Course technical sheet

IPDRR Training Course – Cybersecurity for Water and Environmental Resource Management

Fee
780,00 €
Final exam only

Course code	Test duration	Passing score	Issued
IPDRR_CYBER_WAT	60 min	70%	26/08/2026

Executive summary

The IPDRR training course provides operational knowledge for protecting digital systems used in water and environmental resource management. It addresses risks affecting drinking-water networks, treatment and wastewater facilities, environmental monitoring systems, and the integration of information technology, operational technology, SCADA platforms, PLCs, IoT sensors, and remote-control services. Participants learn how to identify threats and vulnerabilities, classify assets, segment networks, govern remote access, protect credentials and data, manage updates and suppliers, maintain tested backups, and organize incident response. The course links technical safeguards to service continuity, human safety, environmental protection, and the integrity of data used for operational decisions. It also introduces the main relevant frameworks, including NIS2 requirements, critical-entity resilience, ISO/IEC 27001, IEC 62443, ISO 22301, and risk-based approaches for water services. The final assessment measures the candidate's ability to select proportionate controls, prioritize remediation, and support a coordinated response to cyber events within public and private organizations operating in the water and environmental sectors.

Certification process

- Registration or login to the Academy platform.
- Completion of the final course examination only. Any training or preparation may be completed externally or through other channels.
- The test questions refer to the objectives, skills and topics described in this technical sheet.
- Assessment of the result, possible validation and certificate issuance according to the rules applicable to the course.

Important note

On Academy, candidates take only the final course examination. Any training or preparation activity may be delivered externally or through other channels. The test questions refer to the topics described in this technical sheet and in the course syllabus summary.

Syllabus summary

Reference framework: Directive (EU) 2022/2555 NIS2 and Italian Legislative Decree 138/2024; Directive (EU) 2022/2557 CER and Italian Legislative Decree 134/2024; Directive (EU) 2020/2184 on drinking water; ISO/IEC 27001:2022 and Amd 1:2024; ISO/IEC 27002:2022; IEC 62443-2-1:2024, IEC 62443-3-2:2020 and IEC 62443-3-3:2013; ISO 22301:2019; ISO 24518:2015. Syllabus: cyber-risk governance, IT/OT assets, SCADA and IoT, segmentation, access control, supply chain, monitoring, backups, operational continuity, incident response, and protection of environmental-data integrity.

Certification Bodies Management systems
IFZA Business Park - Building A2 - Nadd Hessa - Dubai Silicon Oasis
United Arab Emirates
Phone: +971 502475030
Email: info@certificatoiwz.org
VAT/Tax ID: 104216397000003

Course description

The course develops practical skills for protecting processes, data, and technologies used in water abstraction, treatment, distribution, wastewater management, irrigation, land reclamation, and environmental monitoring. It integrates cybersecurity, operational continuity, physical security, and environmental protection.

Learning objectives

- Understand the differences and interdependencies between IT and OT environments.
- Identify threats, vulnerabilities, and attack scenarios affecting water and environmental services.
- Apply asset inventory, classification, risk assessment, and treatment-priority criteria.
- Select organizational and technical measures proportionate to service criticality.
- Support incident management, business continuity, and continual improvement.

Skills acquired

- Read a SCADA/PLC architecture and identify key exposure points.
- Segment networks through zones, conduits, DMZs, and controlled communication rules.
- Manage privileged, remote, and supplier access.
- Protect sensors, telemetry, databases, GIS systems, and supervisory platforms.
- Plan backups, restoration, monitoring, logging, and incident response.
- Assess the impact of a cyber event on service quality, availability, and safety.

Target audience

ICT, OT, and cybersecurity managers and staff; integrated water-service operators; reclamation and irrigation consortia; environmental authorities; laboratories; plant technicians; digital-transition managers; business-continuity, quality, environmental, and safety managers; consultants and technology suppliers.

Prerequisites

Basic knowledge of information systems and organizational processes. Familiarity with networks, industrial automation, remote control, or environmental management is useful but not mandatory.

Program

- Water and environmental services as critical infrastructure and essential services.
- Governance, roles, responsibilities, and the NIS2/CER framework.
- Inventory and classification of assets, data, dependencies, and suppliers.
- IT/OT architectures: SCADA, PLC, HMI, RTU, IoT sensors, GIS, and laboratory systems.
- Risk analysis, threat scenarios, and impacts on health, the environment, and service continuity.
- Segmentation, firewalling, DMZs, secure remote access, and least privilege.

- Vulnerability, patch, configuration, credential, and legacy-device management.
- Logging, time synchronization, anomaly monitoring, and evidence preservation.
- Measurement-data security: integrity, availability, traceability, and validation.
- Offline or immutable backups, restoration tests, RTO, RPO, and business continuity.
- Incident management, communications, escalation, lessons learned, and exercises.
- Supply-chain security, remote maintenance, and contractual requirements.

Certification process

- Registration or login to the Academy platform.
- Completion of the final examination for the selected course.
- Calculation of the result according to the submitted answers and required threshold.
- Possible administrative validation of the result.
- Issuance of the certificate or attestation under the applicable rules.

Academy delivery model

On Academy, candidates take only the final course examination. Training or preparation may be delivered externally, in person, remotely, or through other learning channels. This technical sheet defines the scope of assessable topics.

Assessment method

The examination consists of 30 questions randomly selected from the course question bank. Questions refer to the topics, objectives, and contents of this technical sheet. Multiple-choice and true/false responses are graded automatically; the result is subject to the validation workflow implemented by the platform.

Test duration

60 minutes.

Certificate / Attestation

A score of at least 70% is required to pass. The issued document confirms successful completion of the course final assessment and does not imply third-party accreditation or recognition unless expressly stated.

Expected outcomes

After completion, participants can identify major sector-specific cyber risks, propose proportionate safeguards, contribute to IT/OT protection, and support an organized incident response focused on continuity of water services and environmental protection.