Remember, an ISO 27001 Information Security Management system is actually a *risk management* system that focuses on information security concerns.

This means that **managing information security controls *begins with assessing risk*** to information confidentiality, integrity, and availability.

That's why this ISO 27001 Lead Implementer track begins with 3-days of ISO risk assessment.

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.*

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

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 Management Systems
    d) ISO 22301 Business Continuity Management Systems
    e) ISO 45001 Occupational Health & Safety
    f) Sarbanes-Oxley Act
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 27001:2014 Information Security Management

c) ISO 22301:2012 Business Continuity Management

d) ISO 14001:2015 Environmental Management

e) ISO 45001:2018 Occupational Health and Safety 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

(1) Hands-on Risk Assessment lab – Assets

b) Vulnerabilities

(1) Hands-on Risk Assessment lab – Vulnerabilities

c) Threats

(1) Hands-on Risk Assessment lab – Threats

d) Controls

(1) Hands-on Risk Assessment lab – Controls

e) Consequence

(1) Hands-on Risk Assessment lab – 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.

2-Day Seminar

Prior attendance of ISO 31000 or ISO 27005 risk management training is strongly recommended.

CPE Credit Hours: ***16***

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.*

CIS POLICY WORKSHOP SERIES: *ISO 27001 INFORMATION SECURITY MANAGEMENT*

Learn ISO 27000 standards for information security governance, and how to leverage the ISO 27000 standards to establish and maintain an information security management system (ISMS) program. Then build-out the initial ISO 27001-conforming information security program policy right in class!

ISO 27001 Information Security Governance

ISO/IEC 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO 27001 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

What you and your colleagues will achieve

This 2-day training and workshop session provides a thorough overview on ISO 27001, as well as setting out advice on the implementation of an information security initiative. The purpose of the course is to:

- Describe the principles and processes of information security governance and management;
- Provide an overview of the requirements of ISO 27001;
- Give practical guidance on designing a suitable framework;
- Give practical advice on implementing information security management;
- Establish a firm program starting point by using ISO 27001, ISO 27002, and 27003 to build out the initial Information Security Management core policy.

Course Content Details

1. Information Security, Information Security Management, and ISO 27001

- Principles of information security
- Review of ISO 27001, ISO 27002, ISO 27003, ISO 27005, ISO 27007, and ISO 27008
- Achieving the benefits of Information Security

2. Information Security Management

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

3. Establish a firm program starting point by using ISO 27001 to build out the initial Information Security Management core policy. Throughout the class, our expert instructor will convert ISO 27000 concepts and requirements into a real ISO 27001-conforming Information Security 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 Information Security program properly initiated by constructing:

- Procedure document for Training and Development Needs Analysis (9-Page template provided)
- Kick-off ISMS project plan (9-Page template provided)
- Procedure document for Identification of Requirements (4-Page template provided)
- Procedure document for identification of statutory, regulatory, contractual, and other requirements (1-Page template provided)

Who should attend

- Policy Approvers / Strategy Decision Makers
- Chief Information Officer (CIO / CISO)
- Information security managers
- IT Managers
- Compliance officers
- Risk managers
- Business continuity 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

Policy Workshop: ISO 27001 Information Security Management

(2-Days)

CERTIFIED Information Security™

Module I. Information Security Governance

A. Comparing information security governance versus management

B. The current state of information security Governance in the world today

   1. expectations
   2. roles
   3. business requirements

C. Information security goals

D. Information security benefits

E. Business compliance drivers for information security

   1. Sarbanes-Oxley
   2. FSA
   3. Basel

F. Information security management system (ISMS) overview

G. Governing information security with ISO standards

H. Certifying internal controls according to ISO standards

Module II. Information Security Standards of best Practice

A. An Overview and Comparison of the ISO 27000 Family of Standards

   1. ISO 27001
   2. ISO 27002
   3. ISO 27003
   4. ISO 27004
   5. ISO 27005
   6. ISO 27006
   7. ISO 27007
   8. ISO 27008

B. An overview of the ISO 27001 Standard for Information Security Management

C. PDCA Process

1. ISMS Planning
2. ISMS Doing
3. ISMS Checking
4. ISMS Acting (Improvement)

D. ISO 9001 and ISO 14001 requirements mapping and integration

1. Documentation
2. Leadership
3. Communication
4. Reviews
5. Continuous improvement and metrics

E. Certifying the Organization to ISO 27001

1. Business drivers
2. Organizational certification process
3. Personal certification process

F. Certifying management and staff for ISO 27001 information security management competence

Module III. Information Security Policy and Scope

A. Information Security Management System Policy

1. Policy construction and the relationship with the organization's enterprise risk policy
2. ISO 27001 ISMS policy requirements
3. Complete ISO 27001-conforming Information Security Management System Policy (15-Page template provided)

B. How to scope the Information Security Management System

C. Resourcing the ISMS

D. Procedure document for Identification of Requirements (4-Page template provided)

E. Procedure document for identification of statutory, regulatory, contractual, and other requirements (1-Page template provided)

F. Kick-off ISMS project plan (9-Page template provided)

Module IV. Organizing Information Security

A. Internal organization

1. Requirements for senior leadership commitment and oversight
2. Management review
3. Information security manager
4. Cross-functional management forum (steering committee)

B. Roles and Responsibilities

1. Board of Directors
2. Executive management
3. Information Security Steering Committee
4. Information Security Management Project Team
5. Information Security Officer/Manager

C. Training and competency requirements

1. Required competencies by role:
   a) Program management
   b) Policy and strategic development
   c) Planning and document development
   d) Document approval
   e) Risk management
   f) ISMS exercising and auditing
   g) Communications and media relations

2. Procedure document for Training and Development Needs Analysis (9-Page template provided)

D. General roles and responsibilities by category

1. Requirements for independent auditing and reviews
2. Ongoing daily management and maintenance

Module V. The Risk Assessment and Statement of Applicability

A. ISO 27001 requirements for risk assessment

B. Risks, impacts, and risk management