EN60 - ASSESS

Cyber Risk Assessment in New and Existing Industrial Systems in Energy, Oil & Gas.

Develop the Industrial Cyber Risk Assessment complying with all the requirements of the ISA/IEC-62443 series of standards with ease, speed and ensuring compliance.

The right methodology is critical to making the right decisions and creating industrial infrastructures that are resilient to all types of threats. Avoid delays and typical errors due to lack of management, knowledge or experience.

At the end of the EN60 course you will be in a position to:

- Properly interpret the requirements of the ISA/IEC-62443 series of standards for the Cyber Risk Assessment (ASSESSMENT) phase.
- Carry out all these risk assessment activities successfully using a minimum amount of time, dedicating most of it to the activities of value.
- Correctly identify the system under consideration, whether these are existing or future systems, starting in engineering stages.
- Collaborate, participate in, and/or lead a detailed cyber risk assessment based on the assessment of realistic scenarios and consequences.
- Make good decisions consistently with other industrial risk disciplines.
- Assist or develop an effective, efficient, and sufficient plan of action to mitigate all risks in accordance with the risk tolerable by the organization.

You will cover the following topics in the course:

- Interpret the requirements of the WBS methodology to meet the requirements of the standards and make good decisions.
- Understand the necessary activities to be carried out during the Cyber Risk Assessment (ASSESSMENT) phase.
- Understand the inputs needed before starting each activity.
- Understand the outputs to be produced because of each activity.
- Establish and know the expectations, roles and responsibilities of each participant.
- Estimate the time, duration, and resources required to complete the risk assessment.
- Analyze, understand, and model zones and conduits.
- Accurately identify the complete list of cyber-assets that make up the system under consideration, including Hardware, Virtual Machines and Software.
- Employ passive, non-intrusive methods and techniques to identify cyber-assets and develop vulnerability studies in existing 7x24 or future systems.
- Identify public vulnerabilities (existing in global databases), private vulnerabilities (specific to the particular installation of the SuC), and zero-day vulnerabilities.
- Classify vulnerabilities such as administrative, cyber, and physical.

- Model the Industrial Cybersecurity risk matrix to be used to calculate Industrial Cyber Risk in a repeatable and auditable way.
- Develop an organizational maturity assessment against global best practices, including ISA/IEC-62443 and regulations for energy, oil, and gas.
- Develop security breach assessments against global best practices, including ISA/IEC-62443 and others.
- Model the company's physical assets and identify all potential consequences through hazard identification and criticality analysis.
- Participate in and/or conduct a detailed cyber risk assessment according to the ISA/IEC-62443-3-2 risk assessment methodology.
- Produce the necessary recommendations to reach the tolerable risk for the organization.
- Produce the necessary reports with the necessary and sufficient recommendations at the level of processes, technology, systems, policies, procedures, and best practices.

Certificate: Specialist in Cyber Risk Assessment in Industrial Systems

- CRE Credits: 1.6
- The certification exam is taken in class at the end of the course. Available in Spanish, Portuguese and English.

Recognitions:

All participants who meet the course requirements and who successfully pass the final exam with a good grade will be awarded a Digital Badge. The Digital Badge certifies that the participant has attended the 2160 training course and has taken the final assessment test with a good grade, verifying that the participant has assimilated the new knowledge in a reasonable way.

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.