dsm SYSTEMS

FORTIS CYBER®

CYBER ESSENTIALS, CYBER ESSENTIALS PLUS & IASME CYBER ASSURANCE CERTIFICATIONS

FORTIS INFORMATION SECURITY & RISK MANAGEMENT

CERTIFICATION BODY CYBER ESSENTIALS

CERTIFICATION BODY CYBER ESSENTIALS PLUS

CERTIFICATION BODY IASME CYBER ASSURANCE

Assured Service Provider
in association with National Cyber Security Centre
Cyber Advisor (Cyber Essentials)

An Introduction to Fortis Cyber®

Fortis Cyber® is an ISO 9001 certified UK based Information Security and Risk Management consultancy

Fortis Cyber® has constructed an arsenal of information security and risk management services, allowing organisations of any size or industry to stay in control of their cyber security. By being able to identify security risks and detect vulnerabilities, companies will be armed with the knowledge required to more easily protect themselves and meet and respond to omnipresent and evolving cyber threats.

Core Values: Trust, Discretion, Delivery, and Privacy

- Founded by a senior cyber expert with 30 years of first-hand experience in the UK Military and Global Enterprise.
- Fortis Cyber® is a trusted partner of the UK Home Office and Police Forces – Cyber Resilience Centre.
- Fortis Cyber® can provide you with access to cross industry skilled, experienced, and certified information security subject matter experts.

The Core Team Members:

- Trusted - All our Consultants are skilled, experienced, and certified professionals, who have an invaluable depth of knowledge in their respective security fields.
- Enterprise Experience - held senior information security architecture and leadership positions for Juniper Networks, Thomson Reuters, Airbus, WorldPay and Atomic Weapons Agency.
- Government Experience - Information Security at government levels, gained from within the UK Defence, UK Home Office, and UK FCO.
- Insight - Security specialists drawn from leading security organisations: HM Forces, global enterprise, and UK intelligence services.

Industry Accreditations and Certifications

Penetration Testing

Vulnerability Assessment

What Is The Cyber Essentials Scheme?

Cyber Essentials is a UK government scheme that sets out five basic security controls to protect organisations against around 80% of the most common cyber attacks.

The scheme's certification process is designed to hep organisations of any size demonstrate their commitment to cyber security - all while keeping the approach simple and affordable.

How Does Cyber Essentials Work?

Cyber Essentials sets out five controls which you can implement immediately to strengthen your cyber defences:

- Use a firewall to secure your internet connection (Firewalls)
- Choose the most secure settings for your devices & software (Secure Configuration)
- Control who has access to your data and services (User Access Control)

- Protect yourself from viruses and other malware (Malware Protection)
- Keep your devices and software up to date (Security Update Management)

What are the benefits?

Most companies rely on digital offerings and services as part of their day to day business, but where there is information technology there is an element of information security risk. These organisations will at some time come under some form of threat from cyber attacks.

This self-assessment and audited Cyber Essentials option will give you protection against a wide variety of the most common cyber attacks. Your Cyber essentials certification will:

- Reassure customers that you are working to secure your IT against cyber attacks
- Attract new business with the assurance you have cyber security measures in place
- Give you a clear picture of your organisation's cyber security level
- Present more business opportunities as many Government contracts require Cyber Essentials certification
- Reduce the risk of your organisation becoming a victim of a cyber attack
- Show your customers that you are committed to the security of their information and help you win their trust

CYBER ESSENTIALS CERTIFICATION

What Does Cyber Essentials Cover?

If you are a company that wants to demonstrate a commitment to safeguarding customer data and ensuring you are guarded against a cyber attack then the CE certification is certainly for you.

Cyber Essentials is appropriate for your business if you want a base-level security certification to demonstrate that you have key technical controls in place and as a company you take cyber security seriously.

Certification Process

The self-assessment questionnaire (SAQ) includes approximately 50 questions related to each of the 5 technical security controls required for Cyber Essentials certification: user access control, secure configuration, security update management, malware protection and firewalls.

The process is simple and depending on your cyber maturity, relatively fast to achieve certification for your company.

Your Simple Route to Cyber Essentials Certification

Fortis Cyber® has a simple methodology to hep you achieve certification:

CE Certification Service Options

The table below shows you the different levels of support available to help you achieve Cyber Essentials certification.

	Do It Yourself	Some Support	Lots of Support
Suitable for	Businesses that are familiar with the CE requirements and have a high degree of IT security knowledge	Businesses that need some help defining the scope and answering the online questionnaire	Businesses that require a lot of support and have no experience of the CE requirements
Includes	Access to the CE Certification questionnaire on the Fortis portal 0 hours consultant-led advice One Retest	Access to the CE+ Certification questionnaire on the Fortis Portal Up to 2.5 hours remote consultant-led advice One Retest	Access to the CE+ Certification questionnaire on the Fortis Portal Up to 8 hours remote consultant-led advice One Retest

What Does Cyber Essentials Plus Cover?

Cyber Essentials Plus (CE+) include an external vulnerability assessment, an internal scan and an on--site or remote assessment. it offers more in-depth testing and therefore stronger assurances of security.

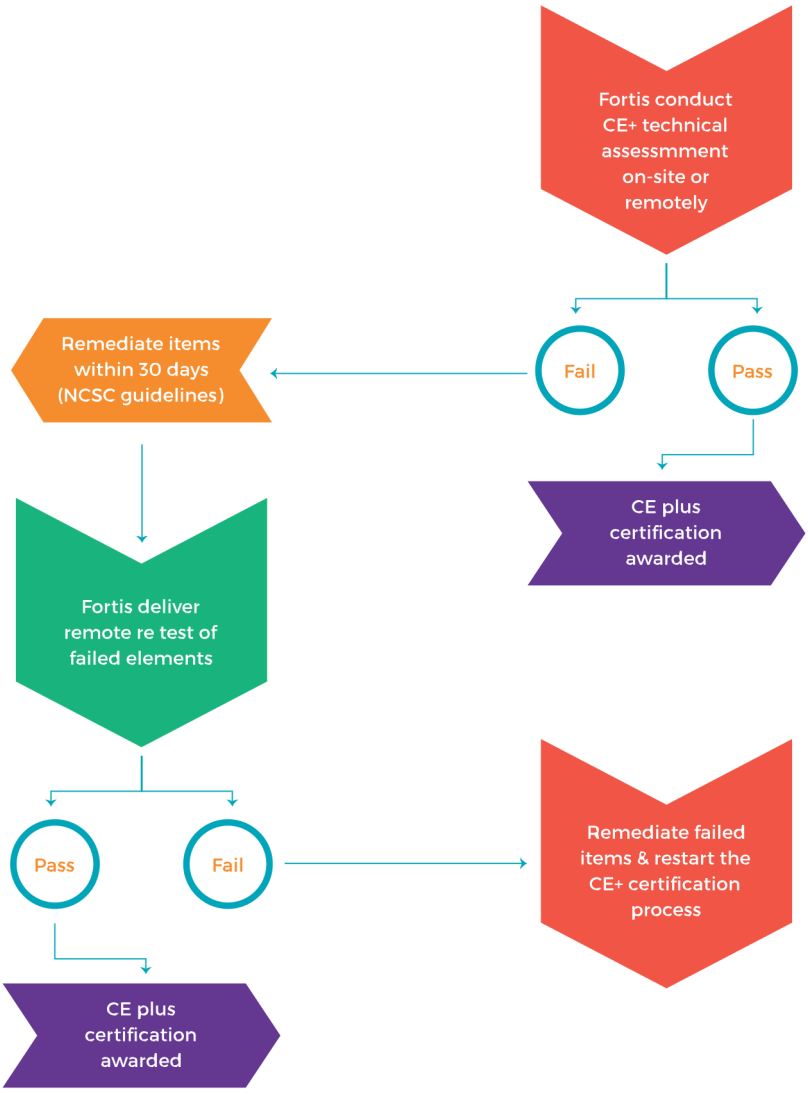
CE+ carries across all elements of Cyber Essentials, including a technical audit of your systems to verify the Cyber Essentials recommended controls are in place.

This higher level of assurance involves completing the SAQ followed by a technical audit of the systems that are in scope for Cyber Essentials. This includes a representative set of user devices, all internet gateways and all servers with service accessible to unauthenticated internet users and virtual desktop environments. Your assessor will test a suitable random sample of these systems (typically around 10 percent) and then make a decision as to whether further testing is required.

You will need to complete your CE+ audit within three months of your last Cyber Essentials basic certification. If you want to gain CE+ straight away, you can complete the CE SAQ as the initial part of the CE+ certification process. Unless it is possible conduct remotely, the assessor will have to visit your head office and a representative sample of your other offices in order to carry out the tests.

The cost of a Cyber Essentials Plus assessment will depend on the size and complexity of your network and devices.

Your Simple Route to Cyber Essentials Plus Certification



CE Plus Certification Service Options

The table below shows you the different levels of support available to help you achieve Cyber Essentials Plus certification.

	Do It Yourself	Some Support	Lots of Support
Suitable for	Businesses that are familiar with the CE+ requirements and have a high degree of IT security knowledge	Businesses that need some help understanding the scope and preparing the environment for CE+ compliance	Businesses that require a lot of support and lack experience in providing a CE+ compliant technical architecture
Includes	Access to the CE+ Certification questionnaire on the Fortis Portal 0 hours consultant-led advice Remote external vulnerability assessment Remote or on-site assessment including: • Authenticated internal vulnerability scan • Malware protection check • End user defences check against malware delivered via email/website One Retest	Access to the CE+ Certification questionnaire on the Fortis Portal Up to 2.5 hours remote consultant-led advice Remote external vulnerability assessment Remote or on-site assessment including: • Authenticated internal vulnerability scan • Malware protection check • End user defences check against malware delivered via email/website One Retest	Access to the CE+ Certification questionnaire on the Fortis Portal Up to 8 hours remote consultant-led advice Remote external vulnerability assessment Remote or on-site assessment including: • Authenticated internal vulnerability scan • Malware protection check • End user defences check against malware delivered via email/website One Retest

Trusted By

Fortis Cyber® helped us to achieve CE+ first time, even during lockdown for Covid-19. Great customer service."

Felix

Director, YGHT Limited

We needed the CE & CE+ certifications for a UK Government contract, but we needed them quickly. Fortis Cyber® responded to our short deadline and we passed both. Thank you."

James

Director, Website Express Limited

What is IASME Cyber Assurance?

The Information Assurance for Small to Medium-Sized enterprises (IASME) Cyber Assurance standard was developed over several years during a UK Government funded project to create a cyber security standard which would be affordable and achievable for small to medium enterprises (SMEs).

The technical controls are aligned with the Cyber Essentials scheme and certification. The IASME Cyber Assurance standard, formerly known as IASME Governance, was originally released in 2010 and has proven very effective for SMEs. It is useful for any SME enterprise that wishes to display commitment to their cyber security policies and procedures.

The IASME Cyber Assurance assessment also includes GDPR requirements and is available either as a self-assessment or on-site audit. By gaining the audited IASME Cyber Assurance certificate your organisation is achieving IASME's highest level of certification and providing assurance to customers and suppliers that your organisation's security has been audited by a skilled, independent third party.

What are the Main Benefits and Objectives of IASME?

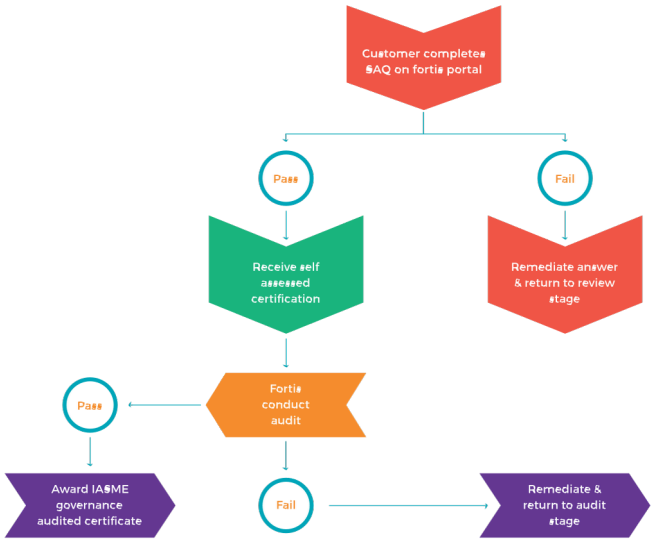
The IASME Cyber Assurance standard is an organised way for a business to implement new ways of securing its information, improve existing ones, and be recognised in its sector for having done so. Implementing the IASME Cyber Assurance standard creates security-aware staff as part of business as usual.

The diagram below illustrates the objectives:

The Fortis Cyber® IASME Cyber Assurance assessors work alongside our ISO certifications team. They leverage synergies for companies that have the ambition to eventually achieve ISO 9001 and ISO/IEC 27001 certifications. This would include more popular subsets such as Cloud Security ISO 27018 and Business Continuity ISO 22301.

Your Simple Route to IASME Certification

The diagram below illustrates this simple process:



Audited IASME Cyber Assurance Certification Service Options

	Do It Yourself	Some Support	Lots of Support
Suitable for	Businesses that are familiar with the IASME Cyber Assurance requirements and have a high degree of IT Security knowledge	Businesses that need some help understanding the scope and preparing the environment for IASME Cyber Assurance compliance	Businesses that require a lot of support and lack experience in providing an IASME Cyber Assurance compliant technical architecture
Includes	Access to the IASME Cyber Assurance Certification Questionnaire on the Fortis Portal No consultant-led advice Remote or on-site assessment including: • an audit of your policies and processes • interviews with members of staff and a review of documentation • assessment of evidence provided to your assessor of you system configuration as per your policy One remote retest	Access to the IASME Cyber Assurance Certification Questionnaire on the Fortis Portal Remote consultant-led advice Remote or on-site assessment including: • an audit of your policies and processes • interviews with members of staff and a review of documentation • assessment of evidence provided to your assessor of you system configuration as per your policy One remote retest	Access to the IASME Cyber Assurance Certification Questionnaire on the Fortis Portal Remote consultant-led advice Remote or on-site assessment including: • an audit of your policies and processes • interviews with members of staff and a review of documentation • assessment of evidence provided to your assessor of you system configuration as per your policy One remote retest

Other Fortis Cyber® Services

Fortis Cyber® has built a suite of Information Security and Risk Management Services to enable organisations of any size or industry stay in control of their cyber security. By being able to identify security risks and detect vulnerabilities, companies are armed with the knowledge to more easily protect themselves, meet and respond to ongoing and changing cyber threats.

Threat and Vulnerability Management

"See the attacker's view of your company"

Vulnerability Assessment scans will map your threat landscape, by identifying vulnerabilities and configuration issues that hackers can use to attack and gain a foothold within your infrastructure. We will prioritise vulnerabilities against your business critical services and report on when those threats are actively exploitable.

This service pairs automated tools with human interaction, providing understanding and analysis on an ongoing basis. Delivered monthly to ensure a constant reduction on a company's risk profile; threats change daily, and systems need to be changed continuously to combat them.

This should be implemented in addition to any existing penetration testing countermeasures you have in place. This external vulnerability scanning will provide additional assurance that your risks are detected, identified and classified across your estate.

Cyber Vulnerability Risk Assessment

"Where is your security risk in the context of business operations"

CVRA is a style of information security risk assessment which includes socio-technical elements. This recognises and measures the interaction between people and technology in workplaces. Traditionally risk assessments haven't included the people working on tech, which is a blind spot for any organisation not assessing the socio-technical component.

In order to effectively target security activities, it is important to understand the holistic risks to businesses. A cyber maturity model should include a modern risk assessment, called a cyber vulnerability risk assessment (CVRA). This offers an enterprise-wide risk assessment of the cyber security posture and awareness of your organisation and highlights key risk areas.

ISO Certification Services

"Win and retain business, stand out from your competitors"

The breadth of our service portfolio enables us to offer a variety of risk management & consultancy support solutions: from a simple one-off gap analysis against a specific standard such as ISO/IEC 27001 or NIST's Cybersecurity Framework, through to complex multi standard integrated management systems projects.

Fortis Cyber® prides itself in achieving a 100% success rate with its clients achieving UKAS Accredited Certification to ISO 27001, 9001, 14001 and many other management systems standards 'first time, every time'.

Fortis Cyber® will continue to work with your organisation beyond certification to support it with the ongoing maintenance of system. Fortis Cyber does this by providing an innovative and pragmatic risk-based approach across the organisation, helping maintain legal obligations, drive down cost and increase profit.

Digital Forensics

"Identify what really happened"

Fortis Cyber® offers a complete, digital forensic investigations package to establish and identify the cause and source of cyber incidents. These events are instigated by internal or external threat actors. These services are carried out by experienced and certified investigators who will utilise versatile and powerful software and technology solutions to undertake digital forensic investigations & data restoration services.

Penetration Testing & Red Team Ethical Hacking

“Taking the vantage point of an attacker and attempting to gain access”

Our Penetration Testing service enable clients to identify, assess and prioritise vulnerabilities and security flaws across their applications & API’s, platforms and infrastructure.

Penetration testing will help to identify security vulnerabilities which might otherwise leave your company open to compromise. Fortis Cyber® has a proven track record in finding such vulnerabilities in some of the most complex, and sophisticated IT environments. The majority of the testers Fortis Cyber® employs work on red teaming engagements as well as penetration testing. This ensures clients receive the highest level of quality, with testers often recognising scenarios that a normal penetration tester wouldn’t have the experience to detect.

The Fortis Cyber® penetration testing and red teaming staff are extremely well certified, holding multiple certifications awarded by bodies such as CREST, Offensive Security and the Tiger Scheme. Fortis Cyber® also complements this focused knowledge with its National Cyber Security Centre (NCSC) CHECK & Certified Cyber Professionals to provide a valuable wider viewpoint to penetration testing assurance.

Incident Response

“Minimise damage, disruption and costs to your business operations”

In the event of a security incident, initial responses and actions undertaken by your organisation will have a direct impact on the level of business disruption incurred. the immediacy and effectiveness of your response will determine how comprehensively your are able to minimise damage, disruption and costs to your business operations.

The Fortis Cyber® Incident Response service has been designed to prepare your organisation through the design and implementation of robust policies, procedures and first responder training specifically tailored to your operational needs. It is important that staff feel prepared and confident to deal with any incident, so planning, preparation and training are key.

Your organisational response to an incident will determine the level of disruption to business operations. When an unexpected incident occurs, having a robust plan in place and staff who know how to implement it will enable your organisation to reduce financial costs and lost productivity, whilst staying in control of the situation.

Please get in touch

www.dsmsystems.co.uk

info@dsmsystems.co.uk

Fortis Cyber Security Limited is a limited company registered in England and Wales.

Company Registration Number: 11162256

VAT Registration Number: 291874659