GOVERN

EN50 - Manager

Industrial Cybersecurity Management for projects in the Energy, Oil & Gas sector

The ability of any organization (end-user or vendor) to develop and implement industrial cybersecurity management projects successfully, making optimal use of resources, in a minimum of time, with a clear visualization of progress is no longer an option.

The modular approach of the WBS methodology with the clarity that it provides, makes it easy, reliable, cost-effective, safe, predictable and visible to all.

At the end of the course you will be able to:

- Understand each of the activities that are necessary to develop in order to implement a mature industrial cybersecurity program complying with international standards by industry consensus and other national regulations.
- Understand the requirements and minimum inputs needed to start each of the activities properly, the resources needed, and a credible time estimate.
- Understand the objectives and deliverables that need to be produced as results of the different activities and the corresponding reports as demonstrative and evidence of such implementation.
- How to demonstrate compliance with the ISA/IEC-62443-X-X series of standards (and other regulations). Important for the organization that wants to certify the CSMP system.
- Formalize and document the completion of each of the major activities of the CSMP program. Observe and analyze the results of everything that is being done.
- Certify progress in a modular way. It can be used by a Project Manager (PM) to monitor progress appropriately in multiple plants and processes at the same time.
- Generate the necessary evidence that the organization is complying with the implementation of a mature and comprehensive Industrial Cybersecurity program.
- Facilitate good decision-making to mitigate Industrial Cyber risks to protect the most valuable assets and create an industrial infrastructure that is resilient to all types of threats.
- Produce and document the elements necessary to justify industrial cybersecurity investments properly with the certainty that security risks are mitigated.

Who is it for?

- Recommended for all personnel in industrial sectors such as: energy, water, oil and gas that are related to the protection of critical infrastructure and control systems.
- The participation of IT security managers, system integrators, suppliers of industrial control systems, plant engineers, production and plant operation management, industrial security, specialists in safety instrumented systems and maintenance personnel is recommended; whether they are senior or middle management.

Certificate: Industrial Cybersecurity and Critical Infrastructure Manager

- CRE Credits: 0.8
- The certification exam is taken in class at the end of the course. Available in Spanish, Portuguese and English.

Modality and schedules:

This course is available in all face-to-face modalities (at WisePlant Offices, at the Client Plant, at the Academy) and Virtual (Synchronous, Asynchronous and On-Demand). Even in face-to-face modalities, the course requires participants to use the Educational Platform in order to access the abundant complementary material and to take the Final Evaluation.

Duration: 8 hours with the teacher, including the final evaluation.

Summary of the course's highlights:

- Available in Spanish, Portuguese and English, both the voice-over and the complete course material. The course material will be available for consultation on the Educational Campus (asynchronous) in Spanish, Portuguese and English.
- Includes hands-on online exercises. Each attendee remotely accesses from campus a dedicated computer networked with the rest of the course computers to perform several practical exercises in Cybersecurity in networks with specific software and applications.
- Abundant supplementary reading material (in original languages only)
- Virtual group study meetings until the exam is taken even after the course is finished.
- All the opportunities you need to take the exam up to 6 months after the end of the course by the Prometric system.
- The attendee can enter the Campus to consult the course material for a period of 1 year.
- Coaching, chat and blog 7×24 for a period of 1 year assisting in the implementation of the practical knowledge acquired in your organization.

Requirements:

It has no specific requirements. It is recommended that the professional has knowledge of some of the following: Project Management according to PI/PMBOK methodology, International Cybersecurity Standards by industry consensus ISA/IEC-62443, Corporate Cybersecurity or Information Security Standards ISO-27000, Industrial risk management standards such as ISA/IEC-61511, functional safety, Regulations and/or national standards such as NIST, NERC, and others; Experience in corporate project management and cultural change management, Other industrial risk management standards (worker safety, environmental safety, etc.).

At WiseCourses we are inspired by innovation in education to create training processes that are representative of the world we live in today. Create and support new systems by empowering educators and practitioners who gain the expertise.