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 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

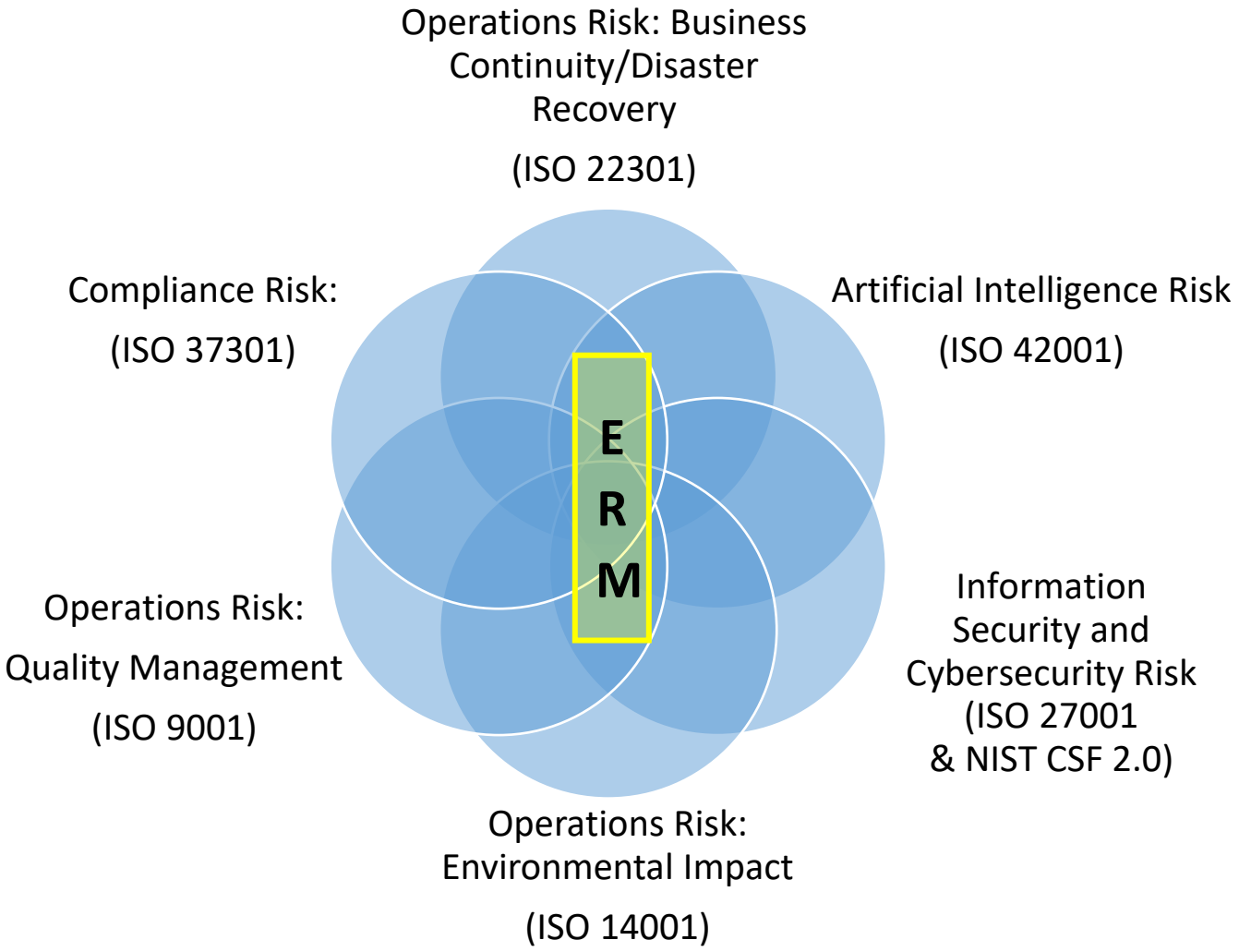
- CEO / Managing Director / Policy Approvers / Strategy Decision Makers
- Chief Information Officer (CIO / CISO)
- Information security managers
- Compliance officers
- Risk managers
- Business Continuity Managers
- Health, Safety, and Environment (HSE) Managers
- Facilities managers
- Operations department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

Further your career with CIS qualifications

## 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*.

1004 Green Pine Circle • Orange Park, Florida 32065 • USA
US 888.547.3481 • Int'l 904.406.4311 • Fax 786.522.9063
info@certifiedinfosec.com • www.certifiedinfosec.com

# ISO 42001 AI MANAGEMENT SYSTEM TRAINING

2-Day Seminar

Recommended Pre-requisite Training:
**CIS Policy Workshop:**
***ISO 31000 Enterprise Risk Management***

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 **30% discount** from public session fees.

## Understanding ISO 42001

ISO 42001, officially known as ISO/IEC 42001:2023, is the world's first AI management system standard. It specifies the requirements for establishing, implementing, maintaining, and continually improving an Artificial Intelligence Management System (AIMS) within organizations. This standard is designed for entities providing or utilizing AI-based products or services, ensuring responsible development and use of AI systems.

The significance of ISO 42001 lies in its comprehensive approach to managing AI. It addresses the unique challenges posed by AI, such as ethical considerations, transparency, and continuous learning. By providing a structured way to manage risks and opportunities associated with AI, ISO 42001 helps organizations balance innovation with governance.

## Implementing ISO 42001 for responsible and trustworthy use of Artificial Intelligence

While the benefits of AI are undeniable, it is crucial to implement AI systems responsibly. ISO 42001 provides a robust framework for achieving this. Here are some key aspects of the standard:

- **Risk Management:** ISO 42001 requires organizations to implement processes for identifying, analyzing, evaluating, and monitoring risks associated with AI systems. This ensures that potential issues are addressed proactively, minimizing the impact on business operations.

  ***NOTE**** - Development of the risk assessment and risk treatment processes required by ISO 42001 is tought seperately in CIS' ISO 31000 and ISO 23894 risk management training recommended as pre-requisite for attendance of thisISO 42001 AI Management System training.

- **Ethical Considerations:** The standard emphasizes the importance of ethical AI use. Organizations must ensure that their AI systems are transparent, fair, and accountable. This includes addressing biases in AI algorithms and ensuring that AI decisions can be explained and justified.
- **Continuous Improvement:** ISO 42001 promotes a culture of continuous improvement. Organizations are required to monitor the performance of their AI systems and implement corrective actions as needed. This ensures that AI systems remain effective and relevant in a rapidly changing

ISO 42001's Annex B, Clause 3.2 describes key roles shared by various organizations collaborating to develop, implement, and utilize AI. These roles, namely **AI Producer**, **AI Developer or Provider**, and **AI User**, each carry specific responsibilities critical for AIMS implementation. Regardless of your organization's role in AI, the ISO 42001 management system framework is the proven roadmap to success.

## What you'll get from this course

- Get thorough coverage of ISO 42001 requirements and recommendations for AI strategy, governance, roles and responsibilities, risk management, assessment, monitoring, review, and improvement;
- Learn how to integrate AI risk management into overall Enterprise Risk Management; and
- Be fully capable of integrating a robust and certifiable 42001 AI Management System.

## Become an ISO 42001 Lead Implementer and Lead Auditor

**Certified ISO 42001 AI Lead Implementer** is the AI management credential supporting a career in the responsible design, development, deployment, use, evaluation and improvement of AI products, services, and systems. This certification validates competence and understanding for developing and managing AI management based upon the ISO 42001 and ISO 23894 international standards of best practices.

**Certified ISO 42001 Lead Auditor** certification extends the Lead Implementer credential with an additional examination validating competence and skills required for internal assessment and external assurance auditing of AI management systems conforming to ISO standards of best practices.

## Who should attend

- **Leadership and Governance:** Set the overall direction for responsible AI development, including policies related to ethics, transparency, and accountability;
- **AI System Management:** Individuals or teams who manage the entire AI system lifecycle, from concept to deployment, including risk assessments and mitigation strategies;
- **Compliance Officers:** Ensure compliance with ISO 42001 standards, as well as managing risks associated with AI development and use;
- **Data Scientists and Developers:** Design, develop, and implement AI systems;
- **Risk Management Teams:** Conduct thorough risk assessments to identify potential risks associated with AI systems, including safety, privacy, and ethical concerns, and develop mitigation plans; and
- **Audit and Review Teams**