netcom
Managed IT Services

Get Your Business Ready for GDPR With Cyber Essentials and IASME Governance

Options & Pricing Guide

HM Government

Netcom are an independent authorised Cyber Essentials and IASME certification body

The Need to be Secure and Ready for GDPR

On the 25th of May 2018, the new European Union General Data Protection Regulation (GDPR) comes into effect, becoming law in 28 Countries simultaneously.

GDPR introduces new obligations and rules for any organisation that holds or handles data of EU Citizens regardless, of their geographical location. It also applies much stricter measures for the control of data, increasing the responsibility of organisations around data security and for the first time, reporting a data breach becomes Law.

Companies will also need to be able to demonstrate actions and measures that have been taken to comply with the rules, and show how they are managing data. A Failure to be able to do so may result in fines that far exceed those previously awarded and pose a credible threat to many SME businesses.

Why the Laws are Changing

The UK has not seen an evolution of the Data protection laws in over 20 years, the last significant change being the introduction of the Data Protection Act of 1998. Since this time, we have seen significant advances in technology in hardware, software, mobile devices. In 2017 the amount of data we give and receive has reached epic proportions and for some businesses has become a currency to trade.

The Data Protection Laws have not significantly changed since

- The emergence of Google in 1998
- The launch of Amazon in 1998
- The launch of Facebook in 2004
- The first-generation iPhone in 2007
- The fist Kindle tablet in 2011

The type and volume of data that companies now hold about us is massive, technology now records our locations, usage and even how many steps we take. Do we know how this is being used, processed or shared? The likely answer is no. This is why a major shake up to protect the individual's right to privacy and protection is overdue.

Add to this the ever-increasing cyber threats, that have risen to record levels with 40% more data breaches reported in 2016 than in the previous year (many have gone unreported) and the high profile and leaking of sensitive information. The world of 2017 is a far more connected and data led world than back in 1998.

The new regulations have been designed to bring data protection laws into the 21st century and re-address the balance of power, handing some control back to the individual.

Why GDPR Does Apply to You

Many organisations are unclear as to the full scope of GDPR and often believe it doesn't apply to them or their business activities. This is not the case. The scope of personal data far exceeds any previous laws, and also includes digital information such as IP addresses and biometric data such as fingerprints. If you hold or categorize any information such as HR records, CRM contacts, customer and supplier contacts, these will fall within the Scope of GDPR and **you will have to be complaint**

To truly understand how GDPR will affect you, you need to think about the following question

Do you Process either as a Controller or Processor, the Personal Data of any data subjects who are in the European union (regardless of where the processing takes place?

An example of the key definitions are below.

Process

Means any operation that is performed on personal data, regardless of automated or not. This includes the collection, recording, organisational structuring, storage, adaptation or altering, retrieval. As well as consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination restriction, erasure or destruction of any personal data.

Controller

Means the natural or legal person, public authority agency or other body which alone ,or jointly with others, determines the purpose and means of the processing of personal data ; where the purpose and means of such processing are determined by union or member state law, the controller or specific criteria for its nomination may be provided for by Union or Member state Law.

Processor

Means the natural or legal person, public authority , agency or other body which processes personal data on behalf of the controller. Any organisation may be a controller or a processor depending on the circumstances of the data processing. A controller can contract multiple processors and a processor can contract sub processors.

Personal Data

Means any information relating to an identified or identifiable natural person (Data Subject); who can be identified, directly or indirectly, in particular by reference to an identifier such as Name, and identification number, location data, and online identifier or to one or more factors to the physical, physiological, genetic, mental, economic, cultural or social identify of that person.

Debunking the Common GDPR Myths

Since the announcement of GDPR there has been much speculation about what this will look like and how it will affect organisations. This has resulted in a number of myths being created that are still in circulation, even though the Information Commissioners Office (ICO) has corrected these.

Myth #1 - GDPR only applies to Personally Identifiable Information (PII)

Fact

Under GDPR, personal data even applies to IP addresses and tracking cookies. It is important that organisations treat non personally identifiable data as personal data. The reason for this is that any data that could be used to distinguish one person from another and could also used for de-anonymising anonymous data could be considered Personally Identifiable Data (PII)

Myth #2 - Information on a business card is not in scope for GDPR

Fact

If a business card only has information that is generic to an organisation such as an email address that is info@ or Account@ and has a generic telephone number this would not be in scope for GDPR. The reason is that this data does not point to a naturalised person.
If however the business card contains a email address of the individual or a mobile number this information is deemed to be personally identifiable and therefore is covered under the scope of GDPR.

Myth #3 - Everyone needs a Data Protection Officer (DPO)

Fact

DPO's need only be appointed if a) your are a public authority or b) Your organisation engages in large scale monitoring or processing of personal data. If you do not fall into these categories you do not have to appoint a DPO.
In the interest of best practice, we would recommend having someone in the organisation undertaking the role of DPO and taking responsibility for data compliance.

Myth #4 - Controllers don't need data processing agreements with processors because GDPR imposes direct obligations on data processors.

Fact

Data processing agreements are vital to any data controller and processing relationships as this provides the understanding and binding terms that both parties will adhere to whilst working with the data. However the controller is ultimately responsible , so if the processor acts in a negligent way the controller will be liable.

netcom
Managed IT Services

Options and Pricing

Three Steps to Get Your Business Ready

With our three-step approach to Security, Governance and GDPR your business is well on its way to demonstrating that it has taken steps to mitigate risks, addressed process and educated the business to the needs of GDPR and data security.

Step One - Cyber Essentials Certification

The Cyber Essentials standard was developed over several years with government backing to create a cyber security standard which would be affordable and achievable.

Cyber Essentials delivers peace of mind, allowing you to focus on your core business activities, safe in the knowledge that you have mitigated the vast majority of Cyber-attacks.

Show You Take Security Seriously

Demonstrate to clients, suppliers, investors and Insurers that you take your duty of care seriously, and have taken precautions to firm up security and reduce risks. This will also show the Information Commissioner Office (ICO) that you have taken reasonable steps, to help to secure systems from Cyber Risks.

Access New Markets or Opportunities

Cyber Essentials also enables organisations to fulfil criteria for government projects/contracts. With CE Certification, becoming mandatory for many UK Government contracts and private sector organisations.

Reduce Costs

Many insurance companies are now looking to reward companies that invest in lowering the risks around cyber security, and some now offer reduced premiums to business that hold CE certification.

Once completed you also receive 12 months free Cyber insurance.

The Five Pillars of Cyber Essentials - Keeping You Secure

Secure Configuration

To ensure that all computers and networked devices are configured to the appropriate standards. This can also identify systems or data that is no longer required and can reduce storage requirements and security vulnerabilities.

Boundary Firewalls and Internet Gateways

Protecting your business requires secure digital perimeters and boundaries to prevent unauthorised access to and from private networks. Good set up of these devices either in hardware or software form is important for these to be fully effective and deliver the right levels of security.

Access Control and Administrative Privilege Management

Firming up and securing access to key systems negates the opportunity for employees to install software and minimises the threats of internal attacks, mistakes and inside threats.

Patch Management

Having appropriate patch management not only improves your systems and software but also closes security vulnerabilities that can be exploited by cyber criminals. Having up-to-date and correctly patched devices, also improves resilience, employee performance as systems run more efficiently.

Malware Protection

Protecting your business against malicious malware is a clear “must have” when it comes to security. This however is often over looked and can result in systems or devices becoming infected and having to be taken off-line. Appropriate malware protection will reduce the risk of such incidents.

netcom
Managed IT Services

Three Steps to Get Your Business Ready

Step Two - IASME Governance

IASME® Consortium

The IASME Governance module takes your Cyber Essentials Certification and reinforces this by looking in more detail at your business information, processes and procedures, identifying key areas to deliver improved security throughout the business.

This incorporates additional topics not covered by Cyber Essentials, that will be required for GDPR readiness, such as assessing business risks, training staff, dealing with incidents and handling operational issues.

As a result of undertaking IASME Governance you may identify GAPS in current working and procedures that will need to be addressed internally or externally to ensure you implement the right process for managing security within an audit-able framework.

Step Three - GDPR Readiness

In addition to IASME Governance, the GDPR readiness module starts to address key areas and processes needed to get your business ready for the new EU legislation.

This is delivered by a set of questions to audit your current systems and processes to meet the recognised standards to achieve GDPR readiness.

ico. Information Commissioner's Office

More information on the General Data Protection Regulations can be found by visiting the Information Commissioners Office www.ico.org

Three Routes to Certification

Becoming certified offers many advantages, such as being able to demonstrate to stakeholders and authorities such as the ICO that you take Cyber Security seriously.

Certification can also deliver you competitive advantage over competitors who are not certified as well as reduce your risks of cyber-attack by 80%

Netcom can help get you certified and have a great range of options to help you achieve Cyber essentials and IASME certification, helping to get your business ready for GDPR and having a recognised standard backed by industry.

Our options have been built around identified business needs, experience and available internal resources.

If you are not sure what the best option is for your business? Our team will be able to guide you to the option that will best suit you.

Self Certification - Do it Yourself

With our Self Certification option, you will receive access to a dedicated portal where you will be able to access the required question set for certification.

Once completed, simply submit for assessment and certification through the portal.

Guided - Get a Little Help

With our Guided option, you will receive the required portal access and self-assessment questionnaires that need to be completed.

Once you have completed your questionnaire submit this to us and our team of IASME experts will review and make recommendations before this goes for final submission.

This option gives you the added benefit of ensuring everything is correct before final submission and will highlight any areas of non-compliance that will require work to meet certification standards before final submission.

Once completed we will submit this to IASME for certification

Supported - Get a Lot of Help

With our Supported option you will benefit from our team managing your CE and IASME journey guiding you through each of the required steps.

Our team of experts will also work through the required questionnaires giving you support and guidance to make the entire process as simple as possible.

Once complete we will undertake pre-submission checks to and work with you to ensure all areas required to achieve certification have been achieved.

Cyber Essentials - Self Certification

Our Self-Certification option allows organisation to deliver Cyber Essentials certification in-house.

If you have experience working within frameworks and standards, the self certification route allows you to undertake the certification at your own pace, and use the provided portal to submit for certification.

The Cyber Essentials, Self-Certification package includes

- Access to your own assessment portal for submissions
- Self Assessment Questionnaire (SAQ) for completion
- Submission to IASME for certification

How This Works

1. You will receive log in details for your online Portal
2. Within the portal complete your self-assessment questionnaire (SAQ).
3. Once completed, submit your SAQ for review through the portal.
4. Subject to a positive outcome, we will issue your Cyber Essentials certificate.
5. If Successful you will also receive your Free Cyber Indemnity Insurance from IASME

Cyber Essentials
IASME Governance and GDPR - Guided

As an IASME accredited certification body, Netcom can provide you with the levels of support and expertise you need to achieve the Government Cyber Essentials certification and IASME Governance inclusing GDPR readiness certification.

Our Guided option, is great for organisations that have experience in delivering certifications or standards for the business and allows you to achieve Cyber Essentials Certification on your first attempt.

The Cyber Essentials, Governance and GDPR Readiness Guided package includes

- Access to your own assessment portal for assessment and certification
- All required Self assessment questionnaires (SAQ) for the IASME modules
- Pre-Submission checks to ensure you "Pass first Time"
- Feedback and guidance on areas that require additional attention and focus
- Submission for certification
- Award of Cyber Essentials certificate and Free Cyber Indemnity Insurance

This combination of products and services will help you to work through each step of your journey to a secure, IASME certified and prepare your business for GDPR.

How This Works

1. Once registered you will receive access to your dedicated Online portal.

2. Within the portal you will have the required Self assessment questionnaires for completion. Work through these and answer all of the questions.

3. When all questions have been completed, our IASME team will review and mark your submission. At this stage we will provide feedback on any areas of non compliance that will require attention.

4. Once you have made the necessary amends, resubmit for review and we will repeat step 3, until we are ready to pass for final submission*

5. Once successful you will receive your Cyber Essentials certificate, certification badges for marketing and details of your free Cyber Indemnity insurance.

conditions

*Fair Usage Policy Applies

Additional remote or on-site consultancy is available for an additional charge.

Cyber Essentials
IASME Governance and GDPR - Supported

Without experience or in-house expertise, Cyber Essentials can be challenging, especially for organisations that have limited experience with frameworks, certification and standards.

Our Supported option removes this worry and allows you to achieve Cyber Essentials Certification on your first attempt.

The Cyber Essentials, Governance and GDPR Readiness supported package includes

- Access to your own assessment portal for assessment and certification
- All required Self assessment questionnaires (SAQ) for the IASME modules
- We work with you to complete the detailed self assessment questionnaires
- External vulnerability scan and report
- Pre-Submission checks to ensure you "Pass first Time"
- Feedback and guidance on areas that require additional attention and focus
- Submission for certification
- Award of Cyber Essentials certificate and Free Cyber Indemnity Insurance

This options removes the worry and complexity and allows you to complete your certification with the benefit of support from our IASME team

How This Works

1. Once registered you will receive access to your dedicated online portal.

2. Within the portal you will have the required Self assessment questionnaires for completion.

3. One of our IASME consultants will contact you to make the arrangements and work with you and your team to complete the necessary questionnaire.

4. The Netcom IASME team will review and mark your submission providing feedback and guidance on any areas of non compliance that require further attention before submitting for final certification.

5. Once any required amends are made, we will submit the application through the portal for Assessment and certification.

6. Once successful you will receive your Cyber Essentials certificate, certification badges for marketing and details of your free Cyber Indemnity insurance.

conditions

The price is applicable to SMEs with 30 staff or less and a single location
Additional remote or on-site consultancy is available for an additional charge.

If you have more than 30 staff or multiple locations please call us to discuss options

Options and Pricing

Do it Yourself

Cyber Essentials - Self Certification

£300

What's Included

> We register your organisation for Cyber Essentials
> Access to a dedicated portal with the Online Self Assessment Questionnaire
> Submission to IASME for certification
> Subject to compliance we award your Cyber Essentials Certificate
> Once successful you will receive Free Cyber Indemnity Insurance

Guided

Cyber Essentials, IASME Governance & GDPR Readiness

£799

What Included

> We register your Organisation for Cyber Essentials, IASME & GDPR
> Once completed we will review your online Self Assessment Questionnaires (SAQs)
> We conduct Pre Submission checks and provide guidance on what needs attention/focus to achieve certification, ensuring you can **"Pass First Time"**
> Submission to IASME for certification
> Subject to compliance we award your Cyber Essentials Certificate, IASME & GDPR
> Once successful you will receive **Free Cyber Indemnity Insurance**

Supported

Cyber Essentials, IASME Governance & GDPR Readiness

£1450

What's Included

> We register your organisation for Cyber Essentials, IASME & GDPR
> We work with you to complete the detailed Self Assessment Questionnaires (SAQs)
> We undertake an external vulnerability scan
> We provide a GAP analysis of any areas that require focus
> We complete Pre Submission checks ensuring you can **"Pass First Time"**
> Submission for IASME for certification
> Includes Free **documentation pack** with templates and tools to help certification
> Subject to compliance we award your Cyber Essentials Certificate, IASME & GDPR
> Once successful you will receive **Free Cyber Indemnity Insurance** *
> Up to 30 users and a single location **

All Prices quoted are subject to our standard terms and conditions of sale.
* Free Insurance provided by IASME details available on request.
| ** If your organisation has more than 30 users or multi-location please call for details.

Additional Options and Support

Education

Staff Awareness Training - Cyber Security

£30 per user

Whilst documents and processes are imperative, human behaviour is often the key factor in any data breach. With our online "CyberSecure" training, you can ensure that staff are aware of the daily cyber risks facing businesses and understand ways to identify and reduce these risks.

Our Cyber Secure staff training works for everyone in your organisation, from Reception to Directors and will help to identify bad behaviors and re educate staff to ensure they are fully aware of how to prevent cyber threats.

CompTIA CYBERSECURE

Support

Technical/Network Engineer

Additional resources may be required from the Netcom Technical team. This support will be charged at our normal rates.

£75 per hour

Support

On-site Consultancy

You may want additional onsite support and consultancy from our IASME experts to help on your journey.

£800 per day

www.netcomtech.co.uk

For More Information Call 0114 361 0062
email: info@netcomtech.co.uk