3-Day Seminar

No pre-requisite training required.

CPE Credit Hours: ***24***

For currently scheduled seminars please see
www.certifiedinfosec.com
+1 (888) 547-3481 (USA)
+1 (904) 406-4311

This course can be arranged as a private on-site training session at up to a 40% discount from public session fees.

** Copies of ISO standards are NOT included in this course, nor provided in class.*

This workshop is included in the "GRC Week" package!

CIS POLICY WORKSHOP SERIES:
ISO 31000 ENTERPRISE RISK MANAGEMENT

Learn Enterprise Risk Management, and how to leverage the ISO 31000 standard to establish and maintain an ERM program, and build-out the initial ISO 31000-conforming risk program policy right in class!

Why Enterprise Risk Management?

Risk management is an increasingly important business driver and stakeholders have become much more concerned about risk. Risk may be a driver of strategic decisions, it may be a cause of uncertainty in the organization or it may simply be embedded in the activities of the organization. An enterprise-wide approach to risk management enables an organization to consider the potential impact of all types of risks on all processes, activities, stakeholders, products and services. Implementing a comprehensive approach will result in an organization benefiting from what is often referred to as the "upside of risk".

A successful enterprise risk management (ERM) initiative can affect the likelihood and consequences of risks materializing, as well as deliver benefits related to better informed strategic decisions, successful delivery of change and increased operational efficiency. Other benefits include reduced cost of capital, more accurate financial reporting, competitive advantage, improved perception of the organization, better marketplace presence and, in the case of public service organizations, enhanced political and community support.

And since information security, business continuity/disaster recovery, environmental health and safety, and other critical management systems have the primary purpose of identifying and treating risk, it is essential that your organization establish a common platform and approach for managing risk.

What you and your colleagues will achieve

This 3-day training and workshop session provides a thorogh overview on ISO 31000, as well as setting out advice on the implementation of an ERM initiative. This course:

- Describes the principles and processes of risk management;
- Provides a thorogh overview of the requirements of ISO 31000 and 31010;
- Gives practical guidance on designing a suitable framework;
- Gives practical advice on implementing enterprise risk management;
- Establishes a firm program starting point by using ISO 31000 to build out the initial ERM core policy.

Course Content Details

1. Risk, risk management and ISO 31000

- Nature and impact of risk
- Principles of risk management
- Review of ISO 31000, 31010, ISO Guide 73, and ISO 27005
- Achieving the benefits of ERM

2. Enterprise Risk Management

- Planning and designing
- Implementing and benchmarking
- Measuring and monitoring
- Learning and reporting

3. Establish a firm program starting point by using ISO 31000 to build out the initial ERM core policy. Throughout the class, our expert instructor will convert ISO 31000 concepts and requirements into a real ISO 31000-conforming Enterprise Risk Policy. Bring your laptop, and you can work right along with the instructor using electronic (MS Word format) templates we provide in class!* Along with the instructor, you will get your ERM program properly initiated by constructing:

- Complete ISO 31000-conforming ERM Policy (18-Page template provided)
- ERM Context and Scope Document (10-Page template provided)
- ERM Risk Assessment and Risk Treatment Methodology Document (18-Page ISO 31010/27005 template provided)
- Procedure for Training and Development Needs Analysis document (8-Page template provided)
- ERM Program project kick-off document (9-Page template provided)
- Procedure for Identification of ERM Project Requirements document (4-Page template provided)
- Procedure for Identification of Statutory, Regulatory, and Contractual Requirements document (1-Page template provided)

Who should attend

- CEO / Managing Director / Policy Approvers / Strategy Decision Makers
- Chief Information Officer (CIO / CISO)
- Information security managers
- Compliance officers
- Risk managers
- Business Continuity Managers
- Health, Safety, and Environment (HSE) Managers
- Facilities managers
- Operations department heads (business unit managers)
- Auditors

For more information, please contact Certified Information Security
Toll Free: (888) 547-3481 • Tel: +1 (904) 406 4311• Fax: +1 (786) 522-9063 • info@certifiedinfosec.com

CIS POLICY WORKSHOP SERIES:
ISO 37301 COMPLIANCE MANAGEMENT

2-Day Seminar

Recommended Pre-Requisite Training: ***None***

CPE Credit Hours: ***16***

Available as a private on-site engagement for groups of 10 or more participants.

www.certifiedinfosec.com
+1 (888) 547-3481 (USA)
+1 (904) 406-4311

Get trained and certified in establishing, managing, operating, and auditing an ISO 37301 Compliance Management System

Every day, organizations face the ever-increasing need to manage and fulfil regulatory and industry requirements to allow them to conduct business. "Compliance" is no longer simply a legal concern isolated to a legal compliance unit. After all, how the organization operates determines its ability to comply with external stakeholder requirements. This means that compliance requirements permeate all business activities - from procurement, to human resource management, to information management, to manufacturing processes, to environmental management - *and on and on*. Since complying with one requirement can impact compliance with another requirement, compliance with all of the various requirements in total gets quite complicated. Compliance must be very carefully designed, managed, and monitored - ***throughout the organization***.

Managing compliance is inexorably linked to managing risk.

Whether fulfilling legal filing and reporting requirements, protecting health and safety, or maintaining quality in manufacturing, we are inevitably managing risk - the uncertainty of successful achieving our objectives. Governmental regulation, industry standards of best practice, and even normal service contracts all exist primarily to ensure the organization manages risk appropriately within externally mandated tolerances. Today, organizations need a mature and well-structured approach to integrating compliance and risk management throughout the enterprise. Not coincidentally, this results in good governance.

What is the ISO 37301 standard?

Developed and published by the International Organization for Standardization in 2021, ISO 37301 provides guidance for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive risk-based compliance management system within an organization. The guidelines on compliance management systems are applicable to all types of organizations. The extent of the application of these guidelines depends on the size, structure, nature and complexity of the organization. ISO 37301 is based on the principles of good governance, proportionality, transparency and sustainability.

ISO 37301 takes a risk-based approach to compliance management. As a result, it aligns with ISO 31000 Risk Management – Principles and guidelines, which according to ISO, "provides principles, framework and a process for managing risk." In conjunction with ISO Standard 31000 (Enterprise Risk Management), ISO 37301 is used to establish a formal enterprise wide management system for Governance, Risk, and Compliance (GRC) that will effectively and measurably improve organizational performance. Since such a program is designed and operated to well-recognized international standards of best practices for GRC, the organization also achieves greater confidence and respect among stakeholders including investors, lenders, regulators, suppliers, customers, and trading partners just to name a few.

ISO 37301 integrates risk assessments, the risk management process, and compliance management. By following ISO risk management practices, organizations embed compliance within the risk-based process. This is an important characteristic of effective compliance management because it breaks down silos and allows the organization to focus on root-cause risks. This streamlines the compliance process, making it easier to meet the obligations of not only government entities, but the host organization's own internal code of ethics and its social responsibility objectives.

Upon completion of this training and certificate program, participants will:

- Understand the principles and processes of risk governance and management;
- Get a thorough overview of the requirements of ISO 37301;
- Get practical guidance on designing and implementing a suitable compliance management framework;
- Establish a firm program starting point by using ISO standard 37301 to build out the initial Compliance Management core policy. Soft-copy editable templates are provided in the instructor-led class.

Who should attend

- Leadership: CEO, COO, CFO, Board Member
- Policy Approvers / Strategy Decision Makers
- Risk managers
- Compliance officers
- ISO 27001 Information security manager
- ISO 9001 Quality managers
- ISO 14001 EMS managers
- ISO 22000 Food safety managers
- Health, Safety, and Environment (HSE) Risk Manager (s)
- Fraud control / security managers / investigators
- Trade union negotiators and liaisons
- IT managers
- Risk manager(s)
- Operations auditors