DigitalXRAID

CYBER SECURITY EXPERTS

Why You Need Cyber Essentials

Secure & Certify Your Organisation to Government Approved Standards

IASME® Consortium

CREST

CYBER ESSENTIALS

Crown Commercial Service Supplier

About Cyber Essentials

CE is designed to ensure organisations understand and mitigate their security gaps. It provides assurance to your customers and competitors that your organisation is complying with government approved security standards.

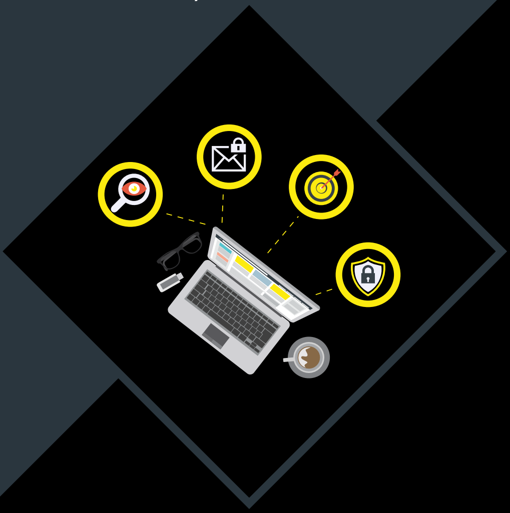
CE will help organisations to understand the importance of cyber compliance and enables them to demonstrate how committed they are to their own cyber security. Each individual organisation is then appraised against the CE benchmark.

How DigitalXRAID can help you

DigitalXRAID are security specialists with years of experience in helping large and small companies understand their responsibilities for securing data assets, increasing their security position and reducing exposure to cybercrime.

We are an accredited Cyber Essentials certifying body. We will help you to conduct your assessment, report the outcome to the Accreditation Body (CREST or IASME) and supply you with your certificate.

We also provide consultancy services to help improve your cyber/information security practices, should this be required. The Cyber Essentials standard gives DigitalXRAID clear objectives: to follow specific grading criteria and report all passes and fails to the Accreditation Body.



Cyber Essentials ‘Basic’

Self-assessment & external vulnerability scan

The baseline Cyber Essentials package is a self-assessment questionnaire, which is completed in conjunction with an external vulnerability scan. The self-assessment questions relate to both the technical and day-to-day controls required to be in place, for example:

- Do all computers and devices which are connected to the Internet have Malware Protection?
- Have all network devices been securely configured with only the minimum services necessary to fulfil requirements and has this been done in such a way to minimise vulnerabilities during installation?
- Are all devices and information on the organisation’s network protected by firewalls to help prevent unauthorised access via the Internet?
- Is Patch Management in place to ensure all software running on both PC’s and Servers is updated with the latest security features?
- Have all User Accounts been assigned to authorised individuals, with minimal access levels granted where appropriate?

DigitalXRAID tailor their consultancy service to help organisations who don’t have the resource or time to complete the assessment. We will guide you through certification quickly and efficiently.
Once the self-assessment is complete, DigitalXRAID will score, review, verify and grade the submission.

Cyber Essentials ‘Plus’

Take your security to the next level with CE+

Cyber Essentials+ (CE+) follows the same principles as CE but with the addition of independent testing which requires an on-site technical assessment.

The self-assessment questionnaire and external vulnerability scan are utilised, as with the Basic level. However, DigitalXRAID use specially, tailored vulnerability criteria, targeting your organisations internet facing infrastructure, workstations and servers.

These tests will highlight any security issues that were not captured in the self-assessment. This will also provide you with peace of mind that your current software builds and software are meeting minimum security requirements.

The time required to complete CE+ depends on the size of your organisation, however a minimum of 3 days will be required in order to complete the assessment, reporting and certification processes.

CE+ is the more extensive Cyber Essential of the two, due to the addition of a technical assessment. By showing you’ve undertaken a more thorough check, you’re providing greater confidence to organisation associates that you’re able to protect your own assets and give due consideration to your cyber security.

Being advocates of best security practice we would recommend CE+ for all organisations of any size. It provides a thorough and impartial validation of your organisation’s present security exposure, giving stakeholders greater assurance.

With either certification, you will decide the systems and devices to be in the scope of your assessment. It may be that you only wish to include the desktop environment and omit mobile (BYOD) devices.

All areas of the CE+ questionnaire are compulsory and guidance on the pass/fail criteria is provided.

On-site Assessment

What to expect

» Production of a report which provides clear, measurable results.

» Award of the certification, if achieved.

The DigitalXRAID approach to CE+ also includes:

» In-depth review and verification of self-assessment questionnaire.

» External vulnerability assessment and scan of your internet facing infrastructure.

» Vulnerability scan of internal systems.

» Email virus delivery check.

» Malicious code web download check.

The self-assessment questionnaire serves two main purposes to your organisation:

» Provides technical scoping information.

» Gives the opportunity to assess your current security measures against industry best practice. The information provided during the certification process can be used to develop your cyber security systems, and should be incorporated into your organisation’s business planning for the future.

Frequently asked questions

I'm not sure on the difference between CE and CE+

CE Plus includes the same requirements as the basic standard, with the addition of a comprehensive on-site configuration and vulnerability assessment. The on-site assessment in combination with the self-assessment questionnaire ensures you are protected against a range of malicious attack scenarios. The independent testing is designed to give you extra peace of mind that your cyber security measures are suitable and sufficient.

CE+ scores highly on tender proposals and demonstrates your companies dedication to Cyber Security. You don't want to be the weak partner in the supply chain.

Should I choose CE or CE+?

Whilst both standards are suitable for any type of organisation, for particularly large or high-risk organisations we would always recommend CE+ due to the extra independent testing involved. Having said that, no matter the size of your organisation CE basic will always cover the necessary compliance for companies in Central Government whose services include the handling of personal information and IT services.

If you're still unsure whether you should go for basic or plus, you can always contact us directly and we'll be more than happy to give our advice based on your organisation.

What systems fall under Cyber Essentials?

Firstly, it's important to say that it remains your choice to determine which of your systems are in-scope. However, for best practice, you should include all end user devices which are connected to the Internet. We would also highly recommend other Internet facing systems, such as email or application servers.

If you need advice regarding the scope, DigitalXRAID can provide guidance by visiting your organisation for an on-site pre-assessment.

I am already certified with an alternative standard. Do I need CE/CE+?

Yes, if you hold certification to other standards, for example ISO, this does not reduce the need for a CE/CE+ assessment, nor does it reduce the requirements of CE standards should you choose to go ahead.

What happens if my organisation fails?

If you fail CE basic you are allowed two weeks to examine the feedback from the assessor and change any simple issues with your network and policies. You can then update your answers and the assessor will perform a second assessment without incurring extra charges. If you fail CE+ the same grace period applies however you will incur a charge for a second on site visit and assessment.

If you still fail after these two weeks you must re-apply and pay the assessment fee again if you decide to continue. However, DigitalXRAID can also provide pre-assessment to give you the best chance of success. We want you pass first time and we offer solutions that will ensure you are ready before you make the application.

How do I maintain my organisation's CE/CE+ certification?

We highly recommend that each organisation maintains the CE or CE+ scheme on a rolling basis, due to the ever-growing number of cyber security threats. Certification is valid for 1 year, annual reassessment will ensure your protection remains up-to-date and benchmarked with any further enhancements to the standard.

Will I receive any feedback?

All clients get feedback on any aspect of the assessment which is not fully compliant. You will get a PDF document of all the answers you gave and comments from the assessor against any that were considered non-compliant.

DigitalXRAID

Contact HM Network
Tel 03333 444 190
info@hm-network.com