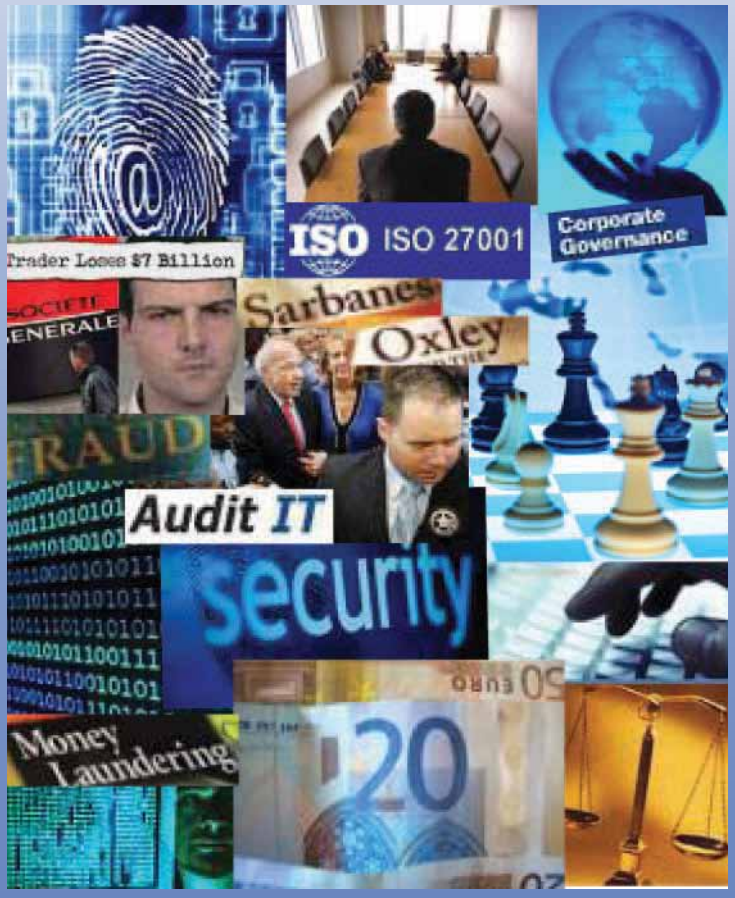
WORLD CLASS CORPORATE GOVERNANCE & COMPLIANCE TRAINING

CERTIFIED Information Security™

2016 SEMINAR CATALOG



- ISO 31000 ENTERPRISE RISK MANAGEMENT
- ISO 27001 INFORMATION SECURITY GOVERNANCE
- ISO 22301 BUSINESS CONTINUITY & DISASTER RECOVERY MANAGEMENT
- ISO 37001 ANTI-BRIBERY & ANTI-CORRUPTION
- FRAUD PREVENTION, DETECTION, & INVESTIGATION
- CIPS PROCUREMENT & SUPPLY MANAGEMENT

www.certifiedinfosec.com

1004 Green Pine Circle • Orange Park, FL • 32065 • USA • Tel: + 1 (904) 406 4311• Fax: +1 (786) 522-9063

Our business is training you to improve your business.

We offer world-class management training for a variety of urgent corporate governance and compliance issues in today's competitive world. Our instruction is provided by published authors, noted speakers, and recognized industry experts.

Since 1999, Certified Information Security has been helping board members, officers, and management gain the critical new knowledge and skills they need to meet internal and external expectations for prudent corporate governance.

Our business training advocates and facilitates a risk-based approach to corporate governance that ensures:

- Precise and appropriate internal controls investment – fulfilling, but not exceeding, all critical organizational business objectives including those related to business process efficiency, performance, availability, and compliance with laws and regulations;
- A structured approach to internal controls deployment, management, and monitoring according to ISO/IEC best practices;
- Effective prevention, detection, investigation, and containment of costly internal fraud and abuse;
- More efficient strategy-driven ISO standard conforming enterprise risk management, information security, and business continuity and disaster recovery management; and
- Fully optimized procurement and supply management according to the practices advocated by the Chartered Institute of Purchasing & Supply (CIPS).

Allen Keele, President & CEO

CISA CISM CISSP

CERTIFIED INTERNAL CONTROLS Risk Analyst ISO 31000

CERTIFIED INTERNAL CONTROLS Architect ISO 27001

CERTIFIED FRAUD CONTROL Manager

CERTIFIED BUSINESS CONTINUITY Manager ISO 22301

At Certified Information Security, we understand and respect that our training is ultimately judged by the return your organization realizes from its corresponding investment. Each of our custom-designed workshop-oriented seminars prove their value by providing explicit and tangible recommended actions for achieving early and measurable improvement and savings. Our customers leave our seminars with a clear action plan for moving forward.

Our president and lead seminar facilitator, Allen Keele, is accredited as an ISO 31000 Certified Internal Controls Risk Analyst, ISO 22301 Certified Business Continuity Manager, ISO 27001 Certified Internal Controls Architect, Certified Fraud Control Manager, Certified Fraud Examiner, Certified Information Security Manager, a Certified Information Systems Auditor, a Certified Information Systems Security Professional, and has over 20 other professional and technical accreditations. Mr. Keele shares over eighteen years of experience in information security and risk management, including thirteen years of conducting professional advanced business lectures and seminars across the United States, the United Kingdom, Asia, and Caribbean. He has spoken many times on behalf of the Institute for Internal Auditors (IIA) and for the Information Systems Audit and Control Association (ISACA). He was a featured speaker for ISACA at its North American conference, CACS. Mr. Keele is also a published author with six texts currently available. His sixth title, *CISA: Certified Information Systems Auditor Study Guide 4th Edition,* was released in March 2016.

Our customers include:

ABN AMRO
AIG
American Express
Bayer Healthcare
Brink's Incorporated
British Gas
British Telecom
Cable & Wireless Telecommunications
Comcast
CUNA Mutual
Deloitte Touche
Duke Energy
Eastern Caribbean Central Bank
Ernst & Young
Financial Guaranty Insurance Company (FGIC)
Fujitsu
General Dynamics
Guardian Life
Hewlett-Packard
IBM
ING
Intuit
J.P. Morgan Chase Bank
Janus Associates
Johnson and Johnson
Mayo Clinic
Northrop Grumman
Protiviti
Research in Motion (Blackberry)
Romtelcom
United States Department of Defense National Security Agency
Raytheon
Royal Caribbean
Towers Perrin
United States Marine Corps
United States Department of Treasury

FRAUD CONTROL CERTIFICATION

Why should you become a fraud control professional?

In a world fraught with personal and corporate financial insecurity, the need for skilled and knowledgeable fraud-control professionals has never been greater. As profits drop and budgets tighten, many internal managers and even officers feel forced to become "creative" with internal accounts. Employees and management alike now face multiple layoffs - often eliminating employee loyalty while making employees desperate with the prospect of living in a global economy that has all but collapsed. It has been estimated that internal occupational fraud and abuse costs organizations around 7% of gross revenues. Organizations need to stop this hemorrhage of profits, and they need to recover what has already been lost.

Moreover, compliance with local and international laws and industry regulations such as Sarbanes-Oxley, BASEL II, CICA Instrument 52-109, and J-SOX have raised the bar globally for professional business practices expected of organizations in terms of internal fraud control, which have in turn increased the need for professionals who know how to help organizations build and maintain a strong fraud-control capability.

The Credential You Need

Your experience in the field is an important component of your value to an employer. But experience isn't enough. Employers need something quantifiable and verifiable to show them you have the know-how they need. Combined with our intensive fraud prevention, detection, and investigation training, CIS credentials such as Certified Fraud Control Associate (CFCA™), Certified Fraud Control Professional (CFCP™), or Certified Fraud Control Manager (CFCM™) can give you the complete package employers are looking for. ***Positions in many large corporations and governmental agencies worldwide now require certification, and credentialed practitioners have a higher earning potential and greatly expanded career opportunities***. Moreover, being certified makes a statement about who you are. You'll be recognized as a knowledgeable, serious, dedicated professional – part of a globally recognized family of business professionals.

Being a member of the CIS certified body of professionals says a lot about who you are, which is, after all, a consummate professional in a world fraught with security threats, including fraud incidents and other business disruptions. Certification gives you the backing, the education, the colleagues, the networking system, and the power to face these threats head on.

With CIS certification, you'll be part of a globally recognized family of information professionals. You'll have access to our full spectrum of global resources, inside informational activities, private forums and peer networking, mentoring and sponsoring, research and teaching, and a wealth of ongoing fraud control management tools at your fingertips.

The Credentialing Process

Achieving your certification is a several step process:

1. **Obtain the Required Experience** – The CIS fraud control certifications have varying experience requirements. Please see the following page to determine which CIS fraud control credential is right for you.
2. **Academic Study** – Taking advantage of the educational materials and courses CIS makes available for you to review and refresh your knowledge before taking the credential examination.
3. **Application** – You must apply for certification and validate your education and/or experience.
4. **Examination** – You must pass the appropriate exam.
5. **Code of Ethics** – You must commit to and abiding by principles and guidelines set forth by CIS.
6. **Endorsement Process** – You must obtain and submit candidate endorsements attesting to your fulfillment of certification eligibility requirements

See complete details of the CIS credentialing process at ***www.certifiedinfosec.com***.

Certified Fraud Control Associate™ (less than two years of experience)

CERTIFIED FRAUD CONTROL Associate™

Fast-track your career with the support and strength of Certified Information Security's body of certified professionals. If you're a student or career changer considering moving into the field of information security, or just starting out in fraud control management, you are eligible to become certified as a Fraud Control Associate by Certified Information Security. By aligning yourself with an industry leader in fraud control education, you're jumping ahead of thousands of others vying for solid positions in the early stages of their careers. Fraud Control is an immensely rewarding career with unlimited possibilities. Earning your CFCA™ is an excellent way to get off to a good start!

Certified Fraud Control Professional™ (at least two years of experience)

CERTIFIED FRAUD CONTROL Professional™

You have already been involved with controlling fraud in your career as an accountant, human resource professional, auditor, security professional, or manager, but are now ready to base your career in fraud control. Your experience in the field is an important component of your value to an employer. But experience just isn't enough. Employers need something quantifiable and verifiable to show them you have the expertise they need. Earning the CFCP™ certification will give you the credential and proof of expertise today's employers require.

Certified Fraud Control Manager™ (at least five years of experience)

CERTIFIED FRAUD CONTROL Manager™

One of your primary responsibilities is protecting the organization from suffering losses and business disruption resulting from internal occupational fraud and abuse. Your experience in the field is an important component of your value to an employer. As a designated leader of fraud prevention, detection, and investigation processes, your employer counts on you to mitigate fraud risk throughout the enterprise. But experience just isn't enough. Employers need something quantifiable and verifiable to show them you have the expertise they need, and you want to establish occupational identity with a respected certification in internal fraud risk prevention and mitigation. Earning the CFCM™ certification will give you the credential and proof of expertise today's employers require.

See complete details of all CIS fraud control certifications at ***www.certifiedinfosec.com***.

1-Day Seminar

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

Continuing Professional Education Credit Hours: ***8***

Available only 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

FRAUD AWARENESS FOR MANAGERS

Make your managers better aware of fraud and how to minimize fraud risk

An excellent general one-day fraud primer for developing and implementing an anti-fraud program, Fraud Awareness for Managers engages participants in an absorbing learning experience to develop familiarity with the practical aspects of fraud detection and prevention.

Learning Objectives

Whether you are an internal or external auditor, accountant, senior financial executive, department head, accounts payable professional, credit manager, or financial services manager, this invaluable one-day seminar provides managers with timely discussion on:

- ◊ **Why No Organization Is Immune to Fraud (Approximately 30 minutes)**
- ◊ **The Human Element of Fraud (Approximately 40 Minutes)**
- ◊ **Internal Fraud: Employee Level (Approximately 90 minutes)**
- ◊ **Internal Fraud: Management Level (Approximately 75 minutes)**
- ◊ **External Fraud: Protecting Against Dishonest Outsiders (Approximately 60 minutes)**
- ◊ **Conducting a Successful Fraud Risk Assessment (Approximately 40 minutes)**
- ◊ **Basic Fraud Detection Tools and Techniques (Approximately 30 minutes)**
- ◊ **Advanced Fraud Detection Tools and Techniques (Approximately 30 minutes)**

Complete details are too lengthy to list on this page. Please visit www.certifiedinfosec.com for further information.

Who should attend

- Executive officers (CEO/CFO/COO...)
- All Operations Managers and Department Heads
- Internal fraud investigators / examiners
- Financial auditors / examiners
- Operations auditors
- Systems auditors
- Human resource managers
- Accountants
- Payroll administrators
- Accounts payable/receivable administrators
- Finance department managers
- Sales managers
- Security managers

Extensive detailed topic outline is available upon request.

FRAUD AWARENESS FOR FINANCIAL INSTITUTIONS

1-Day Seminar

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

Continuing Professional Education Credit Hours: ***8***

Available only 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

Make your managers better aware of fraud and how to minimize fraud risk at financial institutions

An excellent one-day fraud primer for developing and implementing an anti-fraud program specifically at banks and other financial institutions, Fraud Awareness for Financial Institutions engages participants in an absorbing learning experience to develop familiarity with the practical aspects of fraud detection and prevention at banks, investment firms, credit unions, insurance companies, and other financial services providers.

Learning Objectives

Whether you are a bank executive, auditor, accountant, senior financial executive, financial services operations manager, loan officer, regulator, examiner, or even branch manager, this invaluable seminar provides you with essential coverage of:

- ◊ **Why No Financial Services Institution Is Immune to Fraud (Approximately 20 minutes)**
- ◊ **The Human Element of Fraud (Approximately 40 Minutes)**
- ◊ **Internal Fraud: Loan and Mortgage Fraud Basics (Approximately 75 minutes)**
  - Loan Fraud (Non-residential Mortgage)
  - Mortgage Fraud: Types of Internal Mortgage Fraud to Beware Of
  - Red Flags of Employee-Level Loan and Mortgage Fraud
  - Preventing Employee-Level Loan and Mortgage Fraud
- ◊ **Employee-Level Embezzlement (Approximately 75 minutes)**
  - Looting Customer Accounts
  - Looting Non-Customer Funds
  - Theft of Confidential Information
  - Insider Abuse of Computer Systems
  - Red Flags of Employee-Level Embezzlement
  - Preventing Employee-Level Embezzlement and Information Theft
- ◊ **Internal Fraud: Management Level (Approximately 75 minutes)**
  - Looting and Embezzlement
  - Illegal Financial Transactions/Corruption
  - Fraudulent Financial Reporting
  - Deceiving Borrowers, Investors, and Regulators
  - Red Flags of Management-Level Internal Fraud
  - Management-Level Fraud Prevention Checklists
- ◊ **External Fraud against Financial Services Companies (Approximately 60 minutes)**
  - Externally Perpetrated Loan Fraud (Non-mortgage)
  - Externally Perpetrated Mortgage Fraud Schemes
  - New Forms of Identity Theft and Fraud
  - Red Flags of External Fraud
  - External Fraud Prevention Checklists
- ◊ **Conducting a Successful Fraud Risk Assessment (Approximately 30 minutes)**
- ◊ **Legal and Regulatory Compliance for Controlling Fraud Risk (Approximately 30 minutes)**
- ◊ **Fraud Detection in Financial Services Companies (Approximately 30 minutes)**

Who should attend

- Executive officers (CEO/CFO/COO...)
- All Operations Managers and Department Heads
- Internal fraud investigators / examiners
- Financial auditors / examiners
- Operations auditors
- Systems auditors
- Human resource managers
- Accountants
- Payroll administrators
- Accounts payable/receivable administrators
- Finance department managers
- Sales managers
- Security managers

Extensive detailed topic outline is available upon request.

3-Day Seminar

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

Continuing Professional Education Credit Hours: ***24***

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

CORPORATE FRAUD PREVENTION & DETECTION

Step 1: Establish and manage a better anti-fraud function

Discover what should be done to better protect your company from fraud. Learn what you need to do to build a fraud control function - complete with proper fraud function policies, ethics policies, and acceptable conduct guidelines. This course will take you further into leading techniques to manage the risk of fraud and cut its ongoing cost for all types of organizations. You and your decision-making executives will leave with a clear understanding of what business processes need to be created or improved, as well as what roles, responsibilities, and authorization need to be in place.

Get a broad understanding of the field of fraud examination — from what fraud is, to how it is committed, detected, and deterred. Coverage begins with an explanation of fraud examination methodology, followed by detailed examination of the most prevalent fraud schemes used by employees, owners, managers, and executives.

Step 2: Train the right people to prevent and detect fraud

Based upon courseware endorsed by the Association of Certified Fraud Examiners and presented by a fully accredited Certified Fraud Examiner, this seminar provides the understanding and the tools you need to prevent and detect internal (occupational) fraud within your organization.
Modules explain the major schemes and provide relevant statistics on cost and frequency, as well as the perpetrators and victims of these crimes. Each scheme is illustrated with several real-life cases. The course clearly outlines prevention, detection and investigation strategies. Essential terms, questions, and discussion issues help students understand and retain the material. Not to be confused with forensic accounting instruction, this course is designed for a broad corporate management audience.

1. Skimming
2. Cash Larceny
3. Billing Schemes
4. Check Tampering
5. Expense Reimbursement Schemes
6. Register Theft Disbursement Schemes
7. Theft of Non-Cash Assets
8. Corruption and Collusion
9. Common Accounting and Transaction Fraud
10. Fraudulent Financial Statement Schemes
11. Interviewing Witnesses Overview *

To ensure that your organization will achieve early success in detecting internal fraud and abuse, attendees will receive information on 178 proactive computerized audit queries that can be performed to help uncover potential problems. Attendees will also analyze and retain 18 case studies to help them get a better real-life exposure to fraud in the work-place.

* ***For more information on this topic, "Interviewing Witnesses", we recommend Advanced Interview Techniques for Investigating Internal Fraud and Abuse as a subsequent follow on to this course.***

Who should attend

- Internal fraud investigators / examiners
- Executive officers (CEO/CFO/COO...)
- Financial auditors / examiners
- Operations auditors
- Systems auditors
- Human resource managers
- Accountants
- Payroll administrators
- Accounts payable/receivable administrators
- Finance department managers
- Sales managers
- Security managers

Prepare to be certified.

Attendance of this course is required to be eligible to take exam FC101 for CIS fraud control certification. Learn more about the Certified Fraud Control Associate (CFCA), Certified Fraud Control Professional (CFCP), and Certified Fraud Control Manager (CFCM) credentials at www.certifiedinfosec.com.

Extensive detailed topic outline is available upon request.

2-Day Seminar

Recommended Pre-Requisite Training: ***Corporate Fraud Prevention and Detection***

Continuing Professional Education Credit Hours: ***16***

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

Step 3: Once the right people have learned how to find evidence of fraud, train them to investigate and interview

Even good employees sometimes do bad things. If your organization encounters an instance of employee abuse or fraud such as misuse of company resources, theft of assets, fraudulent disbursement, or other issues, investigation of the incident will require interviewing and interrogating employees. Such interviews require special preparation, documentation, and interviewing skills in order to resolve cases of internal fraud or abuse.

Learning Objectives

What are people hiding from you? Criminals, clients, customers and even colleagues may each be hiding something from you. Learn how to be more effective in asking questions and evaluating responses so you can better detect lies and uncover the truth. By enhancing your interview techniques, you will get more information, more insight and less deception from everyone you interview. Even experienced professionals will improve their interviewing skills with this renowned course.

This two-day workshop will give you the knowledge and skills you need to effectively interview and interrogate witnesses, conspirators, and perpetrators potentially involved with incidents of fraud or abuse. Set into a practical workshop format, important concepts are reinforced through your in-class analysis of real videotaped interviews from actual investigations of two cases of internal employee fraud. Concepts are further reinforced through 14 workshop case studies you will help solve in class along with other attendees.

- **Know your boundaries: Legal considerations for investigating and interviewing employees**
  - Do you know your legal authority for conducting interviews?
  - Can you use deception in interviews?
  - How do you avoid breaching the employees' rights under law?
  - How do you avoid employee claims of breach of privacy, emotional distress, defamation, false imprisonment, or assault and battery?
  - What about trade union protection?
- **Understand the science of communication**
  - What are communication facilitators and inhibitors?
  - What is the employee really saying with word choice, tone, and syntax?
  - What is the employee really saying with body language from the head, face, nose, mouth, eyes, arms, shoulders, elbows, hands, legs, feet, and posture?
  - What is the employee really saying with anger, boredom, frustration, and body movements?
- **Learn how to prepare for the interview**
  - How do you prepare for the investigation? Who should participate in your investigative team?
  - How do you develop evidence? How do you organize, handle, and preserve it?
  - How do you properly establish the foundation for your investigation?
  - What is the best venue and physical environment for interviewing?
  - How should you plan the interview for witnesses, conspirators, and perpetrators?
- **Learn how to conduct the interview**
  - What are 13 verbal clues of deception you need to recognize?
  - What are 10 non-verbal clues of deception you need to recognize?
  - What is the proper interviewing sequence and use of questioning? How do you open the interview, get good information, resolve contradictions or deceit, and close the interview?
  - What is the best approach to obtaining an admission of guilt? How do you help the employee rationalize what he or she did and tell you what truly happened?
- **Know how to report your findings**
  - How should your findings be presented to company insiders, attorneys, defendants & witnesses, the press, or juries?
  - What is a good report structure for presenting your findings?

Prerequisite requirement

This workshop is an advanced course especially designed to help attendees investigate incidents of internal fraud or abuse, which are taught in this course's prerequisite ***Corporate Fraud Prevention & Detection***.

Prepare to be certified.

Attendance of this course is required to be eligible to take exam FC102 for CIS fraud control certification.

Extensive detailed topic outline is available upon request.

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

BUSINESS CONTINUITY MANAGEMENT CERTIFICATION

Why should you become a business continuity management professional?

Since Business Continuity Management is more important than ever in today's risk conscious business environment, and because international standards such as ISO 22301 and BS 25999 now provide the opportunity for the organization to certify its Business Continuity Management System, organizations have a new and pressing need for professionals especially trained and skilled at establishing, managing, exercising, and maintaining business continuity according to this new international standard of best practice. Because business continuity planning and response procedures often are inadequate due to the limitations of knowledge and involvement of corporate governance decision makers, the Standard requires exactly the kind of evidence of training and documented understanding the CIS BCM credentialing scheme provides. If an organization wants to get its own ISO 22301, it needs evidence of appropriate training and competence to fulfil the certification requirements of the standard itself.

Certified Information Security provides the third-party training and professional credentialing necessary to set you apart as a BCM authority who knows BCM according to the only international standard of BCM best practices.

The Credential You Need

Your experience in the field is an important component of your value to an employer. But experience isn't enough. Employers need something quantifiable and verifiable to show them you have the know-how they need. Combined with our intensive business continuity and disaster recovery training, CIS credentials such as Certified Internal Controls Risk Analyst (CICRA™), Certified Business Continuity Strategist (CBCS™), Certified Business Continuity Administrator (CBCA™), or Certified Business Continuity Manager (CBCM™) can give you the complete package employers are looking for. ***Positions in many large corporations and governmental agencies worldwide now require certification, and credentialed practitioners have a higher earning potential and greatly expanded career opportunities***. Moreover, being certified makes a statement about who you are. You'll be recognized as a knowledgeable, serious, dedicated professional – part of a globally recognized family of business professionals.

Being a member of the CIS certified body of professionals says a lot about who you are, which is, after all, a consummate professional in a world fraught with security threats, including fraud incidents and other business disruptions. Certification gives you the backing, the education, the colleagues, the networking system, and the power to face these threats head on.

With CIS certification, you'll be part of a globally recognized family of information professionals. You'll have access to our full spectrum of global resources, inside informational activities, private forums and peer networking, mentoring and sponsoring, research and teaching, and a wealth of business continuity management tools at your fingertips.

The Credentialing Process

Achieving your certification is a several step process:

1. **Obtain the Required Experience** – The CIS business continuity certifications have varying experience requirements. Please see the following page to determine which CIS business continuity management credential is right for you.
2. **Academic Study** – Taking advantage of the educational materials and courses CIS makes available for you to review and refresh your knowledge before taking the credential examination.
3. **Application** – You must apply for certification and validate your education and/or experience.
4. **Examination** – You must pass the appropriate exam.
5. **Code of Ethics** – You must commit to and abiding by principles and guidelines set forth by CIS.
6. **Endorsement Process** – You must obtain and submit candidate endorsements attesting to your fulfillment of certification eligibility requirements

See complete details of the CIS credentialing process at ***www.certifiedinfosec.com***.

Extensive detailed topic outline is available upon request.

Certified Internal Controls Risk Analyst™ (less than five years of experience)

The ISO/IEC 27001 certification of an organization's Information Security Management System (ISMS) requires that all security methods and controls must be driven by risk assessment as defined in an organization's formal documented risk management methodology. ISO 22301 certification of an organization's Business Continuity Management System (BCMS) requires the same.

Because all information security analysis, controls, and processes are essentially a product of risk management, ISO 31000 and ISO 27005 provide the framework for how to apply proper risk management within the ISO/IEC 27001/27002 ISMS, or within the ISO 22301 BCMS.

The CICRA credential by Certified Information Security certifies your understanding of ISO 31000 and ISO 27005, and how these frameworks can be used to develop a custom risk management methodology that fulfills the requirements of both ISO 27001, ISO 9001, ISO 14001, and ISO 22301. It also helps fulfil the competence requirements of the certifications themselves.

Certified Business Continuity Strategist™ (less than five years of experience)

The Certified Business Continuity Strategist (CBCS) certification by CIS certifies your ability to develop the formal structure, governance, and policy of the Business Continuity Management System (BCMS). Furthermore the CBCS certification ensures that you are qualified to develop strategic objectives including, but not limited to:

- Determining and guiding the selection of alternative business recovery operating strategies for continuation of business within recovery time and/or recovery point objectives, while maintaining the organization's critical functions.
- Delivering solutions for continuation of business within the recovery time and/or recovery point objectives, whilst maintaining the organization's critical functions.
- Developing, coordinating, evaluating and creating plans and procedures to communicate with internal stakeholders during incidents.
- The provision of post-incident support and guidance for employees and their families.

Certified Business Continuity Administrator™ (less than five years of experience)

Building upon the foundation understanding of the ISO 22301 and BS 25999 Business Continuity Management System (BCMS) platform validated by the Certified Business Continuity Strategist credential, the Certified Business Continuity Administrator (CBCA) certification by CIS attests to your ability to develop the necessary incident management plans (IMPs) and response procedures necessary to fulfill the strategic objectives that have already been finalized. The CBCA also certifies that you have the necessary knowledge and skills to properly administrate the deployment, testing, and maintenance of IMPs and response procedures.

Certified Business Continuity Manager™ (more than five years of experience)

Building upon the foundation understanding of the ISO 22301 and BS 25999 Business Continuity Management System (BCMS) platform validated by the Certified Business Continuity Strategist credential, the Certified Business Continuity Manager (CBCM) certification by CIS attests to your ability ***and experience*** to develop the necessary incident management plans (IMPs) and response procedures necessary to fulfill the strategic objectives that have already been finalized. The CBCM also certifies that you have the necessary knowledge, skills, ***and experience*** to properly administrate the deployment, testing, and maintenance of IMPs and response procedures.

Extensive detailed topic outline is available upon request.

BUSINESS CONTINUITY AND DISASTER RECOVERY ACCORDING TO ISO 22301 AND ISO 22313 STANDARDS

Your revenues are important

Continued operations in the event of a business disruption, whether due to a major disaster or a minor incident, are a fundamental requirement for any organization. Ensuring operational continuity has led to the development of Business Continuity Management (BCM) as a recognized business discipline, but not until the recent publication of BS 25999 has there been an internationally-recognized management framework that adds consistency, credibility and viability to your existing BCM programs.

What is ISO 22301?

ISO 22301 and ISO 22313 are new visionary international standards designed to keep your business going during the most challenging and unexpected circumstances. It provides a basis for understanding, developing, implementing and managing business continuity within your organization and gives you confidence when dealing with stakeholders both within and outside your organization.

Can our organization become certified?

ISO 22301 is an auditable specification standard, which means that through certification by an accredited certification body, you have a framework for continuous improvement and the ability to demonstrate to your stakeholders that your BCM programs meet best practice. Above all, when implementing a Business Continuity Management System and choosing Certified Information Security to train you to understand and meet the requirements of ISO 22301, your organization will be prepared to prove the validity of its BCM programs, preserve its reputation, and enable it continue to operate and trade through business disruptions.

Who is it for?

ISO 22301 has been developed by a group of world-class experts representing a cross-section of industry sectors and governmental organizations which is reflected in its applicability. The standard is suitable for any organization, large or small, from any sector. It is particularly relevant if you operate in a high risk environment such as the finance, telecommunications, transport, utilities and public sectors, where the ability to continue operating is paramount for both you and your stakeholders.

Isn't this pretty much the same as what we have been doing with DRI or BCI in the past?

No.

Previous guidance and training provided by Disaster Recovery Institute International (DRI) or the Business Continuity Institute (BCI) have been largely obsoleted by official international standard ISO 22301.

Neither DRI nor BCI certify business continuity management systems for organizations. ISO 22301 provides a very different and much more mature and business-savvy approach to developing and governing a true business continuity management system (organizational business methodology), supported by appropriate planning and procedures. It introduces an entirely new BCM life cycle approach, and requires deployment according to the Plan-Do-Check-Act Shewhart/Deming cycle. Previous DRI and BCI approaches placed little emphasis on providing structure or specification for the foundation business function of Business Continuity Management, and rather focused on rudimentary concepts of risk management married to loosely-developed recommendations for mitigating procedures. Managing business continuity according to ISO 22301 represents a light-year leap ahead in terms of effectiveness, cost-efficiency, and business strategy maturity.

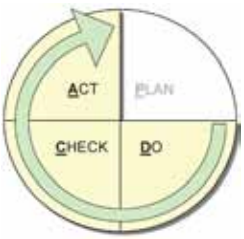
Benefits from adopting ISO 22301 and ISO 22313 for Business Continuity Management

- **Framework**: Provides a common consistent framework, based on international best practice, to manage business continuity.
- **Resilience**: Pro-actively improves your resilience when faced with disruptions to your ability to achieve key objectives.
- **Delivery**: Provides a rehearsed method of restoring your ability to supply critical products and services to an agreed level and time frame.
- **Management**: Delivers a proven response for managing a disruption.
- **Reputation**: Helps protect and enhance your reputation and brand.
- **Competitive advantage**: Opens new markets and helps you win new business.
- **Continuous business improvement**: Enables a clearer understanding of how your entire organization works which can identify opportunities for improvement.
- **Compliance**: Demonstrates that applicable laws and regulations are being observed.
- **Cost Savings**: Creates an opportunity to reduce the burden of internal and external BCM audits and may reduce insurance premiums.

Two seminars are available

This new BCM training series offered by Certified Information Security has been completely re-authored from the ground up to map precisely to ISO 22301 and ISO 22313. We have even empowered this new training further by injecting advanced risk management content from risk assessment framework ISO/IEC Standard 27005:2011, and additional security concepts from ISO/IEC 31000 and 31010 where appropriate.

First Session: **Policy Workshop: ISO 22301 Business Continuity Management (2-Days)**
ISO 22301 advocates applying the same Plan-Do-Check-Act management methodology found in many other BSI, ISO, and IEC standards. Accordingly, this initial session course addresses BCMS Life Cycle key concepts required for BCMS planning, with a heavy emphasis on establishing effective risk management and business impact assessment processes. This course naturally serves as a prerequisite for attendance of "*Best Practices to Develop, Exercise, and Certify Business Continuity and Disaster Recovery Processes*".



Second Session: **Best Practices to Develop, Exercise, and Certify Business Continuity and Disaster Recovery Processes (2-Days)**
This follow-on course addresses BCMS Life Cycle key concepts required for BCMS "Doing, Checking, and Acting" in accordance with ISO 22313 best practices. Prior attendance of "Establishing a Business Continuity Management System" is a prerequisite for attending this course.

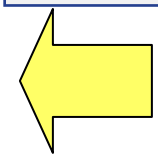
Prepare to be certified.

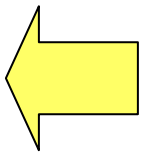
Attendance of these courses is required to be eligible to take CIS certification exams RM101, BCMS101, and/or BCMS102 for CIS risk analyst and/or business continuity management certification. See **www.certifiedinfosec.com** for complete details.

Policy Workshop: ISO 22301 Business Continuity Management:
- 2-Day Seminar
- Recommended Pre-Requisite Training: ***Policy Workshop: ISO 31000 Enterprise Risk Management***
- CPE Credit Hours: ***16***

Best Practices to Develop, Exercise, and Certify a BCMS:
- 2-Day Seminar
- Recommended Pre-Requisite Training: ***Policy Workshop: ISO 22301 Business Continuity Management***
- CPE Credit Hours: ***16***

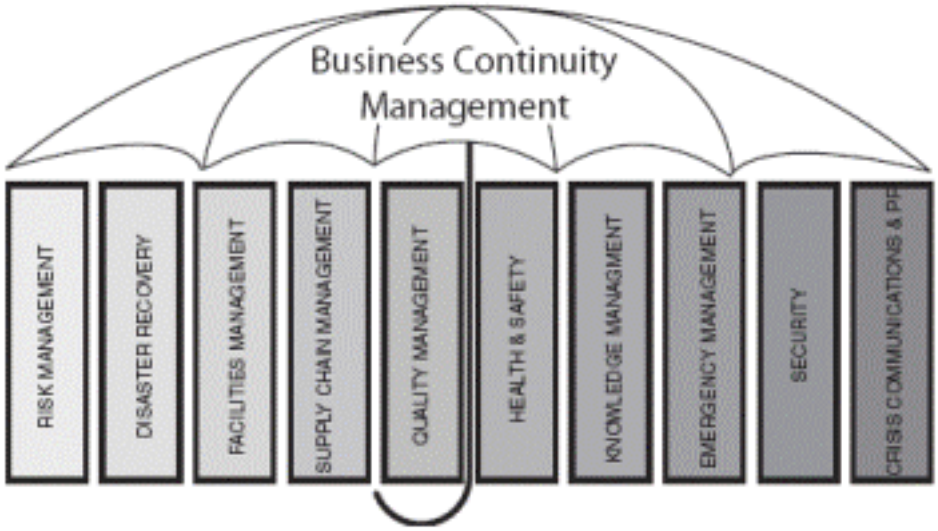
For currently scheduled seminars please see www.certifiedinfosec.com
+1 (888) 547-3481 (USA)
+1 (904) 406-4311





BUSINESS CONTINUITY MANAGEMENT TRAINING OFFERED

Who should attend



- Business Continuity Managers
- Operational Risk Managers
- Operations managers / Department heads
- Business Continuity/Disaster Recovery Steering Committee Members
- Business Continuity/Disaster Recovery Team Leaders
- Human Resource Managers
- Quality Managers
- IT Managers
- Facility Managers
- Public Relations / Corporate Communications Managers
- Information Security Professionals
- Emergency, Health, and Safety Managers
- Consultants
- Internal and external auditors responsible for auditing business continuity practices
- Other professionals interested or involved with introducing business continuity management into an organization

Business Continuity Management Roadmap

Session I:
CIS Policy Workshop: *ISO 22301 Business Continuity Management*

Session II:
Best Practices to Develop, Exercise, and Certify Business Continuity and Disaster Recovery Processes

BUSINESS CONTINUITY & DISASTER RECOVERY

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 22301 BUSINESS CONTINUITY MANAGEMENT

Get a thorough understanding of the ISO 22301 and 22313 standards for business continuity and disaster recovery management, how to leverage the standards to establish and maintain an business continuity management system (BCMS) program. Then build-out the initial ISO 22301-conforming information security program policy right in class!

Why Business Continuity Management?
No two organizations are exactly alike. Even within the same industry and sector, every organization has unique goals, objectives, stakeholders, business processes, and risk tolerance. Ensuring that business processes and related assets ***reliably*** fulfil the organization's strategy is critical to the organization's long-term survival. In order to craft incident response that best fits your organization's needs, you need to establish a system for ongoing understanding and management of those needs. Trying to develop business continuity and contingency procedures before determining what your organization needs and what levels of risk it will tolerate, is akin to trying to author a book without first determining a plot.

The relationship with risk management.
BCM is complementary to a risk management framework that sets out to understand the risks to operations or business, and the consequences of those risks. Risk management seeks to manage risk around the key products and services that an organization delivers. Product and service delivery can be disrupted by a wide variety of incidents, many of which are difficult to predict or analyze by cause.

What you and your colleagues will achieve

This 2-day training and workshop session provides thorough coverage of ISO 22301, as well as setting out advice on the implementation of a business continuity initiative. The purpose of the course is to:

- Describe the principles and processes of business continuity governance and management;
- Provide an overview of the requirements of ISO 22301 and ISO 22313;
- Give practical guidance on designing a suitable framework;
- Give practical advice on business continuity management;
- Establish a firm program starting point by using ISO 22301 to build out the initial Business Continuity Management core policy.

Course Content Details

1. Business Continuity and Disaster Recovery Management, and ISO 22301

- Principles of business continuity, disaster recovery, and incident response
- Review of ISO 22301 and BS 25999
- Achieving the benefits of Business Continuity and Disaster Recovery

2. Business Continuity Management

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

3. Establish a firm program starting point by using ISO 22301 to build out the initial Business Continuity Management core policy. Throughout the class, our expert instructor will convert ISO 22301 and ISO 22313 concepts and requirements into a real ISO 22301-conforming Business Continuity 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 Business Continuity and Disaster Recovery program properly initiated by constructing:

- Business Continuity Management System Policy (29-page template provided)
- Procedure for Training and Development Needs Analysis document (8-Page template provided)
- BCMS Program project kick-off document (9-Page template provided)

Who should attend

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

INFORMATION SECURITY MANAGEMENT CERTIFICATION

Why should you become an information security management professional?

Since information security is more important than ever in today's risk conscious business environment, and because the ISO/IEC 27001 Standard now provides the opportunity for the organization to certify its Information Security Management System, organizations have a new and pressing need for professionals especially trained and skilled at establishing, managing, exercising, and maintaining information security according to this new international standard of best practice. Because information security governance is often inadequate due to the limitations of knowledge and involvement of corporate governance decision makers, the Standard requires exactly the kind of evidence of training and documented understanding the CIS Certified Internal Controls Architect credentialing scheme provides. If an organization wants to get its own ISO 27001 certification, it needs evidence of appropriate training and competence to fulfil the certification requirements of the standard itself.

The Credentials You Need

Your experience in the field is an important component of your value to an employer. But experience isn't enough. Employers need something quantifiable and verifiable to show them you have the know-how they need. Combined with our intensive information security governance training, CIS credentials such as Certified Internal Controls Risk Analyst (CICRA™) and the Certified Internal Controls Architect (CICA™) can give you the complete package employers are looking for. ***Positions in many large corporations and governmental agencies worldwide now require certification, and credentialed practitioners have a higher earning potential and greatly expanded career opportunities***. Moreover, being certified makes a statement about who you are. You'll be recognized as a knowledgeable, serious, dedicated professional – part of a globally recognized family of business professionals.

Certified Information Security provides the third-party training and professional credentialing necessary to set you apart as an ISO 27001 authority who knows information security governance according to the best recognized international standard of information security best practices.

The Credentialing Process

Achieving your certification is a short straight-forward process. See complete details of the CIS credentialing process at ***www.certifiedinfosec.com***.

Certified Internal Controls Risk Analyst™

CERTIFIED INTERNAL CONTROLS Risk Analyst™ ISO 31000

The ISO/IEC 27001 certification of an organization's Information Security Management System (ISMS) requires that all security methods and controls must be driven by risk assessment as defined in an organization's formal documented risk management methodology. ISO 22301 certification of an organization's Business Continuity Management System (BCMS) requires the same.

Because all information security analysis, controls, and processes are essentially a product of risk management, ISO/IEC 27005:2008 provides the framework for how to apply proper risk management within the ISO/IEC 27001/27002 ISMS, or within the ISO 22301 BCMS. The CICRA credential by Certified Information Security certifies your understanding of ISO 31000 and ISO 27005, and how these frameworks can be used to develop a custom risk management methodology that fulfills the requirements of both ISO 27001, and ISO 22301. It also helps fulfill the competence requirements of the certifications themselves.

Certified Internal Controls Architect™

CERTIFIED INTERNAL CONTROLS Architect™ 27001/27002/27005

Building upon the foundation understanding of the ISO 31000 risk management framework validated by the Certified Internal Controls Risk Analyst credential , the Certified Internal Controls Architect (CICA) certification by CIS certifies your ability to develop the formal structure, governance, and policy of an ISO 27001 conforming Information Security Management System (ISMS). Furthermore, the CICA certification ensures that you are qualified to develop strategic objectives including, but not limited to the core ISO 27001 best practices described on the previous page.

Extensive detailed topic outline is available upon request.

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

EXECUTIVE OVERVIEW OF USING ISO 31000 and ISO 27005 TO DEVELOP AND DEPLOY ENTERPRISE RISK MANAGEMENT

1-Day Seminar

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

CPE Credit Hours: ***8***

Available only 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

One-Day Executive Overview of *Using ISO 1/ . . . to Establish a l d Manage Enterprise Risk Management*

Enterprise risk management (ERM) in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives. ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

Risk assessment and management provides the foundation for internal controls management, as well as business continuity and disaster recovery management. After all, the Information Security Management System and the Business Continuity Management System exist purely to manage risk. This means that an ISMS and a BCMS can only be a good as the organization's ability to create, authorize, and practice a single consistent approach to assessing and treating risks. The ISO/IEC 27001 certification of an organization's Information Security Management System (ISMS) requires that all security methods and controls must be driven by risk assessment as defined in an organization's formal documented risk management methodology. BS 25999-2 certification of an organization's Business Continuity Management System (BCMS) requires the same.

ISO/IEC 31000, 31010, and 27005 provide guidelines for information security and operational risk management. The standards support the risk management requirements specified in ISO/IEC 27001 and are designed to assist the satisfactory implementation of information security based on a risk management approach. As internationally accepted best practice guidelines for developing a solid risk management methodology that is fit-for-purpose for the organization, ISO 31000, 31010, and 27005 can also ensure fulfillment of ISO 22301's requirements for such a risk management capability.

The problem with many organizations is that the very people who should be leading or performing risk assessment have never been sufficiently trained to be able to do the job properly. Risk assessment and management is complex - complex enough to have its own ISO/IEC standard! Certified Information Security provides the training and credentialing you need to become recognized as an authority in leading or facilitating risk assessment and management according to the ISO/IEC risk management standards.

Corporate Governors and Senior Management will learn how to set up the enterprise risk management program, policy, and team.

Your business governors (Board Members) and your business leaders (business process owners) may not initially have the time to devote to the complete coverage of "***CIS Policy Workshop: ISO 31000 Enterprise Risk Management".*** This one-day subset session provides a concise introduction to Enterprise Risk Management as a concept, and how to use the ISO risk management frameworks to:

- Learn how to prepare the organization to properly manage operational risks
- Compare and contrast ISO 31000, 31010, 27005, and COSO risk management approaches
- Set up the Enterprise Risk Management Program, Policy, and Team
    - Learn how to properly scope the risk management program
    - Establish formal roles and responsibilities to manage operational risk throughout the enterprise
    - Establish risk context criteria for risk acceptance, risk evaluation, and business impact

Who should attend

- Executive Officers (CEO/CFO/CIO/COO)
- Information security managers
- Compliance officer
- Revenue protection manager
- Risk managers
- Operations managers
- Facilities managers
- Department heads

AUDITING OPERATIONS RISK MANAGEMENT AND THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

1-Day Seminar

Mandatory Pre-Requisite Training:

- ***Using ISO 27005 to Develop and Deploy Enterprise Risk Management***
- ***Governing Information Security Using ISO 27000 Best Practices***

CPE Credit Hours: ***8***

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

How mature and well-developed are your organization's systems for governing risk management, information security management, and business continuity management?

Organizations are striving to use risk assessments to ensure that risks to critical operations and assets are managed appropriately. Controls used to mitigate the risk of related information security concerns or other business disruptions should be selected, deployed, and managed as a result of risk assessment. Unfortunately, many organizations perform these risk assessments without first auditing the organization's own approach, competence, and methodology for managing risk to begin with. After all, how can an organization rely upon results of a risk assessment, if the risk management system driving the risk assessment is poorly defined, loosely managed, and inherently flawed?

You need to improve your organization's ability to perform risk assessment before you can use risk assessment results to improve operations and information security. Only after validating the organization's risk management system can the auditor attempt to measure the maturity and effectiveness of the business system used to govern related information security controls and management.

How we can help.

Based upon the newly released ISO 27007:2011 and 19011:2011 Standards, this one-day course will provide an intensive overview of how to manage an audit of an organization's risk management program in along with its corresponding information security management system. This course will also provide valuable guidance on conducting the audits, and on establishing and validating the competence of ISMS auditors.

What else you will learn in this one-day seminar

1. Managing a Risk Management System (RMS) and Information Security Management System (ISMS) audit program

- Establishing the audit program objectives
  - Role and responsibilities of the person managing the audit program
  - Competence of the person managing the audit program
  - Determining the extent of the audit program
  - Identifying and evaluating audit program risks
  - Establishing procedures for the audit program
  - Identifying audit program resources
- Implementing the audit program
  - Defining the objectives, scope and criteria for an individual audit
  - Selecting the audit methods
  - Selecting the audit team members
  - Assigning responsibility for an individual audit to the audit team leader
  - Managing the audit program outcome
  - Managing and maintaining audit program records
- Monitoring the audit program
- Reviewing and improving the audit program

2. Performing an audit

- Initiating the audit
  - Establishing initial contact with the auditee
  - Determining the feasibility of the audit
- Preparing audit activities
  - Performing document review in preparation for the audit
  - Preparing the audit plan
    - Auditing the RMS scope and corresponding ISMS scope, policy and risk assessment approach
    - Auditing risk identification, analysis and evaluation, and risk treatment option identification and evaluation
    - Auditing the selection of control objectives and controls, approval of the proposed residual risks, management authorization, and Statement of Applicability
    - Auditing the implementation and operation of the ISMS
    - Auditing ISMS monitoring and review processes
    - Auditing ISMS maintenance and improvement
    - Auditing ISMS documentation
    - Auditing RMS and ISMS management responsibility
    - Auditing Internal RMS/ISMS audits and RMS/ISMS management review
- Conducting the audit activities
  - Assigning work to the audit team
  - Preparing work documents
  - Conducting the audit activities
  - Preparing and distributing the audit report
  - Completing the audit
  - Conducting audit follow-up

3. Competence and evaluation of auditors

- Determining auditor competence to fulfil the needs of the audit program
- Establishing the auditor evaluation criteria
- Conducting auditor evaluation
- Maintaining and improving auditor competence

Who should attend

This course is applicable to those needing to understand or conduct internal or external audits of an risk management system supporting an ISMS, or how to manage an ISMS audit program.

Extensive detailed topic outline is available upon request.