Learnsoft
ENTERPRISE TRAINING

Cyber Security for Managers & Executives

Length: 2 Days

About this course: This course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. You will not just learn about security, you will learn how to manage security. The diligent manager will gain vital, up-to-date knowledge and skills required to supervise the security component of any information technology project.

Essential security topics covered in this management track include: network fundamentals and applications, power, cooling and safety, architectural approaches to defense in depth, cyber-attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, offensive and defensive information warfare, culminating with our management practicum.

:

Intended Audience: IT Supervisors, Managers, Directors, Executives who are looking to gain a deeper understanding of the methods used to implement Cyber Security within their organization.

COURSE CONTENT

Module 1. Secure executive support and set the objectives

Making a decision to implement an ISMS compliant with ISO/IEC 27001 should always start with getting the involvement / confirmation of the organization's top management. This group decides the allocation of resources and budget for defining and maintaining the management system, sets its objectives, and communicates and supervises it in the organization.

Setting the objectives is an iterative process and hence requires annual updates. The information security system objectives should be determined by the top management, and reflect the business and regulatory needs of the organization.

Module 2. Define the scope of the system

ISO/IEC 27001 is well-grounded in the reality and technical requirements of information security. This is why the organization should, in the first place, choose those security measures and requirements set out in the standard that directly affect it. The standard defines the processes that should make up the Management System of the organization as well as the security measures that the organization should implement to ensure information security. The results of these actions provide a basis for the subsequent Modules of the implementation.

Module 3. Evaluate assets and analyze the risk

The next Module is to evaluate information processing assets and carry out a risk analysis for them. What is asset evaluation? It is a systematic review, which results in a description of the information processing assets in the organization.

Module 4. Define the Information Security Management System

At this stage of implementation, the executive support has been secured, objectives have been set, assets have been evaluated, the risk analysis results are already available, and the risk management plan is in place. As a result, the remaining elements of the Information Security Management System can be defined and security measures can be implemented in the organization. Usually this is an iterative process where ISMS components are defined.

Module 5. Train and build competencies for the Roles

At this stage, the organization should specify the competencies and skills of the persons/roles involved in the Information Security Management System. The first Module after defining the ISMS is to explain it and notify the organization about the scope and manner of the ISMS operation, as well as about how each employee affects information security. This element should be included in the organization's management system by defining roles, competencies required for the roles, and the manner of passing this knowledge onto new employees and refreshing it in people who have been already trained. At this point it is worth defining the training, guides and competence profiles for each role

Module 6. System maintenance and monitoring

Before commencing the certification of the information security management system it should already work in the organization. Ideally, a fully defined system will have been implemented and maintained in the organization for at least a month or two prior to the start of the certification audit, providing the time for conducting the necessary training, carrying out a management system review, implementing the required security measures, and adjusting the risk analysis and risk management plan. During this period, the first actions set out in the infrastructure maintenance and security management plan should be carried out as well.

Module 7. Certification audit

The implementation of an information security management system in a company is confirmed by a certificate of compliance with the ISO/IEC 27001 standard. The certification requires completing a certification audit conducted by a body certifying management system. The certification audit has two phases. Phase I usually involves a check of the scope and completeness of the ISMS, i.e. a formal assessment of the required elements of a management system, and in phase II the system is verified in terms of whether it has been implemented in the company and actually corresponds to its operations.