How To Implement CyberSecurity Measures for **Digital Health Technologies**

A general overview of the:

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

CYBER ESSENTIALS

> “
>
> It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.
>
> -Stephane Nappo

CYBERSECURITY

Cybersecurity is of the utmost importance for healthcare innovation due to the critical nature of **patient data** and the potential consequences of **security breaches**.

A breach in cybersecurity could lead to **unauthorized access, manipulation, or theft** of patient data, compromising privacy, trust, and potentially **endangering patient safety**.

In This Carousel,

We will talk about how HealthTech companies can **implement cybersecurity measures** in a safe and robust manner.

More specifically, we will be diving into the Cyber Essentials Scheme that is backed by the UK government and also the ISO 27001 standard that is globally recognised.

CYBER ESSENTIALS

Cyber Essentials is a **UK Government backed** scheme that aims to protect organisations, whatever its size, against a whole range of the most common cyber attacks.

There are **2 levels of** certification:

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

CYBER
ESSENTIALS

This **basic level (self-assessment)** certification covers the full set of controls required to achieve certification and demonstrate compliance with the **foundational level of cyber hygiene** as set out within the Cyber Essentials Standard.

Applicants **complete and submit an online questionnaire** which is marked by a certified Cyber Essentials assessor.

THE 5 KEY CONTROLS:

Secure Configuration

The organisation's **computers and network hardware** should be configured for maximum security.

Firewall

All devices with internet connectivity must have a **firewall installed** in order to comply with the Cyber Essentials Scheme.

Access Control

Only authorised users should be given access to accounts, and they should only have the barest of privileges on computers, networks, and applications.

Software Update

Setting up your systems to **update automatically** ensures that your systems are protected the moment a new version becomes available.

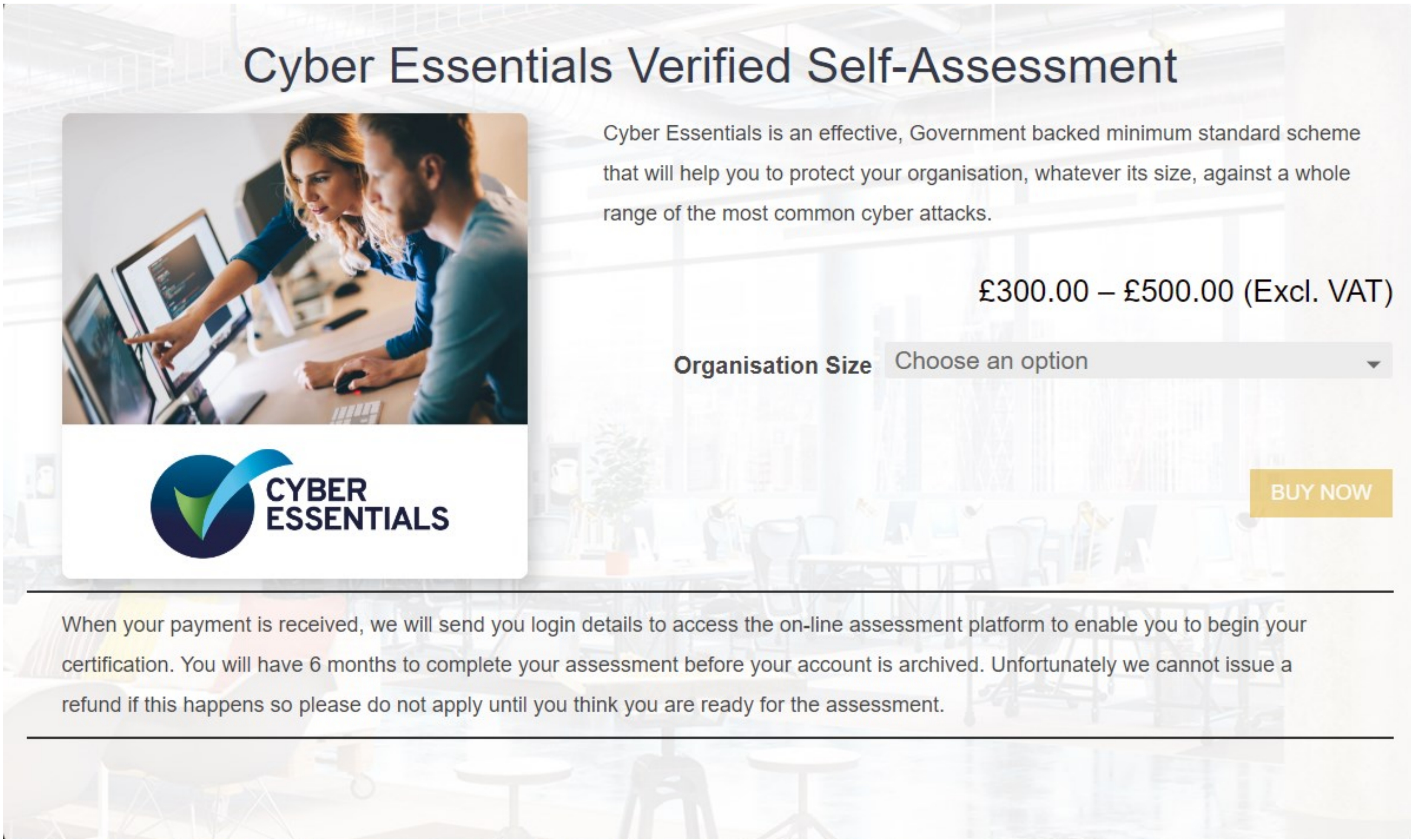
Malware Protection

Organisations should deploy **anti-malware software** on all devices with internet access to protect against viruses and other malware.

CERTIFICATION

In order to complete assessment, you must enter your answers via **IASME's online assessment platform.**

You must **answer all questions** in order to achieve certification.



Cyber Essentials Verified Self-Assessment

Cyber Essentials is an effective, Government backed minimum standard scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

£300.00 – £500.00 (Excl. VAT)

Organisation Size: Choose an option

When your payment is received, we will send you login details to access the on-line assessment platform to enable you to begin your certification. You will have 6 months to complete your assessment before your account is archived. Unfortunately we cannot issue a refund if this happens so please do not apply until you think you are ready for the assessment.

CERTIFICATION

After completing the self-assessment questionnaire (SAQ) for Cyber Essentials that is independently verified,

Successful applicants will subsequently receive their **Cyber Essentials certificate** and be added to the IASME database.

IASME
CONSORTIUM

CYBER
ESSENTIALS
PLUS

Organisations wanting to provide a higher level of assurance that they take security seriously can look to also achieve **Cyber Essentials Plus** certification.

It has the same implementation requirements as Cyber Essentials, but your implementation is verified through an in-person technical audit that must be completed **within three months** of your basic Cyber Essentials certification.

TECHNICAL AUDIT

The technical audit includes:

1) **A series of internal vulnerability scans** and tests of your in-scope systems, which are usually conducted remotely.

2) These tests **cover all Internet gateways**, and a random, representative sample of **internally hosted servers and user devices**.

3) The technical audit concludes with an **external vulnerability scan (conducted remotely)** of your Internet-facing networks and applications to ensure there are no obvious vulnerabilities.

Applicants that pass all elements of the audit are issued their **Cyber Essentials Plus certificate**, which will again be added to the IASME database.

WHY IS THE CYBER ESSENTIALS NEEDED?

✓ To note, a growing number of **UK Government Contracts MANDATE** the need for a Cyber Essentials Certification prior to **being eligible to apply**.

✓ For HealthTech specifically, Cyber Essentials form an important part of the **NHS DTAC application** process as well.

✓ **Good stepping stone** for more advanced security frameworks (such as the **ISO 27001**).

ISO 27001 is the **most widely adopted** Information Security standard in the world.

It is part of a set of standards developed to handle information security:

The ISO/IEC 27000 series.

It provides a framework and guidelines for establishing, implementing and managing an **information security management system (ISMS).**

ISO 27001

To note, ISO 27001 is a risk-based standard.

- Risk based refers to understanding what risks exist within an organisation and how best to **implement policy, procedures, processes, and technical controls** to manage the risks to an acceptable level.
- Largely focused on **policy and process**.
- Applicable to **all forms of information assets** (physical and digital).

This is in contrast to Cyber Essentials that **mainly deals with digital assets only**.

ISO 27001

The standard references a set of **93 safeguards/controls** organised into **4 domains/sections:** Organisational, People, Physical, and Technical.

Topics Include:

- **Information** Security Policy
- **Organization** of Information Security
- **Risk** Assessment and Treatment
- **Asset** Management
- **Access** Control
- **Cryptography**
- **Physical** Security
- **Operations** Security
- **Communications** Security
- **System** Acquisition, Development and Maintenance
- **Supplier** Relationships
- **Compliance** with Legal Requirements and Industry Standards
- **Information** Quality Management
- **Risk** Monitoring and Review

CERTIFICATION

To achieve ISO 27001 certification, an organisation must first **develop and implement an ISMS** that meets all the requirements of the Standard.

Once the ISMS is in place, the organisation can then register for certification with an accredited certification body.

The certification body will **carry out an audit of the ISMS** to ensure it meets the requirements of ISO 27001. If the ISMS is found to be compliant, the certification body will issue an ISO 27001 certificate.

CERTIFICATION PROCESS

The ISO 27001 accreditation process consists of **two stages** and is conducted by a qualified auditor.

Stage 1:

The auditor will **review your documentation** to check that the ISMS has been developed in accordance with the Standard.

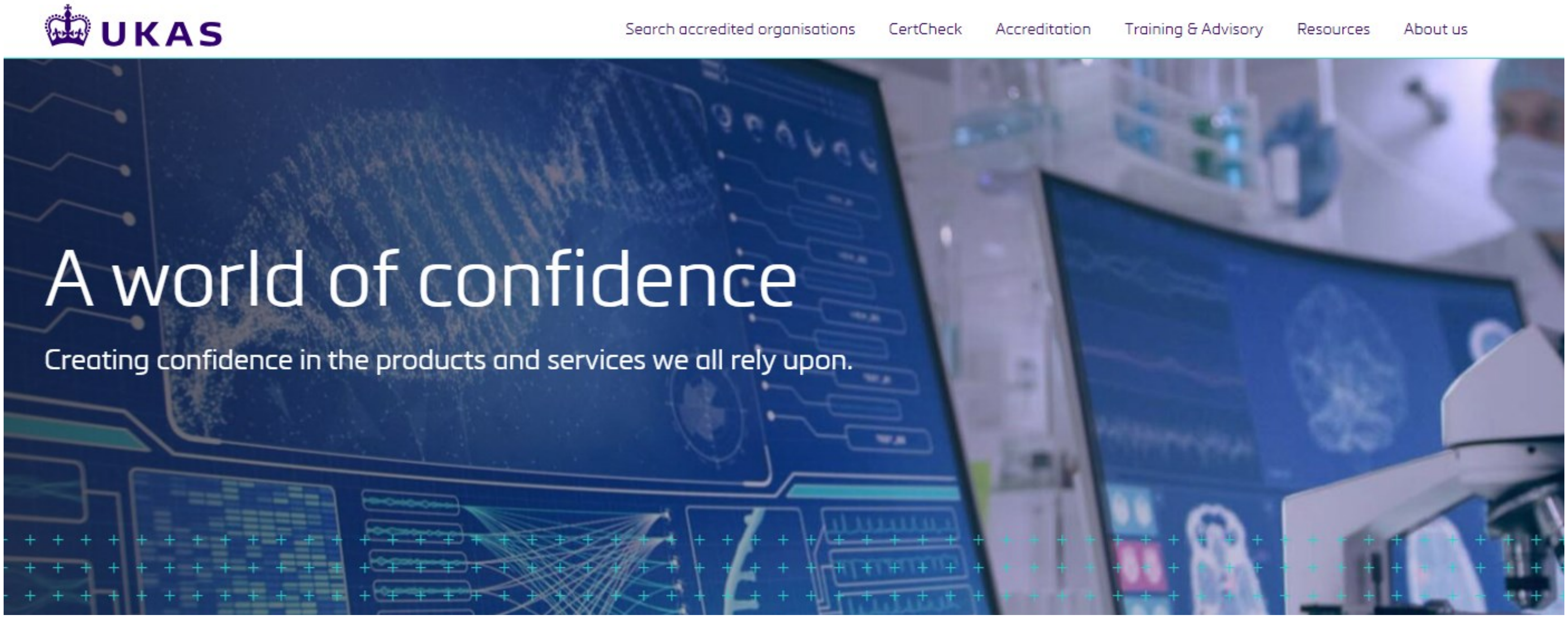
Stage 2:

If you pass the first stage, the auditor will **conduct a more thorough assessment**.

This assessment will **involve reviewing the activities** that support the development of the ISMS.

UKAS

It is important to search for a formally accredited body via **UKAS (in the UK)** for the purpose of certification.



A world of confidence

Creating confidence in the products and services we all rely upon.

Once granted, the ISO 27001 certification **remains valid for up to 3 years.**

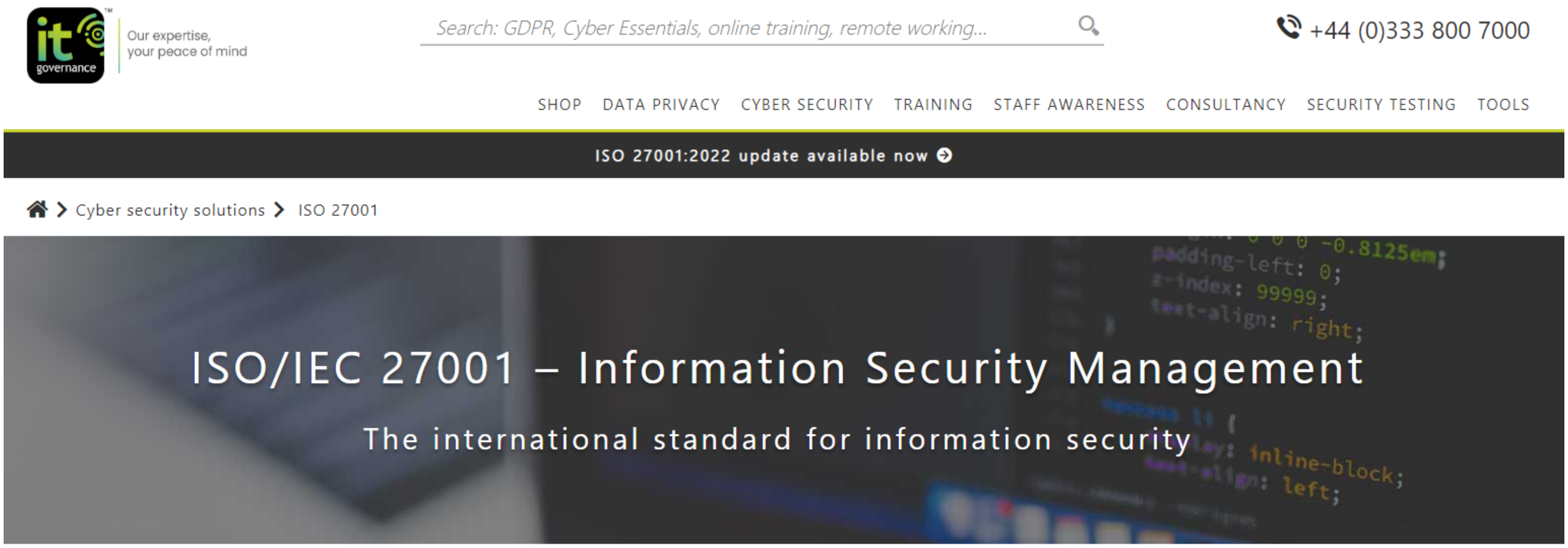
SUMMARY

	Cyber Essentials	ISO 27001
Region	UK only	International Standard
Type of standard	Technical Compliance Based Standard	Risk based standard
Assets	Digital assets only	Physical and Digital assets
Contractual	Mandatory for UK Government and MOD contracts	Implementation and certification are optional.
Frequency	Annual Renewal	3 year renewal

***Often easier** to obtain Cyber Essentials first before ISO 27001

I would highly recommend the resources available at **the IT governance website:**

https://www.itgovernance.co.uk/iso27001

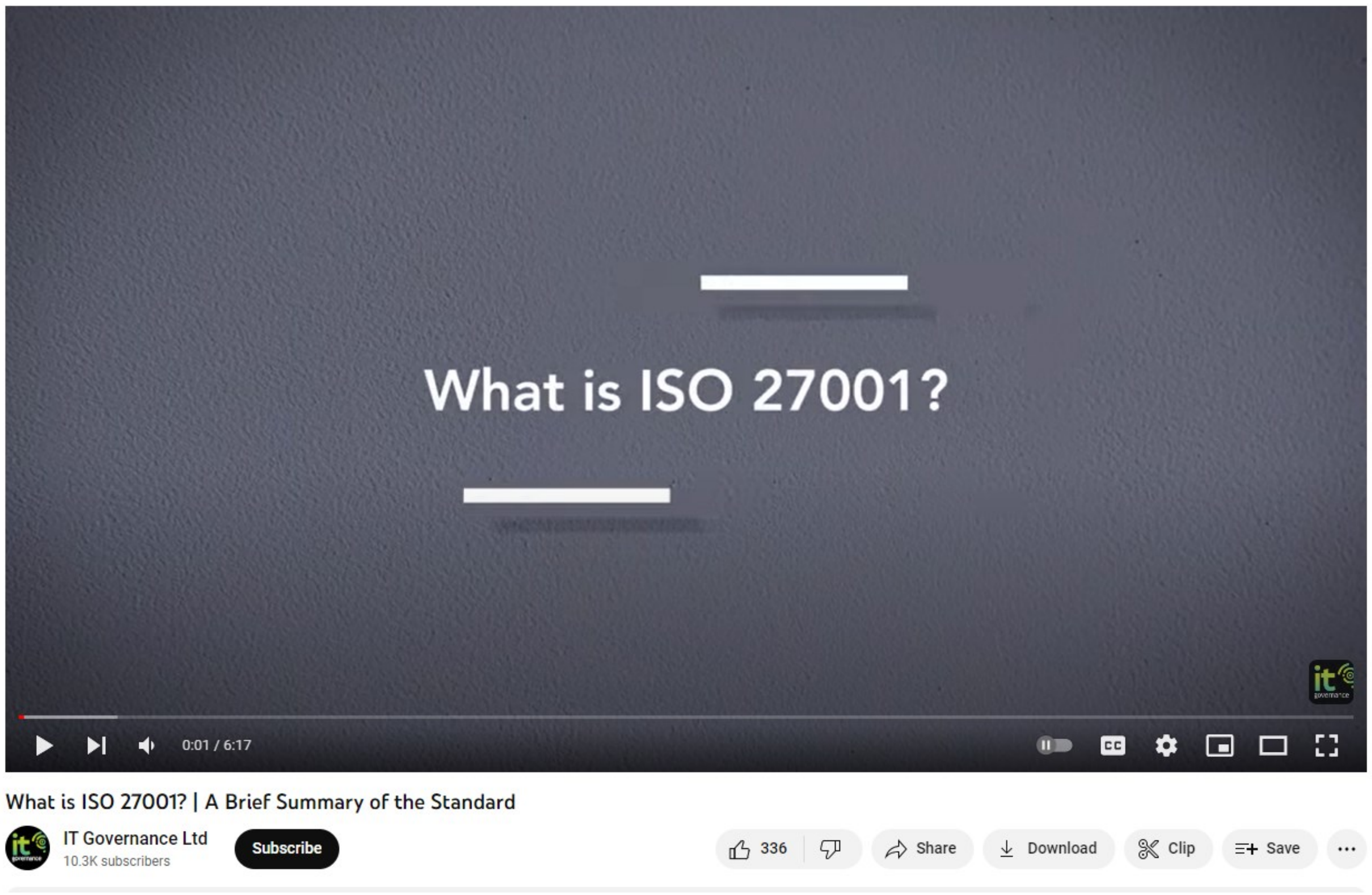


ISO 27001:2022 update available now

Cyber security solutions > ISO 27001

ISO/IEC 27001 – Information Security Management

The international standard for information security



What is ISO 27001?

What is ISO 27001? | A Brief Summary of the Standard

IT Governance Ltd
10.3K subscribers

Hope you found this helpful!

This is a series we are making to help HealthTech Innovators access better resources.

Just our small way of helping!