



ICS Managers Security Fundamentals course

1 day | 7 CPEs | No equipment needed

Course code: ICS110



The NCSC Assured Training course **ICS Managers Security** course, which is also CIIISec Accredited training, has been designed to provide those at Managerial or equivalent level with an understanding of today's cybersecurity challenges facing their ICS environments. This knowledge is vital when managing and leading the day to day running of all aspects of security risk for these environments. The course will show students how to best identify and support their organisations cybersecurity and risk mitigation/reduction strategies for the ICS environments, whether they are currently 'in role' or moving into the role, either through promotion or lateral movement within the business.

Siker have worked in partnership with the UK's National Cyber Security Centre (NCSC) and the Centre for the Protection of National Infrastructure (CPNI) as well as leading Critical National Infrastructure companies to produce this short course.

Pre-Requisites

There are no pre-requisites for this course and a handbook will be provided for each student.

Course Design

The necessity for this course was identified from experience of delivering OT Security training to people from many different professional backgrounds spanning more than a decade. The course author has 30+ years of engineering experience designing Industrial Control Systems for industrial plant experience.

Who Should Attend

If you are a manager responsible or accountable for any aspect of an ICS environment including:

- Business Technical/Engineering Lead
- Procurement Lead
- ICS Policy/Decision Maker
- Site/Asset Single point of Accountability (SPA)
- Site/Asset IT Manager
- Site/Asset Physical Security/Facilities Manager Lead

Training Formats

<https://sikercyber.com/siker-courses/>

Live Training - Classroom, Private

Online Training - Awareness, eLearning, Instructor-led



What You Will Learn

By the end of the course you will be familiar with:

- Identifying the current and emerging threats to your ICS environments
- Where your ICS environments may be vulnerable
- What actions you need to take to secure those environments and help reduce the risk
- How to prepare for and manage a cybersecurity incident
- The importance of Security Awareness and Training

Session Descriptions

Session 1: Background Contents:

- An exploration of ICS terminology and a description of the elements involved
- What are the differences and similarities between IT and OT?
- What does your ICS Attack Surface look like?
- An introduction to ICS Security risk
- A discussion of ICS Security incidents

Session 2: Securing ICS Contents:

- Planning to reduce the security risk to your ICS environments
- Operational Security
- Vendor and Supply Chain risk
- How to build security into the procurement process
- An introduction to ICS cyber incident response

Accreditation

This course has been assessed under the NCSC Assured training scheme and Chartered Institute of Information Security (CIIISec) Accredited Training scheme. Attendees can earn 7 CPEs.

CyBOK Knowledge Areas

This course addresses the following Knowledge Areas: - Adversarial Behaviours - Risk Management and Governance - Security Operations and Incident Management

Training Formats

Live Training - Classroom, Private
Online Training - Awareness, eLearning, Instructor-led

<https://sikercyber.com/siker-courses/>