



Auditing Operational Technology / SCADA / ICS (Advanced)

Course Introduction:

Operational Technology (OT) systems, including Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS), are critical for managing essential infrastructure such as power grids, manufacturing plants, oil and gas facilities, and water treatment plants. As cyber threats targeting these environments increase, auditing OT, SCADA, and ICS environments has become a crucial aspect of cybersecurity and risk management. This five-day advanced training program is designed to provide participants with a deep understanding of auditing methodologies, risk assessment techniques, regulatory compliance, and security best practices specific to industrial control systems.

This course explores advanced auditing frameworks, threat landscapes, and security controls tailored for OT environments. Participants will gain insights into vulnerability assessment, network architecture review, incident response strategies, and governance models that ensure secure and compliant OT operations. By the end of this training, attendees will be equipped with the theoretical knowledge required to evaluate OT security controls, identify risks, and enhance the resilience of critical infrastructure against cyber threats.

Course Objectives:

Upon completion of this course, participants will:

- Understand advanced auditing techniques for OT, SCADA, and ICS environments.
- Learn risk assessment methodologies for industrial control systems.
- Identify vulnerabilities and security gaps in OT infrastructure.
- Explore regulatory and compliance requirements (NERC CIP, IEC 62443, NIST 800-82).
- Understand threat intelligence and attack vectors targeting OT networks.
- Learn secure architecture principles for OT and SCADA networks.
- Gain insights into log analysis, anomaly detection, and forensic auditing in ICS environments.
- Develop strategies for governance, incident response, and security reporting.

Who Should Attend?

This course is designed for professionals and individuals such as OT security auditors and compliance professionals, ICS and SCADA security specialists, Industrial cybersecurity analysts and engineers, IT and OT risk management professionals, Network and systems administrators responsible for critical

infrastructure, Incident response and forensic investigators, and Government and regulatory compliance officers.

Course Outline:

Day 1: Fundamentals of OT, SCADA, and ICS Auditing

- Overview of OT, SCADA, and ICS environments
- Differences between IT and OT security auditing
- Key standards and regulatory frameworks (NERC CIP, IEC 62443, NIST 800-82)
- Common vulnerabilities and risks in industrial control systems

Day 2: Risk Management and Compliance for OT Environments

- Risk assessment methodologies for OT networks
- Understanding compliance requirements for critical infrastructure
- Security policies, governance, and best practices for OT auditing
- Case studies on compliance failures and security breaches

Day 3: Network Security and Threat Intelligence in OT Auditing

- ICS network architecture and segmentation best practices
- Threat intelligence and attack vectors targeting OT systems
- Logging, anomaly detection, and forensic auditing methodologies
- Reviewing security controls for firewalls, IDS/IPS, and access control mechanisms

Day 4: Security Governance, Incident Response, and Resilience Strategies

- Incident response planning for OT environments
- Forensic auditing and threat hunting in SCADA/ICS networks
- Secure remote access and third-party risk management
- Developing cybersecurity strategies for OT resilience

Day 5: Future Trends, Reporting, and Audit Recommendations

- Emerging threats and future trends in OT/ICS cybersecurity
- Best practices for documenting audit findings and security recommendations
- OT security automation, AI-driven monitoring, and cloud integration challenges
- Course review, Q&A session, and discussion on advanced OT auditing strategies

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