Service Catalogue 2020

Effective Date: 30.09.2019

Review Date: 30.09.2020

Certification / Compliance

(Assisted) IASME Governance 'STD' Certification – (Price on Application)

The IASME Governance Standard is risk-based and includes aspects such as physical security, staff awareness and data backup. The UK Government recently recognised it as the best cyber security standard for companies. The IASME Governance Standard includes both Cyber Essentials Standard and an official assessment against the General Data Protection Regulation (GDPR), intended to strengthen and unify data protection for all individuals within the European Union.

The IASME Governance Standard, Cyber Essentials and GDPR Readiness is an online self-completing questionnaire, which is certified by a GCHQ Assessor. A CRIBB Assessor will arrange to visit you on two separate days to assist with the understanding, policy fulfilment (all required policies are provided as part of the service) and assessment completion. On successful completion of the IASME Governance, (with Cyber Essentials and GDPR Readiness) your certificates and logos will be issued. As an additional bonus, successful certification will entitle you to Cyber Liability Insurance indemnity through IASME insurers.

Primary Requirements:

- No Unsupported Internet Accessible Systems
- No Generic "User" Login Accounts
- Restriction of Administrative Account Login Day to Day Use
- Standard Business and Information Governance Polices Implemented

Benefits of Service

- Access to Assessment Portal and full brief and explanation.
- Policy Review and Realisation, GDPR Consultation and Q&A Completion Review.
- Advice on Policies and their Understanding with provision of missing policies for all standards.
- Improved overall security and the recommended route for clients looking to achieve additional standards.

(Audited) IASME Governance 'GOLD' Certification* – (Price on Application)

Audited IASME Governance (sometimes known as IASME Gold) is an independent on-site audit of the level of information security provided by your organisation. It offers a similar level of assurance to the internationally recognised ISO 27001 standard but is simpler and often cheaper for small and medium-sized organisations to implement.

*In order to achieve the IASME Governance Audited standard, you must first pass the IASME Governance assisted-assessment.

We will discuss the scope of the assessment with you and arrange a mutually convenient time to visit your organisation's head office to carry out an audit of your policies and processes. This audit usually involves interviews with members of staff and a review of documentation and system configuration. It does not involve a technical assessment, although it may be helpful to have technical staff available to provide evidence to the assessor of your system configuration. The assessor may also wish to visit branch offices or other locations in order to satisfy themselves that your good security practice is reflected across the organisation.

Cyber Essentials Only Certification – £350

Cyber Essentials is a government-backed cyber security certification scheme that sets out a good baseline of cyber security suitable for all organisations in all sectors. An independently verified self-assessment, organisations assess themselves against five basic security controls and a qualified GCHQ assessor verifies the information provided on behalf of the IASME Consortium.

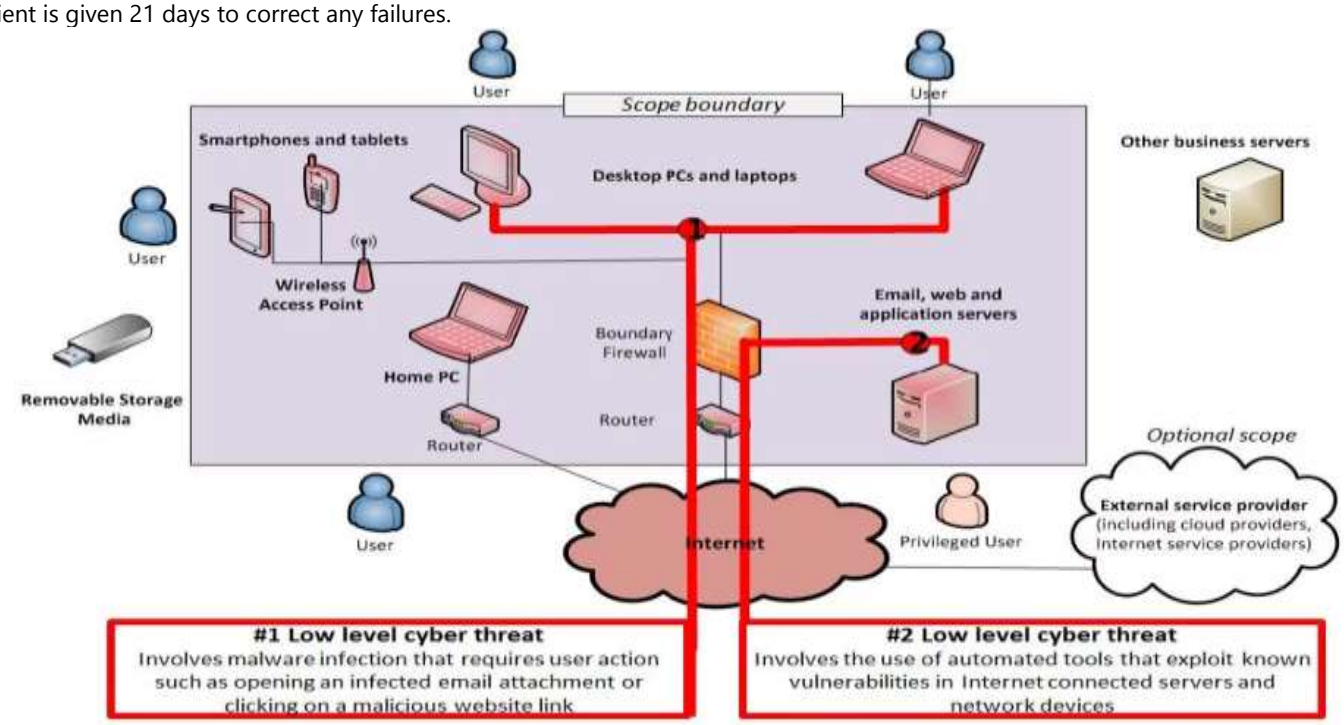
Benefits of Service

- Can help to reduce around 80% of cyber-attacks.
- It shows your commitment to security; demonstrating to your business partners, regulators and suppliers that you take cyber-security seriously.
- It is a mandatory requirement for government suppliers and for all public service contracts.
- It gives you a competitive advantage, particularly in comparison to rivals without accreditation.

Cyber Essentials Plus Certification – (Price on Application)

Cyber Essentials Plus involves 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 services accessible to unauthenticated internet users. The assessor will test a suitable random sample of these systems (typically around 10%) and then make a decision on whether or not further testing is required.

The assessor will need to visit your head office and a representative sample of your other offices in order to carry out the tests. The quantity of other offices visited depends on the complexity of your organisation - in a multinational organisation the assessor may need to visit a number of countries. Some tests may be carried out remotely provided that the agreed on-site visits have been carried out. The client is given 21 days to correct any failures.



CMCA – Cyber Maritime Assurance – (Price on Application)

'CRIBB Maritime Cyber Assurance' – aka CMCA - is a unique and affordable alternative to ISO27001 that was recognised by the leading industry and government sectors to assist in maritime cyber assurance.

The CMCA solution from Ice Technology Services and CRIBB Cyber Security offers clients the chance to increase their protection, to improve their defences, to assess their data protection global-readiness, to help achieve as high a level of compliance as possible and to ultimately aim for a higher profit margin through eliminating inefficiency and tightening up business processes across the board. CMCA guarantees full briefing and consultation throughout the project, assistance with Security Policies, an evaluation of existing 'organisation of information' and a thorough assessment of the current compliance level. There will be an evaluation of the current level of Operations Security, guidance and an assessment on Management, guidance with Subject Access, a review of current policies, procedures and processes – all by an experienced and certified GDPR practitioner – plus assistance with Human Resources and an access Control check. As if there were not enough, you can also expect an evaluation and assessment of Supplier Relationships, Physical & Environmental checks, assistance with Business Continuity Management, a validation of equipment, technical controls and network / cloud, Firewalls and Malware protection, help with managing Security Incidents, guidance on Cryptography and Asset Management advice.

Detection

Vulnerability Review – (Price on Application)

Mid-level vulnerability scanning carried out remotely on behalf of the client to detail cyber security flaws and vulnerabilities both internally and externally and website related. All servers and networks are reviewed with the results detailed in a management and technical report on its completion. If faults are found, details of full corrective solutions are issued which the client can address internally or where required, corrected by a trusted fixer. Vulnerability scanning has five alternate verifications similar to Penetration Testing, although it is not as intrusive in comparison.

Internal

Vulnerability scanning helps an organisation identify and remediate vulnerabilities within their IT environment before hackers and thieves gain access to, modify or destroy confidential information. Our Internal Vulnerability Scanning services help our clients manage their vulnerabilities more rapidly and cost effectively on threats that need addressing either in a Low, Medium or Critical threat status.

External

External vulnerability scanning works along the same lines as the internal scanning option yet looks for holes in your network firewall(s), where malicious outsiders can potentially break in and attack your network.

Web Applications

Checks for potential security vulnerabilities in the web application and architectural weaknesses, performing a black-box test advising on threats in a Low, Medium and Critical threat status.

PCI DSS

To comply with requirement 11.2 of the PCI DSS, merchants and service providers must conduct and pass a quarterly vulnerability test (meaning one scan every 90 days, or 4 scans per year). This service provides the PCI scan certification necessary to demonstrate quarterly compliance and which is applied for both internally and externally relating to all payment gateways.

Unauthenticated Penetration Testing – (Price on Application)

Unauthenticated penetration tests inspect the security of a target system from an outside perspective that doesn't require the need for the login credentials of a user. The services helps determine whether you systems are vulnerable to attack, if the defences were sufficient, and which defences (if any) the tests defeated.

Internal

An Internal Penetration Test differs from a vulnerability assessment in that it actually exploits the vulnerabilities to determine what information is actually exposed. An Internal Penetration Test mimics the actions of an actual attacker exploiting weaknesses in network security without the usual dangers. This test examines internal IT systems for any weakness that could be used to disrupt the confidentiality, availability or integrity of the network, thereby allowing the organisation to address each weakness.

External

An External Penetration Test mimics the actions of an actual attacker exploiting weaknesses in the network security without the usual dangers. This test examines external IT systems for any weakness that could be used by an external attacker to disrupt the confidentiality, availability or integrity of the network, thereby allowing the organisation to address each weakness.

Web Applications

The primary objective for a web application penetration test is to identify exploitable vulnerabilities in applications before hackers are able to discover and exploit them. Web application penetration testing will reveal real-world opportunities for hackers to be able to compromise applications in such a way that allows for unauthorised access to sensitive data or even take-over systems for malicious/non-business purposes.

Consultancy

Data Protection Consultancy – 1 Day Service - £850

The qualified and approved consultants at CRIBB are on hand to help organisations understand what they need to do to comply with the GDPR and all other Data Protection regulations.

Are you worried about GDPR and how it will affect your company?

The General Data Protection Regulation (GDPR) is the biggest and most significant change regarding data privacy in the last 20 years. It involves the protection of personal data that companies retain which can be used to identify an individual, such as name, address, mobile number, IP address and also sensitive data such as gender and sexual preference.

Our expert consultants can help you achieve compliance with the GDPR and other Data Protection regulations. Our GDPR Review service allows us to verify the level of your current compliance and advise on which requirements are missing, so that you can combine this with the work you have already done or are carrying out yourselves. This is with the security of having fully trained and experienced people to back you up as needed.

PCI DSS Consultancy – Starting with 1 Day Service - £850

Organisations storing, processing or transmitting credit card data are required to demonstrate compliance with the Payment Card Industry Data Security Standard (PCI DSS).

The aim of PCI DSS Compliance is to provide assurance to both customers and payment processors such as Visa, Mastercard, Amex and JCB, that adequate IT security controls are in place to reduce the risk of payment card theft and fraud.

CRIBB Cyber Security initiate all PCI DSS projects with a strategy review, assessing which parts of the business are currently in scope for PCI DSS and deciding how to deal with these elements in a cost effective way that reduces risk whilst ensuring that the standard is met.

Our qualified consultants can provide advice, reduce complexity, and manage your journey to achieving and maintaining compliance through our PCI DSS Review Service.

Cyber Security Consultancy – 1 Day Service - £850

The unstoppable growth of cyber-crime means that businesses of all sizes should seriously rethink their approach to the security of their websites and data.

You may think that you are 'too big' to be targeted by a computer hacker yet recent history has taught us that this is simply not true. When you then consider that 60% of small businesses never recover after a serious cyber-attack, it becomes clear that we all need to take this very seriously and we here at CRIBB are here to help.

Our Cyber Security Review service allows us to verify the level of your existing security and then advise you upon the missing requirements you need to put in place. Our professional and highly qualified consultants can play as both the attacker and the defender in computer systems, networks, and software programs.

Our aim is to instil the best practices in Cyber Security deep within your business so that you are fully prepared.

IG Adviser Assistance – (Price on Application)

Unsure on the correct application of information governance within your organisation? Need help completing those data management forms, registers or polices? Then we are the right choice to speak to. Our (IGA) Information Governance Assistants are available to assist you in all matters regarding the management of information within your organisation. Backed up by industry recognised auditors and data protection specialists, our IG Assistants ensure that you are following the correct information governance thereby ensuring that you remain legally compliant and information governed correctly.

DPO as a Service (DPOaaS) – Starting with 10hrs per year - £1000

Our DPO as a Service (DPOaaS) is a cost-effective solution for organisations that don't have the data protection expertise and knowledge to fulfil their DPO (data protection officer) obligations under the GDPR (General Data Protection Regulation). Our certified and internationally-approved DPOs can assist you with all data protection requirements: GDPR 2018, DPA 2018, CCPA 2019, APP 2019, PECR 2003.

By outsourcing DPO tasks and duties to our industry experts, you get access to expert advice and guidance that helps you address the compliance demands of data protection, all the while staying focused on your core business activities.

Software Licence Compliance – Starting with 1 Day Service - £850

Software Licence Compliance (SLC) is focused on avoiding 'under-licencing', by ensuring compliance with licence entitlements – often with (inadequate) focus on the number of licences as compared to software deployments. However, compliance must take into account other licence parameters such as device configuration, geographic location, employee/non-employee status and many others.

The worst thing to do is to react to a software audit without thinking. It is far wiser to involve your in-house legal department and outside licencing consultants so that you can understand how best to respond to the audit notice without exposing your company to unnecessary risks. Software Asset Management (SAM) best practices help you manage licence compliance throughout your organisation. When you effectively track and document your software licences, you lower the risk of non-compliance. It is extremely important to ensure that accounting for capital assets and depreciation is in compliance with the management's objectives.

Our certified assessors can assist in all levels of your compliance that relate to; Software Detection, Licence Understanding, Software Management and requested legal Licencing Audits for Microsoft and Federation Against Software Theft (FAST)) to ensure your compliancy.

Maintenance Support Services

We are able to provide a bespoke maintenance and support agreement for cyber security, data protection and re-certification services. This reduces the costs of your cyber security budget whilst ensuring your cyber security and data protection compliance remains a primary goal – please contact us to discuss further.