TOSHIBA

The NIS Regulations

Network and Information Systems Regulations

What are the NIS Regulations?

The Network and Information Systems (NIS) Regulations came into force in the UK on 10th May 2018. The NIS Regulations aim to raise levels of the overall security and resilience of network and information systems.

All organisations deemed by the NIS Competent Authorities (CA) to be 'Operators of Essential Services' (OES) are affected and include:

- Digital Infrastructure
- Energy
- Transport
- Water Supply
- Healthcare

NCSC and the NIS Regulations

The National Cyber Security Centre (NCSC) has produced its own Cyber Assessment Framework (CAF). This draws heavily on the work of the National Institute of Standards and Technology (NIST) in its Framework for Improving Critical Infrastructure Cybersecurity, widely known as the Cybersecurity Framework[1]. NCSC strongly recommends that the CAs use the CAF to conduct NIS Regulations audits.

NCSC is promoting the use of individuals and companies certified under one or more of their Professional Services schemes to support the audit process for the CAs and provide appropriate advice to the OES.

What does it mean for the Operators?

The UK CAs are taking a proactive approach by implementing an assessment framework including an audit programme to encourage their respective OES to prevent incidents happening. Most of the CAs have confirmed that they will be implementing the NCSC CAF as their compliance auditing tool.

Several of the CAs have initiated their auditing by instructing OES to assess themselves against the CAF and submit their findings supported by independent assurance from a third party approved by the NCSC.

Toshiba work with Arcanum, an NCSC certified company to support OES with audits and advice.

"The NIS Directive provides legal measures to boost the overall level of cybersecurity in the EU"

The key benefit of the Regulations is expected to be an improvement in security that leads to a reduction in the risks posed to essential services relying on networks and information systems.

Cyber Security Incidents for large firms[2]

72% **experienced a breach of attack**

27% **of breaches stopped staff carrying out their daily work**

52% **don't know the source of their worst breach or attack**

TOGETHER INFORMATION

1) https://www.ncsc.gov.uk/collection/nis-directive/cyber-assessment-framework
*2) *Source – DCMS Cyber Security Breaches Survey 2018*

Why Toshiba?

We work together with Arcanum, who are specialists in Cyber and Information Security.

- Consultants are individually accredited as CCP Security and Information Risk Advisors by the NCSC and all have at least 12 years' experience in cyber security.
- Arcanum are a NCSC Certified Cyber Security Consultancy in both Risk Assessment and Risk Management.
- NCSC is promoting the use of companies like Arcanum who are certified under one or more of their Professional Services schemes to support the audit process for the CAs and provide appropriate advice to the OES.
- Together, we will help your organisation achieve and maintain NIS compliance through the highest level of consultancy and auditing.
- Arcanum are an experienced consultancy with a long track record of working within a range of industries.

For more information please contact one of our IT Services consultants:

Toshiba Tec UK Imaging Systems Ltd.

Telephone
020 7735 9992

Email
ITServices@toshibatec.co.uk

Website
www.toshibatec.co.uk

Toshiba Tec UK deliver these services in conjunction with Cyber and Information Security Consultancy specialist, Arcanum.

About Arcanum
Formed in 2008, Arcanum Information Security Ltd has grown quickly to become a leading provider of Cyber Security Consultancy services to Government and the private sector. Their highly trusted staff have Certified Cyber Professional status awarded by the National Cyber Security Centre (NCSC), part of GCHQ.

www.arcanum-cyber.com

Arcanum CYBER SECURITY