

CIS POLICY WORKSHOP SERIES: ISO 31000 ENTERPRISE RISK MANAGEMENT

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.

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 thorough 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 thorough overview of the requirements of ISO 31000, 31010, and 23894;
- 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, 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

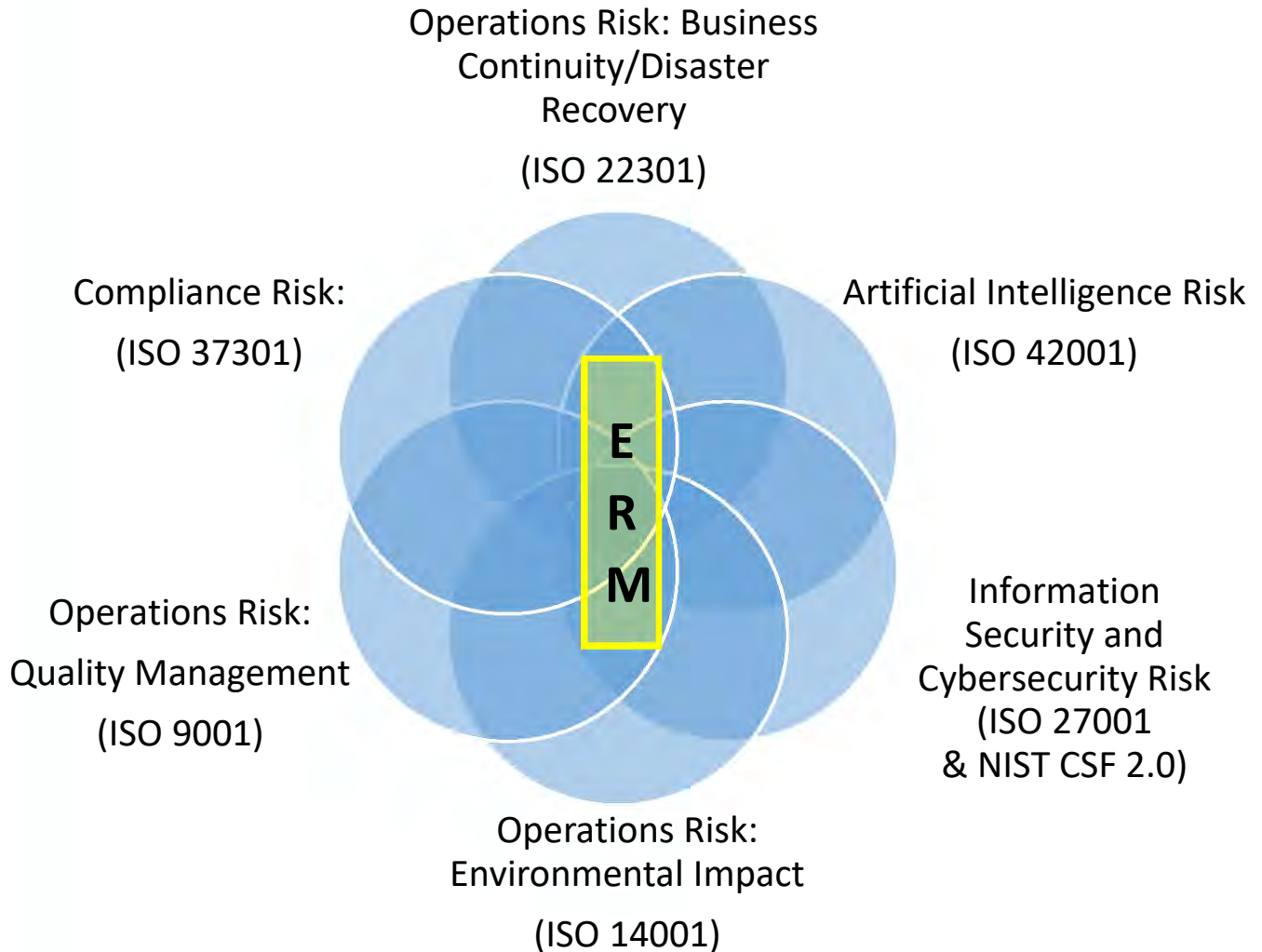
- CEO / Managing Director / Policy Approvers / Strategy Decision Makers
- Chief Information Officer (CIO / CISO)
- Information security managers
- Compliance officers
- Risk managers
- Business Continuity Managers
- Health, Safety, and Environment (HSE) Managers
- Facilities managers
- Operations department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

Enterprise risk management ties other risk management together to create a better and more effective ‘big picture’ approach to managing and governing an organization.

Risk “Silo’s” must be better coordinated and collectively managed to reduce overall costs of redundant controls, to ensure that no “risks” fall through the gaps, and to safeguard against a control causing unintended risk to the organization.



Enterprise Risk Management (ERM) guides and informs all other risk managing specialties, or silo’s, on how risk is to be uniformly measured, and to which tolerances (risk tolerance or risk appetite). ERM is essentially the core risk assessment, management, and communication framework at the heart of the organization’s other risk managing specialties including ISO 9001 quality management, ISO 22301 Business Continuity Management, ISO 14001 Environmental Management, ISO 37301 Compliance Management, and even ISO 42001 AI Management. As such, the Enterprise Risk Management framework, or program, should be designed and deployed prior to forming other risk managing specialties – *not after*.



Policy Workshop: ISO 31000 Enterprise Risk Management

(3-Days)

CERTIFIED

Information Security[™]

Module I. Introduction

- A. Introduction to Enterprise Risk Management Concepts
 - 1. Overview of Enterprise Risk Management
 - 2. How does “*Enterprise*” Risk Management differ from “*Risk Management*”?
- B. Risk management drives business continuity management, information security, quality management, environmental health and safety, and even occupational health and safety
 - 1. Business drivers for risk management: Regulatory and other external requirements
 - a) ISO 9001 Quality Management Systems
 - b) ISO 14001 Environmental Management Systems
 - c) ISO 27001 Information Security Cybersecurity, and Privacy Management Systems
 - d) SO 22301 Business Continuity Management Systems
 - e) ISO 42001 Artificial Intelligence Management Systems
 - f) ISO 37301 Compliance Management Systems
 - g) NIST Cybersecurity Framework
 - 2. Leveraging ISO standards 31000, 31010, and 27005 to establish consistent, formal, and documented approach for risk management
- C. Risk Architecture & Strategy drives other Management Systems’ Architecture & Strategy
 - 1. Leadership (Mandate and Commitment) Requirements
 - 2. Typical senior leadership responsibilities
 - a) Risk Officer and the Risk Committee
 - b) Senior Executive Leadership
 - c) Top-Down Risk Management
 - d) Getting senior management buy-in and commitment
 - 3. How Enterprise Risk Management leadership transcends to automatically fulfil leadership requirements for Quality Management, Environmental Management, Information Security Management, Business Continuity Management, and Occupational Health and Safety
- D. Using the organization’s business context to develop fit-for-purpose Enterprise Risk Management, Quality Management, Environmental Management, Information Security Management, Business Continuity Management, and Occupational Health and Safety
 - 1. Corporate Governance

2. ISO Requirements for “Context”
 - a) ISO 9001:2015 Quality Management
 - b) ISO 22301:2013 Business Continuity Management
 - c) ISO 14001:2015 Environmental Management
 3. Managing internal and external stakeholder input and collaboration
 - a) Procedure for Identification of ERM Project Requirements document (4-Page template provided)
 - b) Procedure for Identification of Statutory, Regulatory, and Contractual Requirements document (1-Page template provided)
- E. Governance and Management Roles & Responsibilities
1. Possible Organizational Structure for Establishing ERM
- F. How to Get Started in Establishing ERM

Module II. Risk Architecture and Strategy

- A. How does risk management relate to the organization?
- B. ISO 31000 Roadmap to ERM
- C. 11 Core Principles of ERM (Defining ERM and its high-level objectives)
- D. Risk Management Leadership
- E. Risk governance versus risk management
- F. Stakeholder collaboration for determining internal and external context requirements for risk management
 1. Communication and consultation
 2. Determining internal business context requirements
 3. Determining external business context requirements
 4. Using business context to establish risk criteria
 - a) Impact criteria
 - b) Acceptance criteria
 - c) Evaluation criteria

G. Establishing the risk management policy

1. Complete ISO 31000-conforming ERM Policy (18-Page template provided)
2. ERM Context and Scope Document (10-Page template provided)

H. Enterprise risk management roles and responsibilities

1. Risk committees
 - a) Risk oversight (CEO and Board)
 - b) Risk management
2. Enterprise Risk Manager
3. Specialty risk managers
 - a) Quality management
 - b) Environmental management
 - c) Business continuity management
 - d) Information security management
 - e) Compliance
 - f) Fraud control
4. Business unit manager and/or department head
5. Internal audit manager
 - a) Auditors
6. Training manager / HR manager
 - a) Training Needs Analysis Procedure document (8-Page template provided)
7. Staff

I. Integration into organizational processes

J. Resource allocation

K. Communication and consultation program requirements

Module III. Implementing the ERM Program and Establishing a Formalized Risk Assessment and Risk Treatment Methodology

A. Leveraging ISO 31010 and ISO 27005 to establish a formalized risk assessment and risk treatment methodology

1. ERM Risk Assessment and Risk Treatment Methodology Document (18-Page ISO 31010/27005 template provided)

B. Risk Assessment

1. Risk Identification

a) Assets

b) Vulnerabilities

c) Threats

d) Controls

e) Consequence

2. Risk Analysis

a) Risk analysis techniques (procedures)

3. Risk Evaluation

Module IV. Risk Treatment

A. Calculating residual risk

B. Risk treatment alternatives

C. Risk treatment constraints

Module V. Risk Acceptance, Communication, Consultation, Monitoring, and Review

A. Risk Treatment Certification and Accreditation

B. Risk review (Risk communication and consultation)

C. Risk monitoring and review

Module VI. Using CIS' ISO 31000 Policy Document Toolkit

- A. ERM Project Kick-Off Plan (9-Page template provided)
- B. Training Needs Analysis Procedure document (8-Page template provided)
- C. ERM Context and Scoping (10-Page template provided)
- D. Enterprise Risk Management Framework Policy (18-Page template provided)
- E. Risk Assessment and Risk Treatment Methodology (18-Page ISO 31010/27005 template provided)

* ISO Standards are **NOT included in this risk management training**, nor provided in class. Students are encouraged to bring their own hard-copies of the standards to the class. ISO standards are available for purchase at www.iso.org.