bestpractice@advent-im.co.uk

0121 559 6699

Directive on Security of Network and Information Systems (NIS) Training

Background

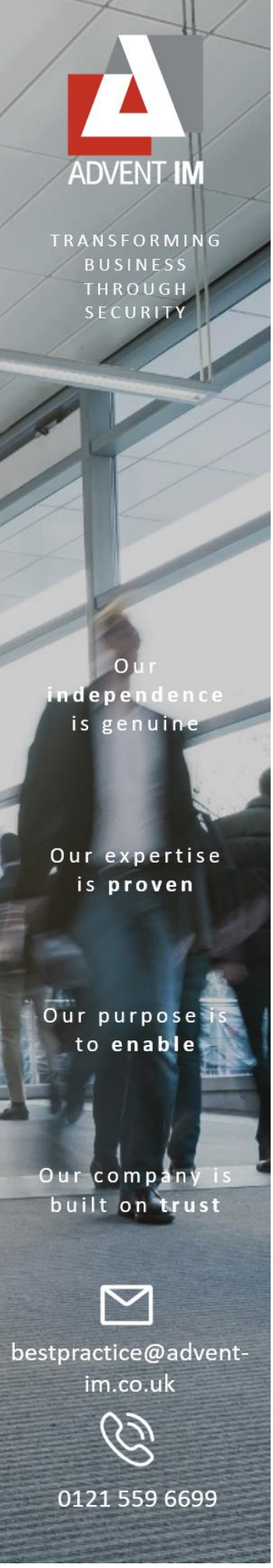
The aim of the Directive is to achieve a high common standard of network and information security across all EU Member states and the UK, following their departure from the EU and it provides legal measures to boost the overall level of cybersecurity by setting a range of network and information security requirements that apply to operators of essential services and digital service providers (DSPs).

The NIS Directive has been incorporated into UK Legislation as the Network and Information Systems (NIS) Regulations 2018, and affects UK operators in a range of sectors including transport, water, energy, transport, health and digital infrastructure. The NIS Regulations also establish a number of Competent Authorities that will provide appropriate oversight and an enforcement regime for the NIS Regulations.

Given how quickly the cyber threat landscape is evolving, it is vital that organisations affected by the NIS Regulations ensure that key staff tasked with implementing, managing and assessing compliance have appropriate, relevant and up-to-date skills.

Who Should Attend?

This 1 day course is designed for staff that are accountable for the implementation and ongoing compliance to the NIS Regulations. It is equally suitable for senior management and individuals in supporting roles requiring a greater understanding of the Regulations and how it might impact their organisation.



Directive on Security of Network and Information Systems (NIS) Training

Scope of Training

The course seeks to put the NIS Regulation (2018) into context using real life examples and delegate role-based scenarios and includes:

- Understanding the principles, why they are important and how to put them into an organisational context;
- Comparing the desirable outcomes against current practices, identifying and assessing the severity of shortcomings and how to produce a prioritised remediation plan;
- Identifying, containing and recovering from cyber security incidents and breaches including reporting obligations;
- Implementing a culture of effective risk management and the use of a principles based approach to cyber improvement;
- The relationship between the National Cyber Security Centre (NCSC) and the National Competent Authorities (CAs);
- The relationship between the NIS Regulation requirements and current ISO Standards i.e. the ISO2700x, ISO 22301 etc.

At the end of this course, delegates will have a good understanding of the new Regulations, the role of the NCSC and CAs, and how working practices need to be adapted to meet the requirements.

bestpractice@advent-im.co.uk 0121 559 6699