MASS

A COHORT PLC COMPANY

CYBER SECURITY

Safeguarding your information and reputation against cyber threats

Cyber essentials and the DCPP

Cyber security training cyber threats

Contents

Introduction to Cyber Essentials (CE)

Stories of organisations exposing customers' information to cyber threats continue to create headlines in the media, it is becoming increasingly important to not only maintain a robust cyber security stance but also to demonstrate this to their stakeholders.

Government requires all suppliers bidding for certain sensitive and personal information handling contracts to be certified against the CE Scheme.

CE is the Government-backed cyber security certification scheme that sets out a baseline of cyber security suitable for all organisations. The scheme's five security controls prevent around 80% of cyber attacks.

The CE scheme has been developed by Government and industry to fulfil two functions:

- To provide a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based attacks
- Through the Assurance Framework, to offer a mechanism for organisations to demonstrate to customers, investors, insurers and others that essential precautions have been taken.

CE Concentrates on 5 Key Controls

Secure Configuration

Boundary Walls and Internet Gateways

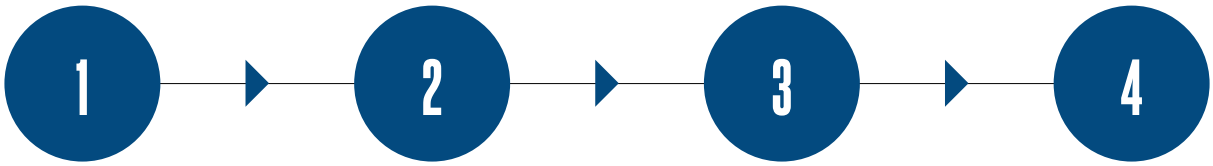
Access Control and Administrative Privilege Management

Patch Management

Malware Protection

CE Concentrates on 5 Key Controls

Cyber essentials basc (stage 1)



Systems in scope for certification are decided between the organisation and IASME Certifying Body

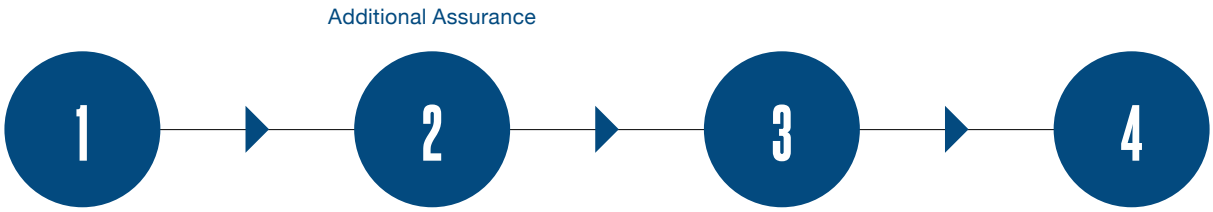
The organisation fills in a questionnaire to self-assess their implementations of the CE control themes

IASME Certifying Body scores the questionnaire

IASME Body issues the certificate

CE Basic certification is awarded on the basis of an independently verified self-assessment questionnaire. Organisations assess themselves against the five security controls. The questionnaire is then verified by a Certification Body to assess whether an appropriate standard has been achieved, and certification can be awarded.

Cyber essentials plus (stage 2)



Systems in scope for certification are decided between the organisation and IASME Certifying Body

IASME Certifying Body performs both an internal and external vulnerability scan (via remote and on-site testing).

IASME Certifying Body scores the questionnaire and vulnerability scan and determines a pass/fail result

IASME Certifying Body issues the certificate

CE Plus offers additional independent assurance that an organisation is complying to Cyber Essentials through both internal and external tests of the organisation's network and computers. These tests are more stringent than CE Basic (Stage 1).

DCPP CSM

The CSM recognises that the level of risk is not the same for all work done in defence and therefore specifies different controls, depending on the risk identified. All companies in the defence supply chain will be required to follow the CSM process but the controls this requires them to apply will depend on the level of risk.

DCPP has published cyber risk profiles which set out controls and measures that apply at various levels of cyber risk. There are 5 possible outcomes from the risk assessment ranging from ‘Not Applicable’ to ‘High’, it is not expected that many contracts will fall in the ‘Not Applicable’ category.

Stage 1 - Risk Assessment

To be conducted by contracting authority; - this could be MOD, or a defence supplier, sub-contracting elements of work.

Stage 2

MASS recommended minimum

Not applicable	Very low	Low	Moderate	High
No action required	Cyber essentails	Cyber essentials plus	Cyber essentials plus	Cyber essentials plus
		+16 low controls	+16 low controls	+16 low controls
			+16 moderate controls	+16 moderate controls
				+11 high controls

Stage 3 - Assessment compliance and monitoring

Use the MOD supplier assessment tool to provide evidence against your risk standard

Stage 4 - Assessment compliance and monitoring

MOD to monitor/audit continued compliance

Cyber Essentials and the Defence Cyber Protection Partnership (DCPP) Model

There is no doubt that cyber threats are real. The MOD is committed to ensuring that their supply chain is appropriately protected. The MOD has been working jointly with Industry and other Government departments in the Defence Cyber Protection Partnership (DCPP) to develop a proportionate means of achieving this.

From 1st January 2016 all MOD identifiable information transferred from customer to supplier or generated by a supplier, specifically in support of the MOD contract, requires suppliers to have a Cyber Essentials (CE) certificate by the contract start date at the latest, and for it to be renewed annually. This requirement must be flowed down the supply chain.

The DCPP Cyber Security Model (CSM) requires some suppliers to ensure additional cyber security controls are in place ahead of contract award.

Cyber security training why choose MASS?

The cost of a single cyber security incident can easily reach six-figure sums and any damage or loss to a company's reputation could lead to dramatic loss of profits or future business.

Cyber security training fundamentally underpins the security mechanisms in place to protect corporate assets.

Cyber security is now fundamental to the ability of any organisation to prosper in an increasingly complex and rapidly developing online world. The benefits of having appropriately trained staff will be immediately apparent on the bottom line.

MASS has an advanced training capability, combining specialist trainers, courseware development, and deep cyber security domain experience. This combination has allowed us to develop a range of courses tailored to the real and practical risks that companies, local government and central government departments face, and keep them up to date with the most advanced methods of instruction.

We have been trusted to design and build some of the UK Government's most secure IT systems for more than 30 years, and continue to keep those systems secure in the face of ever more complex threats.

MASS cyber security training courses

All courses can be delivered in our state of the art training facilities in Lincoln, or if preferred, our team will travel to your premises. Course costs are dependent on location.

Our Information Assurance (IA) professionals have experience developed over many years engaged in various security positions across Defence, the Public Sector and Industry. All our IA professionals are CESG Certified Professionals and members of the CESG Listed Advisor Scheme (CLAS).

Our own holistic approach to cyber security looks at technical security, policies and procedures as well as the people who use the systems. This approach has enabled us to produce security training material that will provide staff at a variety of levels with an understanding of the threats to information and the countermeasures they can adopt to better protect company information assets.

General security awareness training

The cost of a single cyber security incident can easily reach six-figure sums and any loss to a company's reputation could lead to dramatic loss of profits or future business. Security Awareness fundamentally underpins the security mechanisms in place to protect corporate assets. The awareness modules outlined below can be selected as required and delivered as individual sessions or 2 or more combined to provide a more robust insight into the threats associated with IT systems and the risks to information security.

The course provides company staff with an understanding of the threats to security and the measures they can or should adopt can greatly reduce the risk of security breaches.

Course modules

The threat

An overview of cyber threats to organisations, outlining the impacts of cyber security incidents as well as tactics and strategies to aid cyber defence.

Physical security

Gives computer users a basic understanding of the layers of defensive tactics employed to protect information and information systems.

Passwords

Designed to provide users with an understanding of the importance of strong passwords along with some simple techniques to assist users in choosing and managing their passwords.

Data / information security

An overview of data and information security best practices, including data classification, data transfer and storage as well as providing an overview of data protection legislation and international standards.

Home computer security / home working

Provides additional guidance for protecting systems and data within a user's home network environment, including firewalls, update and backup strategies.

Mobile working

Intended to provide an understanding of the additional threats to systems and data when working remotely. Guidance on preventative measures is drawn from public best practices.

Bring your own device (BYOD)

This module aims to introduce users to the growing trend of BYOD, analysing the pros and cons as well as providing guidance on BYOD policy considerations.

Communication security

An introduction to the threats posed to communications by the use of e-mail, Wi-Fi, Bluetooth and radio frequency identification. This module intends to give users an overview of how weaknesses in these technologies can be mitigated.

Browsing / safe internet use

This module will discuss the relative similarities of the common web browsers, how they work and the threats posed to web browsing. Guidance and information about resources to assist users in safe internet use.

Phishing

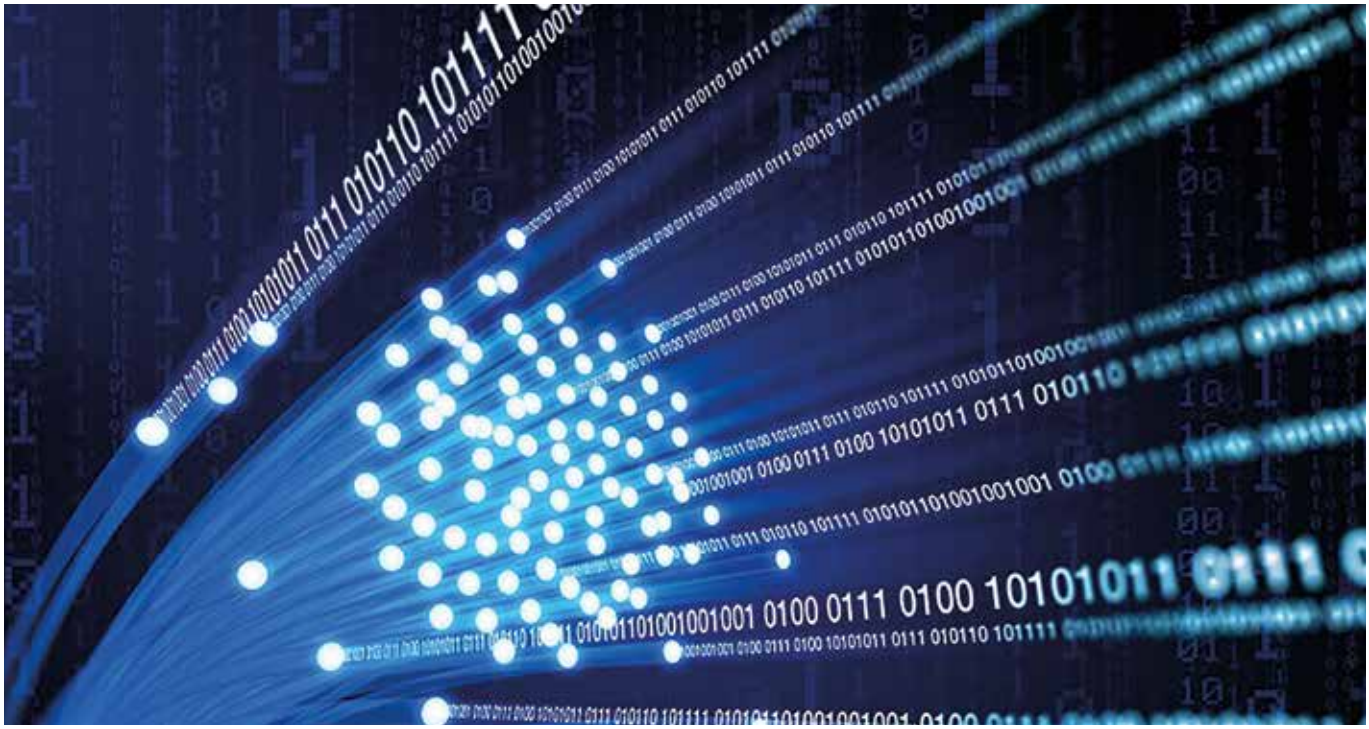
This module takes a detailed look at what phishing is, why it poses a threat and how users can minimise their exposure to phishing attacks.

Course Duration

Module length varies from 30 minutes to 70 minutes but can be tailored to fit with an organisation's requirement. The entire course is therefore configurable from half a day to one day.

Entry Requirements

Each module can be further tailored to target particular audience groups.



Reducing the Cyber Risk 10 Key Steps

In 80% of cyber attacks, it is considered that basic risk management would have prevented the attack. By taking steps to review and invest to improve security in a number of key areas, your business can concentrate their efforts on defending against the remaining 20% of attacks. This course will consider the 10 key areas for managing the risk to information and provide guidance and a methodology to aid in the development of policies & processes.

Course content

The information risk management regime

Understanding risk appetite and engaging the board in risk management decisions.

Managing user privileges

Considerations of user access rights and highly privileged accounts.

Secure configuration

Developing patching strategies and assessing vulnerabilities.

Network security

Policing the network perimeter and testing the security controls.

Monitoring

Implementing monitoring strategies and policies.

Removable media controls

Limiting the use of removable media and producing policy to support this.Incident management
Establishing and obtaining approval for incident management plans.

User education and awareness

User security policies and awareness training.

Malware protection

Establishing anti malware defences and developing policies.

Home and mobile working

Creating appropriate policies and applying baseline builds to limit the associated risk.

Course length

3 – 5 Days.

Entry criteria

This course is aimed at IT Managers or Information Security Practitioners.

Privacy Impact Assessments

The 2008 Data Handling Review, which was commissioned by the Government as a result of two major personal data losses, reported in June 2008. One of the mandatory requirements was that Privacy Impact Assessments (PIA) must be conducted on certain initiatives.

Attendance on this course will enable students to meet legal obligations in terms of the Data Protection Act 1998 a Privacy Impact Assessment which must be conducted on any new and in-service project.

Course content

Background information on the privacy impact assessment

Privacy explained, the PIA process and compliance with the data handling review.

How to determine if a PIA is needed

The PIA screening process – identifying key characteristics of a project.

Identifying personal and sensitive personal data

Interpreting the Data Protection Act 1998 and the 8 data protection principles.

Managing a privacy impact assessment

Roles, responsibilities and resources.

Conducting a privacy impact assessment

Exploring the phases, tasks within phases and deliverables.

Data protection compliance checklist

Determining whether personal data on a system is afforded appropriate protection.

Course length

2 Days

Entry criteria

This course is aimed at information asset owners, data protection officers, IT Managers and Information Security Practitioners.

Developing a forensic readiness plan

Forensic readiness is the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation.

How an organisation's staff initially reacts when discovering a security breach is of paramount importance. Without a formal forensics readiness plan, digital forensic evidence could be tampered with, changed, mismanaged or lost completely causing any post incident investigation to stumble or fail.

This course will demonstrate the importance of such a plan, its goals and benefits, whilst giving clear guidance on the concepts, key principles and the plan's formulation.

Course content

Introduction and background

Introduction to digital forensics.

Concepts and overview

Defines the key terms associated with forensic readiness and gives an overview of how these should be adopted by an organisation.

Business drivers

Benefits of having a forensics readiness plan, risks of not having one and costs associated with forensic readiness.

Common principles

Looks at the common principles of forensic readiness and how organisations should consider the extent of applicability of each principle.

Development of plan

An overview of key content and associated planning practices required for the creation of a suitable forensic readiness plan.

Course length

1 – 2 Days.

Entry criteria

This course is aimed at IT Managers or Information Security Practitioners.

Government incident management requirements

In the high tech world of today, security incidents are inevitable. When they occur organisations need to have the ability to identify, assess and manage the response quickly and efficiently. In order to achieve this, a pre-planned strategy with full support from senior management, well-rehearsed processes and formal procedures need to be in place to minimise the business impact of such events.

This course will cover key principles and approaches to security incident management, implementation, reporting and in some cases mandatory legal requirements and activities.

Course content

Introduction and overview to HMG incident management

A look at business drivers, responsibilities, accountabilities and standards.

Key common principles

Examine the five significant principles for an effective incident management capability.

An holistic approach

Understanding how security weaknesses in one area could have a profound effect on other areas.

Implementation

What to consider when deciding on the best implementation of security incident management for your organisation.

HMG requirements, documentation and points of contact

Clarification of formal requirements, accountabilities and official documentation.

Support agencies

Information and contact details of HMG support agencies.

Support documentation

An overview of available support documentation.

Course length

1 – 2 Days.

Entry criteria

This course is aimed at IT Managers or Information Security Practitioners.

Protective monitoring – interpreting HMG good practice guide 13

Protective Monitoring is a set of business processes, using essential support technology, which is required in order to properly oversee how ICT systems are being used and provide suitable accountability for when those systems are abused.

This course demonstrates how the provision of an effective monitoring and alerting framework is an essential contribution to the successful treatment of information security risks in accordance with HMG Good Practice Guide 13 (GPG 13).

Course content

Understanding the key principles of protective monitoring

Strategy, policy, value, provisioning, resourcing, documenting, reviewing.

Understanding the benefits of protective monitoring

Compliance, risk management, reporting, situational awareness, accountability, network defence.

Protective monitoring processes

Understanding the three core processes and further subsidiary processes.

Applying PMCs based on applicability

Understanding the application of PMCs in accordance with the baseline control set and segmentation model.

Constructing a solution

An overview of current techniques and technologies.

People and processes

Establishing supporting processes and roles.

Information security incident management and forensic readiness

Guidelines for the implementation of information security incident management and forensic readiness plans.

Course length

2 - 3 Days.

Entry criteria

This course is aimed at IT Managers or Information Security Practitioners.

Encrypting data – understanding government requirements

The loss of a single laptop or piece of media that does not employ any encryption could cost an organisation up to £500,000, & cause significant loss of reputation The ICO recommends that organisations using portable equipment to process or transfer sensitive and personal data should encrypt the devices or media using approved products. This course will introduce best practice considerations for encrypting data at rest or when transferring bulk quantities of data.

Course content

Why is encryption necessary?

Introducing the various recommended best practice and mandatory requirements to practitioners as well as demonstrating why unencrypted devices such as laptops are susceptible to data compromise.

Determining the level of encryption required

Introducing the business impact levels to aid classification of information and what levels of encryption are applicable to the impact levels.

Encryption standards

We take a look at the federal information processing standard and discuss each level of the standard as it applies to encryption solutions. This module will help to define which FIPS compliant solutions can be applied to information of different impact level.

Media encryption for physical transfers

Alternative solutions for encrypting data on physical media, including the use of file encryption, full disk encryption and hardware or software solutions.

Course length

1 Days.

Entry criteria

This course is aimed at IT Managers or Information Security Practitioners.

Managing an IT health check / penetration test

Penetration Tests can include a large amount of activities against a multitude of potential targets. Managing these activities effectively will increase the effectiveness and benefits of such a test. It may also help prevent any one of these activities having a catastrophic effect on the system, thus affecting the productivity of your organisation resulting in loss of revenue and reputation. The information gathered can be used to provide management with assurance in regard to the secure nature of the system or justification for further investment of security measures if required. Attendees on this course will learn how to safely and effectively conduct an IT Health Check/Penetration Test.

Course content

Planning

How to formulate a test strategy.

Choosing the right type of test

How to assess the level of assurance required.

Develop the Scope of Work

Identification of attack vectors, targets of attack and application assessments.

Out of scope

Consider what should not be included in the test.

Pre engagement

Identify what agreements should be in place before the start of the test.

Wash-up meeting

Assess results, plan any remedial action, identify and report any remaining risks.

Course length

1 – 2 Days

Entry criteria

This course is aimed at IT Managers or Information Security Practitioners

Gaining List X compliance

In order for any contractor to be able to hold government protectively marked assets at their premises, the contractor is required to achieve List X status for that site.

This course will identify the mandatory requirements, baseline controls, roles and responsibilities which have been designed to flexibly provide appropriate levels of protection for sensitive government assets and help to achieve List X status.

Course content

Understanding the responsibilities of the Board of Directors

Contractual responsibility for the security of government assets held on the contractor's premises rests solely with the company Board of Directors.

Mandatory supervision requirements

The contractor must create certain appointments to satisfy mandatory requirements for the supervision of the appropriate security aspects.

Roles and responsibilities

Guidance on mandatory roles and their responsibilities for the protection of protectively marked assets.

Security instructions

Clear instruction for handling protectively marked assets must be given to and understood by every employee regardless of their role or position in the company.

Homeworking

Guidance on the security requirements and responsibilities of homeworkers and the company security controller.

Control of visitors

Understanding and exercising the required controls for visitors to the premises.

Un-cleared visitor areas (UVAs)

Required controls and placing of UVAs.

Inspections by local and regulatory bodies

Understanding the statutory right of entry and legal obligations.

Preparation and contingency plans

Inspection by the Joint Arms Control Implementation Group (JACIG).

Change of ownership or closure of a List X contractor

Responsibilities and obligations.

Course length

2 - 3 Days

Entry criteria

This course is aimed at Senior Managers or Information Security Practitioners.

Secure sanitisation – interpreting HMG information assurance standard No5

The lack of appropriate controls to sanitise electronic media places organisational information at risk of compromise. Secure sanitisation, in proportion to the confidentiality of the data and the threat, minimises the impact of such compromises. This workshop aims to provide IT and security practitioners with the knowledge and understanding to incorporate secure sanitisation methods in to their organisation's information assurance policies.

Course content

Policy and governance

Determine who the decision makers are, understand the requirements for decommissioning and disposal.

The threat

Risk and threat introduction, different attack types and additional guidance resources.

Techniques and products

Understand the typical sanitisation methods and those methods to avoid as well as learn where to find utilities and equipment.

Re-use strategies and business impact levels

Understand when sanitisation allows release to other environments operating at different business impact levels.

The secure sanitisation baseline control set

Determining the correct sanitisation method using the baseline controls.
A number of commercial providers of secure sanitisation and destruction facilities as well as the opportunity to discuss requirements with them directly.

Course length

1 - 2 Days

Entry criteria

This course is aimed at IT Managers or Information Security Practitioners & will include presentations from a number of commercial providers of secure sanitisation & destruction facilities as well as the opportunity to discuss requirements with them directly.

Conducting physical security assessments – security assessment of protectively marked assets

The risks from undetected compromise stem primarily from espionage activity (ranging from the traditional Foreign Intelligence Service (FIS) to commercial or industrial attack), but may also come from terrorism, as terror groups have exploited opportunities to access sensitive information in the past. The Security Assessment of Protectively Marked Assets (SAPMA) considers these other threats but only from the surreptitious attack perspective. This course will train the student to conduct real assessments using the SAPMA methodology, tools and questionnaire.

Course content

The SAPMA framework, defence in depth, when and when not to use it

Understand when the use of the tool is appropriate, introducing the principal of defence in depth and which documents can be used to support your approach. Introducing the operational requirements framework, catalogue of security equipment and security policy framework.

The SAPMA questionnaire

Hands on workshop and live use of the questionnaire, understanding where the scores are obtained from and what they mean.

The SAPMA summary and baseline controls

Interpret the summary scores, identifying the flaws in your defence in depth and selecting appropriate controls to resolve any gaps.

Takeaway tools and techniques

The real worked examples used on the course will aid your understanding of the use of this tool and you will take away aversion of the tool developed by our IA practitioners.

Course length

1 Days

Entry criteria

This course is aimed at Security Practitioners who have a requirement to safeguard protectively marked assets and who hold at least the baseline personnel security standard (Security Clearance).

"A governance, policy and procedural approach to Cyber Security has demonstrated this is not enough to combat cyber attacks.

Cyber Essentials includes technical measures to help combat a very complex problem and secures your information, organisation, reputation and bottom line."

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

MASS Head Office:

Enterprise House | Great North Road | Little Paxton | St Neots | Cambridgeshire | PE19 6BN | UK

T: +44 (0)1480 222600 | **E:** systems@mass.co.uk | www.mass.co.uk

MC/MARKTG/FLY0115/3