



Course Introduction:

Operational Technology (OT), including Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS), is critical for managing essential infrastructure in industries such as energy, manufacturing, transportation, and utilities. As cyber threats targeting OT environments increase, the need for rigorous auditing, compliance assessments, and risk management strategies has never been more crucial. This five-day intermediate training program provides professionals with a deep understanding of auditing methodologies for OT, SCADA, and ICS environments, focusing on security frameworks, risk assessments, regulatory compliance, and best practices for securing critical infrastructure.

Throughout the course, participants will explore key auditing techniques, learn how to identify vulnerabilities in OT systems, and understand regulatory requirements such as NIST, IEC 62443, and ISO 27019. The program covers cybersecurity controls, network monitoring strategies, and incident response planning for OT environments. By the end of this training, attendees will be well-equipped with the theoretical knowledge necessary to conduct OT/SCADA/ICS audits, assess risks, and strengthen security postures across industrial control systems.

Course Objectives:

Upon completion of this course, participants will:

- Understand the fundamentals of OT, SCADA, and ICS auditing.
- Learn key frameworks and regulatory requirements for OT security.
- Identify and assess security risks in OT environments.
- Explore methodologies for auditing OT network architecture and access controls.
- Understand common vulnerabilities and attack vectors in industrial control systems.
- Gain insights into best practices for securing SCADA/ICS infrastructure.
- Analyze security logging, monitoring, and compliance reporting strategies.
- Develop strategies for improving OT security governance and incident response.

Who Should Attend?

This course is designed for professionals and individuals such as IT and OT auditors, Cybersecurity professionals focused on industrial security, SCADA and ICS security analysts, Compliance and risk management officers, Industrial automation and control engineers, SOC team members monitoring OT networks, and Government and regulatory compliance professionals.

Course Outline:

Day 1: Fundamentals of OT/SCADA/ICS Auditing

- Introduction to OT, SCADA, and ICS environments
- Differences between IT and OT security auditing
- Overview of key OT/SCADA/ICS security frameworks (NIST, IEC 62443, ISO 27019)
- The role of compliance and regulatory requirements in OT audits

Day 2: Risk Assessment and Threat Landscape for OT Security

- Identifying threats and vulnerabilities in OT/SCADA/ICS
- Common cyberattack tactics, techniques, and procedures (TTPs) targeting OT
- Risk assessment methodologies for industrial control systems
- Case studies: Real-world OT/SCADA/ICS security breaches

Day 3: Auditing OT Network Security and Access Controls

- Network architecture and segmentation in OT environments
- Secure authentication and access control mechanisms
- Remote access risks and mitigation strategies for SCADA systems
- Reviewing security configurations and firewall rules in ICS networks

Day 4: Security Monitoring, Logging, and Compliance Reporting

- Best practices for security logging in OT/SCADA/ICS environments
- Using SIEM solutions for industrial security event monitoring
- Auditing incident response and disaster recovery plans
- Compliance reporting requirements and documentation strategies

Day 5: Emerging Trends and Best Practices in OT Security Auditing

- The role of AI and machine learning in OT cybersecurity auditing
- Integration of IT and OT security for enhanced resilience
- Future trends in OT cybersecurity, including Zero Trust and cloud adoption
- Course review, Q&A session, and discussion on best practices for OT security auditing

Course Methodology:

A variety of methodologies will be used during the course that including:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play

- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods
- Lectures
- Case Studies and Self Questionnaires
- Group Work
- Discussion
- Presentation

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Fees:

To be advised as per course location. This rate includes participant's manual, Hand-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session