCSC is the UK's technical authority for cyber security. Through Cyber Essentials, it provides a set of minimum cyber security controls specifically designed to protect against commodity cyber threats. These controls are carefully risk-assessed on your behalf, so you don't have to.
Is Cyber Essentials relevant to international suppliers?	Whilst the certification scheme is UK-centric, the controls set out within Cyber Essentials are important for businesses all over the globe. As a customer, you should look to ask for the Cyber Essentials controls to be in place and develop international assurance mechanisms to verify this. Many other countries around the world recognise the quality and value of CE as a solid baseline for cyber hygiene and are seeking to reproduce it in their own domestic schemes.
What if the small suppliers I work with don't have the expertise to certify?	The Cyber Advisor scheme is designed to help small and medium organisations improve their cyber security and certify. As part of the supply chain focus, there is an opportunity for large organisations to purchase a set amount of hours (1-2-1 consultancy time) to support SME suppliers.
We don't currently have Cyber Essentials – how can I ensure the messaging is right to require this of our suppliers?	Cyber Essentials is the UK Government's minimum baseline standard for cyber security for organisations of all sizes. Large, complex enterprises have achieved Cyber Essentials Plus certification and we encourage you to start your journey towards this and seek support. We encourage you to outline that you intend to move towards Cyber Essentials - and that this may take time as a large, complex organisation - and that your suppliers should be doing the same.
Can Cyber Essentials be scoped to a certain part of the organisation?	Yes, CE is a system-level certification, enabling organisations to be flexible if they need to, in how they apply it. However, over 90% of organisations scope their full organisation. It is a customer's responsibility to check that the scope adequately covers the risk they are taking by contracting with the supplier. The IASME certificate search (and Supplier Check tool) allows you to check the scope of the certificate.
If I have Operational Technology on my estate, can I still get Cyber Essentials?	Yes, you can. Cyber Essentials focuses on basic IT security controls for internet-connected IT systems, and doesn't explicitly focus on OT. OT should be appropriately isolated through network segmentation, monitoring and access control. Where OT interacts with IT (e.g. shared networks or remote access), those interfaces must meet Cyber Essentials requirements.