

2150

PROJECT MANAGEMENT · VERSION 3.20

Industrial Cybersecurity Management

For project managers in manufacturing industries



WBS Methodology

Planning · Resources · Deliverables

8 hours

Includes final assessment

0.8 CRE

Knowledge credits

3 languages

Spanish · Portuguese · English

Managing industrial cybersecurity projects through a modular approach helps organize activities, optimize resources, and visualize progress. The WBS methodology brings clarity to implementation and makes it easier to track evidence and deliverables.

01 / COMPETENCIES

Learning outcomes

Upon completion of the course, you will be able to:

- Understand each activity required to implement a mature industrial cybersecurity program that complies with international industry consensus standards and other national regulations.
- Understand the requirements and minimum inputs needed to initiate each activity properly, the necessary resources, and realistic time estimates.
- Understand the objectives and deliverables that must result from each activity, together with the corresponding reports that demonstrate and provide evidence of implementation.
- Demonstrate compliance with the ISA/IEC 62443 series of standards and other regulations. This is important for organizations seeking certification of their CSMP system.
- Formalize and document the completion of each main CSMP program activity. Observe and analyze the results of all work performed.
- Verify progress on a modular basis. A project manager can use this approach to monitor progress across multiple plants and processes simultaneously.
- Generate the evidence needed to demonstrate that the organization is implementing a mature and complete industrial cybersecurity program.
- Support sound decisions to mitigate industrial cyber risks, protect the most valuable assets, and create industrial infrastructure resilient to all types of threats.
- Produce and document the elements needed to justify industrial cybersecurity investments appropriately, with assurance that security risks are mitigated.

Who should attend?

- Recommended for industrial personnel involved in protecting critical infrastructure and control systems.
- Recommended participants include IT security managers, systems integrators, industrial control system suppliers, plant engineers, production and plant operations management, industrial safety personnel, safety instrumented systems specialists, and maintenance personnel at senior or middle management levels.

02 / SYLLABUS

Course content

01 Policies and procedures

Development of the minimum policies and procedures required for the industrial cybersecurity program, CSMP.

02 Competencies and awareness

Development of the necessary competencies, training programs, and organization-wide awareness.

03 Auditing and continual improvement

Auditing, compliance, and continual improvement.

04 Lifecycle phases

Industrial cybersecurity risk assessment and decision-making to mitigate intolerable risk.
Security design and implementation to protect all industrial assets and potential risk receptors.
Operation and maintenance to sustain the minimum security needed to keep risk within the organization's tolerance.

05 Suppliers and engineering

Development and classification of suppliers for industrial security.
Engineering, design, procurement, construction, testing, and security validation for new systems.

06 Implementation strategy

Implementation strategy and essential recommendations that will save the company more than 50% in implementation effort and resources.

Prerequisites

There are no specific prerequisites. Knowledge or experience in some of the following areas is recommended:

Project management (PMBOK); ISA/IEC 62443; information security (ISO 27000); industrial risk management and functional safety (ISA/IEC 61511); national regulations or standards such as NIST and NERC; corporate project and cultural change management; worker safety, environmental safety, and other industrial risk management standards.

03 / LEARNING EXPERIENCE

Training and support

8 hours with the instructor

Duration includes the final assessment.

Delivery formats and scheduling

Available in person at WisePlant offices, the client's facility, or the academy, and virtually through synchronous, asynchronous, and on-demand formats. In every format, participants use the learning platform to access supplementary materials and complete the final assessment.

Course highlights

- Available in Spanish, Portuguese, and English, including both instruction and complete course materials. Materials remain available for asynchronous consultation on the educational campus in all three languages.
- Includes online practical exercises. Each participant remotely accesses a dedicated computer through the campus, networked with the other course computers, to perform cybersecurity exercises using specialized software and applications.
- Extensive supplementary reading materials, available only in their original languages.
- Virtual group study sessions until the examination is taken, including after the course has ended.
- As many examination attempts as needed for up to six months after course completion through the Prometric system.
- Access to course materials on the campus for one year.
- Coaching, chat, and blog support available 24/7 for one year to assist with applying the acquired practical knowledge within the organization.

Materials and digital access

Participants receive materials through the learning platform, including access to online lessons, documents, videos, and supplementary resources for further study, plus campus access to download information and software.

04 / PROFESSIONAL DEVELOPMENT

Knowledge and experience

Two stages of recognition linked to training and practical application.

01 / KNOWLEDGE CERTIFICATE

Practitioner in Industrial Cybersecurity and Critical Infrastructure Lifecycle Management

Awarded after completing the course and passing the assessment. Provides 0.8 CRE credits. The examination is taken in class at the end of the course and is available in Spanish, Portuguese, and English.

02 / EXPERIENCE CERTIFICATE

Expert in Industrial Cybersecurity and Critical Infrastructure Lifecycle Management

Issued after demonstrating experience through active participation in real projects that use the methodology. CRE credits are cumulative and depend on the duration of the activities performed.

Digital badge and supervised experience

Participants who meet the course requirements and successfully pass the final examination receive a digital badge recognizing attendance and the knowledge acquired.

For experience recognition, participants must demonstrate practical involvement and accumulate the minimum required hours in the corresponding activities under the supervision of a certified project leader.



Learn. Build. Advance.

Explore the course and training options:

wisecourses.com/courses/2150sp320/