

## Cyber Resilience Voucher Scheme FAQs

- 1. What is the Cyber Resilience Programme?** - The Cyber Resilience Programme (CRP) is the last of the Digital Scotland Business Excellence Partnership (DSBEP) projects. Where the other projects are designed to encourage Digital Participation, the CRP is designed to help business do so in a safe manner. The programme has two work packages (i) the Cyber Resilience Toolkit (ii) The Cyber Resilience Voucher.
- 2. What is the Cyber Resilience Toolkit?** - The Cyber Resilience Toolkit is being designed by PwC on behalf of DSBEP after winning a procurement exercise. The toolkit is designed to be a useful guide for company facing staff within the Scottish Business Support Network so that they can highlight the topic to their companies. The guide will bring together the current information available to businesses on how to be cyber resilient in one place. Further to the guide PwC will be running a number of workshops across Scotland both in person and online on the toolkit once it has been completed. These workshops are likely to run from June 2016 to September 2016.
- 3. What is the Cyber Resilience Voucher?** - The Cyber Resilience voucher is an award to a company that will make it possible for them to secure the services of an industry expert to help them with their cyber security strategy. This expert will also be able to answer any questions they might have to help them get their systems sense checked by the Cyber Essentials UK Government Standard. The voucher is of the value of up to £1.5k per company. The voucher scheme went live on the 29<sup>th</sup> of April. The application form can be accessed via your HIE, SE or Business Gateway contact.
- 4. What is Cyber Essentials?** - Cyber Essentials is a UK Government Programme designed to check whether businesses are taking the appropriate precautions to minimise the risk of a cyber attack on their business. The programme is designed to be delivered as a self assessment which is then passed to an industry expert to review and indicate whether the company meets the minimum requirements or not. Once you have carried this out it can be displayed on your website to demonstrate that you are serious about protecting your customers' data.

More information can be found at <https://www.cyberstreetwise.com/cyberessentials>.

- 5. A large proportion of small businesses take the attitude that “No one will target me will they?”** - All citizens and businesses are a potential target of an attack, particularly if they do not take some simple precautionary measures to protect themselves. Any company that relies on computerised systems for payroll, marketing via social media or a website, booking systems, databases of customer details including payment details and/or any Intellectual Property or Patent information that could be of value. Companies can also be targeted as a route in to businesses who they supply goods or services to.

A business does not need to be specifically targeted to become a victim; cyber criminals constantly scan websites, systems and/or devices to detect vulnerabilities. Therefore, if you are not taking the appropriate steps, you will flag up as an easy target during this scanning process.

- 6. Am I eligible for a Cyber Resilience Voucher?** – The Cyber Resilience Voucher is business that meets the following criteria:

- a. Based in Scotland;
- b. Are V.A.T registered
- c. Meet the SME definition\*
- d. Have a relationship with either Business Gateway; HIE or SE
- e. As the voucher is paid out to the company once the work has been completed the business will have to demonstrate that they have the financial means to cover the costs of their chosen supplier (please see the flow diagram on page 2 for more information).

**\*SME eligibility**

An SME as defined by [http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index\\_en.htm](http://ec.europa.eu/enterprise/policies/sme/facts-figures-analysis/sme-definition/index_en.htm). Please note that this web link is correct at the time of publication of the guidance. You should ensure that you have checked for the latest version of this guidance.

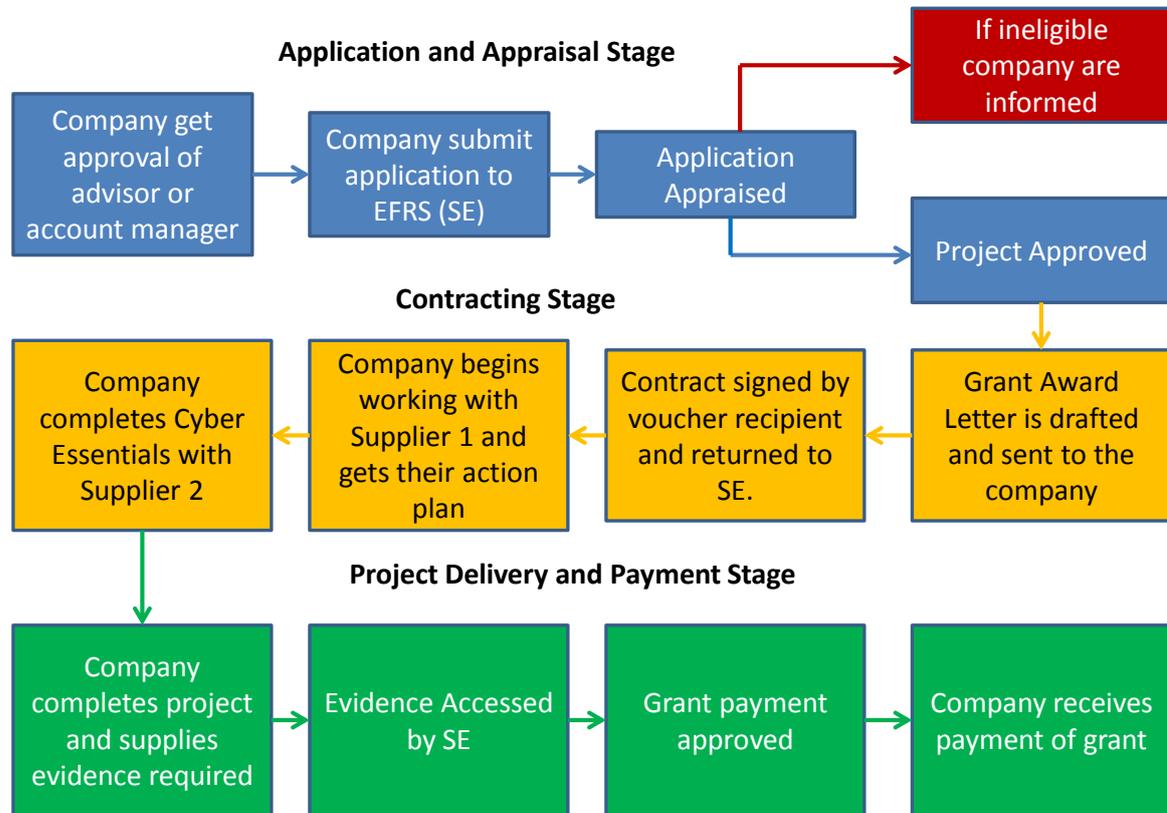
The main factors determining whether a company is an SME are:

- number of employees and
- Either turnover or balance sheet total.

<b>Enterprise category</b>	<b>Headcount</b>	<b>Turnover</b>	<b>Balance sheet total</b>
Medium sized	<250	≤ €50 million	≤ € 43 million
Small	<50	≤ €10 million	≤ 10 million
Micro	<10	≤ €2 million	≤ 2 million

The Cyber Resilience Voucher is funded under *de minimis* regulations – your business should not have received more than €200k of public support in total in the last three financial years. The full regulations can be found at <http://www.bis.gov.uk/policies/europe/state-aid/de-minimis-aid-regulations>.

**7. How do I apply for the Cyber Resilience Voucher?** – The application & payment process is highlighted below.



- a. To apply, a company should be endorsed either by their Business Gateway Advisor or Highlands & Islands/Scottish Enterprise Account Manager or High Growth Start up Manager. This endorsement will simply be a copy of an email from the companies business support contact confirming they are happy for them to proceed.
- b. Once the application has been completed it will be appraised by Scottish Enterprise to assess eligibility.
- c. Once this step has been completed if the company are eligible the grant offer letter will be sent to the company.
- d. The company should sign and return the voucher offer letter before proceeding to carry out the work.

Please note that work should not commence in advance of signing and returning the voucher offer letter. The voucher cannot be used to cover the costs of any existing work that is already underway.

**8. What are eligible costs associated with the Voucher?-** The voucher is for the following two areas of support:

- a. To work with an expert contractor to introduce a basic Cyber Resilience action plan for the business.
- b. To have the steps you have taken under section a sense checked by another industry expert, which will allow the company to find out whether they are now meeting the basic requirements or not.

It is expected that the recipient of the voucher will meet the basic cyber essentials standard by completing both parts of the project.

**9. How do I identify suppliers?** - To complete the project you will need to use two different suppliers.

- The first supplier will be contracted to provide the expert advice and assist the company to put a Cyber Resilience Strategy in place; and
- The second supplier will provide a sense check of the information you provide via the Cyber Essentials Assessment Questionnaire.

Please note that two different suppliers have to be used for completing steps 1 and 2 above in order to provide neutrality in the step 2 sense check. Both suppliers should be selected from the lists provided via the links below as accredited suppliers of Cyber Essentials.

- [QG Management](#)
- [CREST](#)
- [IASME](#)
- [APMG](#)

These four companies were selected to design the Cyber Essentials Programme by the UK Government. Each body has a slightly different process for businesses to complete however each programme is equally recognised, so the decision on which supplier to use will determine which process you will follow.

**10. When will I receive payment of the Cyber Resilience Voucher?** – Please see the diagram above. The company will receive payment of the voucher once they have:

- completed the project;
- paid their supplier and can show bank statements to confirm payment;
- supplied SE with a copy of both invoices on the contractors letter headed paper; and
- provide SE with a copy of the Cyber Resilience Completion and Claim Form.