



# Our business is training you to improve your business.



**Allen Keele, President & CEO**

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 information security governance.

Our business training advocates and facilitates a risk-based approach to information security 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; and
- More efficient strategy-driven business continuity and disaster recovery management based upon British Standard 25999

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 seminar leader, Allen Keele, is accredited as a Certified Internal Controls Risk Analyst, Certified Business Continuity Manager, Certified Fraud Control Manager, Certified Fraud Examiner, a 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 nine 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 five texts currently available. His fifth title, *ExamCram 2: Certified Information Systems Auditor*, was released in April 2005.



## Our customers include:



ABN AMRO  
AIG  
American Axle and Manufacturing  
Bayer Healthcare  
British Gas  
British Telecom  
Cable & Wireless  
Comcast  
CUNA Mutual  
Deloitte Touche  
Duke Energy  
DynaCorp  
Ernst & Young  
Financial Guaranty Insurance Company (FGIC)  
Fujitsu  
General Dynamics  
Guardian Life  
Hewlett-Packard  
Idaho Power  
IBM  
ING (Moscow)  
Intuit  
J.P. Morgan Chase Bank  
Janus Associates  
Johnson and Johnson  
Mayo Clinic  
Northrop Grumman  
Protiviti  
Research in Motion (Blackberry)  
Romtelcom  
University of Pittsburgh  
Raytheon  
Royal Caribbean  
Towers Perrin  
United States Marine Corps  
United States Department of Treasury

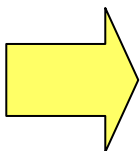
## Why should you become a fraud control professional?

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](http://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](http://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](http://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](http://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

## 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

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

3-Day Seminar

Recommended Pre-Requisite Training: *None*

Continuing Professional Education Credit Hours: **24**

For currently scheduled seminars please see [www.certifiedinfosec.com](http://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](http://www.certifiedinfosec.com).

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

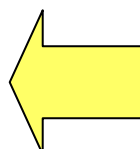
Even good employees sometimes do bad things. If your organization encounters an instance of employee abuse or fraud such as misuse of company resources, theft of assets, fraudulent disbursement, or other issues, investigation of the incident will require interviewing and interrogating employees. Such 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.



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

- ◇ **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.



## Why should you become a business continuity management professional?

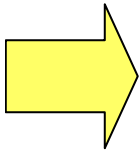
Since Business Continuity Management is more important than ever in today's risk conscious business environment, and because BS 25999 now provides the opportunity for the organization to certify its Business Continuity Management System, organizations have a new and pressing need for professionals especially 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 BS 25999 certification, 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](http://www.certifiedinfosec.com).

## 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. BS 25999-2 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 BS 25999 BCMS.

The CICRA credential by Certified Information Security certifies your understanding of ISO/IEC 27005, and how the 27005 framework can be used to develop a custom risk management methodology that fulfills the requirements of both ISO/IEC 27001, and BS 25999-2. 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 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 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.

## 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 BS 25999?

BS 25999 is a new visionary international standard 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?

BS 25999-2 is an auditable standard, which means that through certification by an accredited British Standard 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 BS 25999-2, 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?

BS 25999 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. Per BS 25999, Part 1, "Scope and Applicability":

*This Standard is intended for use by anyone with responsibility for business operations or the provision of services, from top management through all levels of the organization; from those with a single site to those with a global presence; from sole traders and small-to-medium enterprises (SMEs) to organizations employing thousands of people. It is therefore applicable to anybody who holds responsibility for any operation, and thus the continuity of that operation.*

## 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 obsolete by BS 25999.

Neither DRI nor BCI certify business continuity management systems for organizations. BS 25999 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 BS 25999 represents a light-year leap ahead in terms of effectiveness, cost-efficiency, and business strategy maturity.

## Benefits from adopting BS 25999 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

Just released in 2009, this new BCM training series offered by Certified Information Security has been completely re-authored from the ground up to map precisely to BS 25999, parts 1 and 2. We have even empowered this new training further by injecting advanced risk management content from recently released risk assessment framework ISO/IEC Standard 27005:2008, and additional security concepts from ISO/IEC 27001:2005 where appropriate.



### **First Session: Stage 1 - Establishing and Governing a BS 25999 Business Continuity Management System (3 Days)**

BS 25999 advocates applying the same Plan-Do-Check-Act management methodology found in many other BSI, ISO, and IEC standards. Accordingly, this stage 1 course addresses BCMS Life Cycle key concepts required for BCMS planning. This course naturally serves as a prerequisite for attendance of "Stage 2 - Using BS 25999 Best Practices to Develop, Exercise, and Certify Business Continuity and Disaster Recovery Processes".



### **Second Session: Stage 2 - Using BS 25999 Best Practices to Develop, Exercise, and Certify Business Continuity and Disaster Recovery Processes (2 Days)**

This stage 2 course addresses BCMS Life Cycle key concepts required for BCMS "Doing, Checking, and Acting". Prior attendance of "Stage 1 - Establishing and Governing a BS 25999 Business Continuity Management System" is a prerequisite for attending this course.

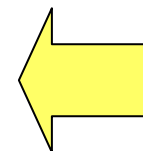
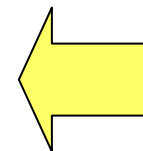
### **Establishing a Business Continuity Management System:**

- 3-Day Seminar
- Recommended Pre-Requisite Training: **None**
- CPE Credit Hours: **24**

### **Using BS 25999 Best Practices to Develop, Exercise, and Certify a BCMS:**

- 2-Day Seminar
- Recommended Pre-Requisite Training: **Establishing a Business Continuity Management System**
- CPE Credit Hours: **16**

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



## Prepare to be certified.

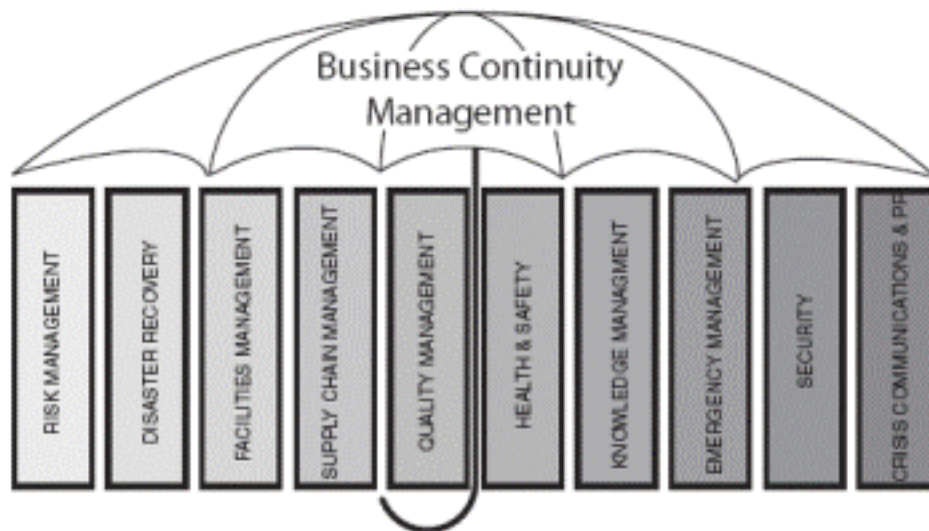
Attendance of these courses is required to be eligible to take CIS certification exams RM101, BCMS101, and/or BCMS102 for CIS risk analyst and/or business continuity management certification. See [www.certifiedinfosec.com](http://www.certifiedinfosec.com) for complete details.

## Who should attend

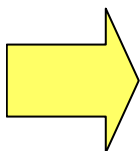
Training requirements for management personnel are specified in BS 25999:

- **Part 1, “Scope and Applicability”:** This Standard is intended for use by anyone with responsibility for business operations or the provision of services, from top management through all levels of the organization; from those with a single site to those with a global presence; from sole traders and small-to-medium enterprises (SMEs) to organizations employing thousands of people. It is therefore applicable to anybody who holds responsibility for any operation, and thus the continuity of that operation.
- **Part 1, Clause 3.2: “BCM and Organization Strategy”:** All organizations, whether large or small, have aims and objectives, such as to grow, to provide services and to acquire other businesses. These aims and objectives are generally met via strategic plans to achieve an organization’s short, medium and long term goals. BCM understanding at an organization’s highest level will ensure that these aims and objectives are not compromised by unexpected disruptions.
- **Part 1, Clause 5 “BCM Programme Management”:** ...The participation of top management is key to ensuring that the BCM process is correctly introduced, adequately supported and established as part of the organization’s culture.
- **Part 1, Clause 10.3 “Skills Training”:** The organization should have a process for identifying and delivering the BCM training requirements of relevant participants and evaluating the effectiveness of its delivery. The organization should undertake training of BCM staff for tasks such as: BCM program management,
  - conducting a business impact analysis,
  - developing and implementing BCPs,
  - running a BCP exercise program,
  - risk and threat assessment,
  - media communications; and
  - Non-BCM staff requiring skills to undertake their nominated roles in incident response or business recovery.

Accordingly, the following key operations and risk management are recommended to attend since each is required to participate in the Business Continuity Management System:



- 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 BS 25999 into an organization



## **Business Continuity Management System (British Standard 25999 conformant)**

### **STAGE 2 – DO-CHECK-ACT**

#### *Using BS 25999 Best Practices to Develop, Exercise, and Certify Business Continuity and Disaster Recovery Processes*

- 4) **Developing and Implementing a BCM Response**
  - a) Developing, coordinating, evaluating and creating plans and procedures to communicate with internal stakeholders during incidents.
  - b) The provision of post-incident support and guidance for employees and their families.
  - c) Developing and implementing emergency response procedures for responding to and stabilizing the situation following an incident or event.
  - d) Establishing and managing an Emergency Operations Centre to be used as a command centre during the emergency.
  - e) Practical experience in handling incidents/emergencies.
  - f) Develop Incident response procedures to fulfill BCM objectives. Designing, developing and implementing business continuity and incident management plans that provide continuity within recovery time and/or recovery point objectives.
- 5) **Exercising, Maintenance and Review**
  - a) Pre-planning and coordinating plan walkthroughs/exercises.
  - b) Evaluating, updating, improving and documenting the results of exercises.
  - c) Developing processes to maintain the currency of continuity capabilities, business continuity and incident management plans in accordance with the organization's strategic direction.
  - d) Establishing appropriate policies and procedures for coordinating incidents, continuity and restoration activities with external agencies whilst ensuring compliance with applicable statutes and/or regulations.
  - e) Practical experience in dealing with external agencies.
- 6) **Embedding Business Continuity Management within the Organization's Culture**
  - a) Preparing a program to create and maintain corporate awareness and enhance the skills required to develop and implement the business continuity management program or process and its supporting activities.
- 7) **Certifying Your Organization's Business Continuity Management System to BS25999-2**
  - a) The certification process
  - b) Preparing for the certification audit
  - c) Case Studies

### **STAGE 1 – PLAN**

#### ***Establishing and Governing a BS 25999 Business Continuity Management System***

- 1) **BCM Policy and Program Management**
  - a) Establishing the need for a Business Continuity Management (BCM) Process, including: resilience strategies, recovery objectives, business continuity and incident management plans, obtaining management support for such a process.
  - b) Organizing and managing the formulation of the function or process either in collaboration with, or as a key component of an integrated risk management initiative.
    - i) Roles and Responsibilities; team development
  - c) Developing, coordinating, evaluating and creating plans and procedures to communicate with external stakeholders, including the media, during incidents.
- 2) **Understanding the Organization**
  - a) Business Impact Analysis:  
Identifying the impacts resulting from disruptions and disaster scenarios that can affect the organization and developing techniques that can be used to quantify and qualify such impacts.  
Establishing critical functions, their recovery priorities and inter-dependencies so that recovery time objectives can be set.
  - b) Risk evaluation and control:
    - i) Determining the events and environmental surroundings that can adversely affect the organization and its facilities with disruption and/or disaster and understanding the damage such events can cause.
    - ii) Establishing the controls needed to prevent or minimize the effects of potential loss.
    - iii) Providing cost-benefit analysis to justify investment in controls to mitigate risks.
    - iv) Using ISO 27005 and other risk assessment frameworks to support Business Impact Analysis
- 3) **Determining Business Continuity Management Strategies**
  - a) 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.
  - b) Delivering solutions for continuation of business within the recovery time and/or recovery point objectives, whilst maintaining the organization's critical functions.

## 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](http://www.certifiedinfosec.com).

### Certified Internal Controls Risk Analyst™

**CERTIFIED  
INTERNAL CONTROLS**  
**Risk Analyst™**  
27005

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.

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 BS 25999 BCMS. The CICRA credential by Certified Information Security certifies your understanding of ISO/IEC 27005, and how the 27005 framework can be used to develop a custom risk management methodology that fulfills the requirements of both ISO/IEC 27001, and BS 25999-2. 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 27005 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.

## Enterprise risk management (ERM)

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 as 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 27005:2011 provides guidelines for information security and operational risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2011. ISO/IEC 27005:2011 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security. As an internationally accepted best practice guideline for developing a solid risk management methodology that is fit-for-purpose for the organization, ISO 27005 can also ensure fulfillment of BS 25999'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 27005 Standard.

## What else you will learn in this two-day seminar

- Learn how to prepare the organization to properly manage operational risks
- Compare and contrast ISO 27005, ISO 31000, and COSO risk management approaches
- Establish risk context criteria for risk evaluation, business impact, and risk acceptance
- Learn how to properly scope your risk management program
- Establish formal roles and responsibilities to manage operational risk throughout the enterprise.
- Learn how to perform professional risk assessment by properly identifying risks, assets, threats, existing controls, vulnerabilities, existing controls, and consequences
- Create a "fit-for-purpose" risk analysis methodology that is custom-suited to your organization
- Learn how to use incident consequence and likelihood to define composite risk levels
- Learn to evaluate assessed risks
- Learn how to properly combine risk treatment alternatives
- Establish your organization's risk treatment plan acceptance process
- Learn how to embed risk management throughout the enterprise using proper risk communication and consultation
- Establish your organization's requirements for ongoing risk monitoring and review

## Who should attend

- Information security managers
- Chief Information Officer (CIO / CISO)
- Compliance officer
- Revenue protection manager
- IT managers; IT administrators
- Risk managers
- Facilities managers
- Department heads
- IT/Systems auditors

## Prepare to be certified.

Attendance of this course is required to be eligible to take CIS certification exam RM101 for the CIS Certified Internal Controls Risk Analyst certification. See [www.certifiedinfosec.com](http://www.certifiedinfosec.com) for complete details.

2-Day Seminar

Recommended Pre-Requisite Training: **None**

CPE Credit Hours: **16**

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



## Where does your organization stand in governing information security risk management, controls strategy, and compliance fulfillment?

### The problem.

Many organizations have the misunderstanding that “information security” is the same thing as “IT security”. Managing and controlling access to information throughout the organization - whether electronic or hard copy - is now a concern throughout the entire organization. Today, the concern for controlling information confidentiality, integrity, and availability even transcends beyond the organization’s boundaries to how information is regulated, how it is used and protected by vendors, and how the expectations of our customers and trading partners affect our current information management processes. In short, managing information security has become much, much more than keeping hackers out of an IT network. It has become a corporate governance issue that requires professional management and oversight according to international standards.

### The solution.

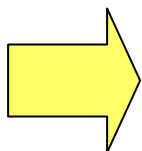
Your organization needs to migrate from IT-centric information security management that is rife with a lack of proper segregation of duties, to a fully mature program that is planned, deployed, monitored, and continually improved according to a set of internationally recognized standards. Better yet, your organization can then move forward to have its information security management system certified by the International Organization for Standardization, or ISO.

### How we can help.

Exploring the use of ISO/IEC standards 27001, 27002, and 27003 this course provides critical information for understanding the business drivers for information security, as well as the core concepts for planning and implementing information security according to the internationally accepted best practices.

### What else you will learn in this two-day seminar

- Developing an Information Security Management System program
- Project managing a successful ISO 27001 internal controls implementation
- Core ISO 27001/27002/27003 best practices relating to:
  - Information security policy and scope
  - Risk assessment and Statement of Applicability
  - External party controls
  - Asset management
  - Human Resources security
  - Physical and environmental security
  - Equipment security
  - Communications and operations management
  - Malicious software controls
  - Network security management and media handling
  - Monitoring of information security and incident management
  - Business continuity management
  - Compliance Exchange of information
  - Electronic commerce, e-mail and internet security
  - General, network, operating system, and application access control
  - Systems acquisition, development and maintenance
  - Cryptographic controls
  - Development and support process security
  - Monitoring of information security and incident management
  - Business continuity management
  - Compliance
- Preparing for an ISO/IEC 27001 audit
- **You and your team will be performing 12 in-class gap assessments**, resulting in your own custom executive summary gap assessment for your enterprise-wide information security program that clearly indicates what is most critical to initiate or improve your program, and how to best move forward in doing it throughout all departments in the organization.



### Who should attend

- Information security managers
- Chief Information Officer (CIO / CISO)
- Compliance officer
- Revenue protection manager
- IT managers; IT administrators
- Risk managers
- Facilities managers
- Department heads
- IT/Systems auditors

### Prepare to be certified.

Attendance of this course is required to be eligible to take CIS certification exams ISMS101 and ISMS102 for the CIS Certified Internal Controls Architect information security management certification. See [www.certifiedinfosec.com](http://www.certifiedinfosec.com) for complete details.



2-Day Seminar

Recommended Pre-Requisite Training:  
*Using ISO 27005 to Develop and Deploy Enterprise Risk Management*

CPE Credit Hours: 16

For currently scheduled seminars please see [www.certifiedinfosec.com](http://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

#### 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

#### 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

### Who should attend

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

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