

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).

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.



Allen Keele, President & CEO



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)
Rometelcom
United States Department of Defense National Security Agency
Raytheon
Royal Caribbean
Towers Perrin
United States Marine Corps
United States Department of Treasury

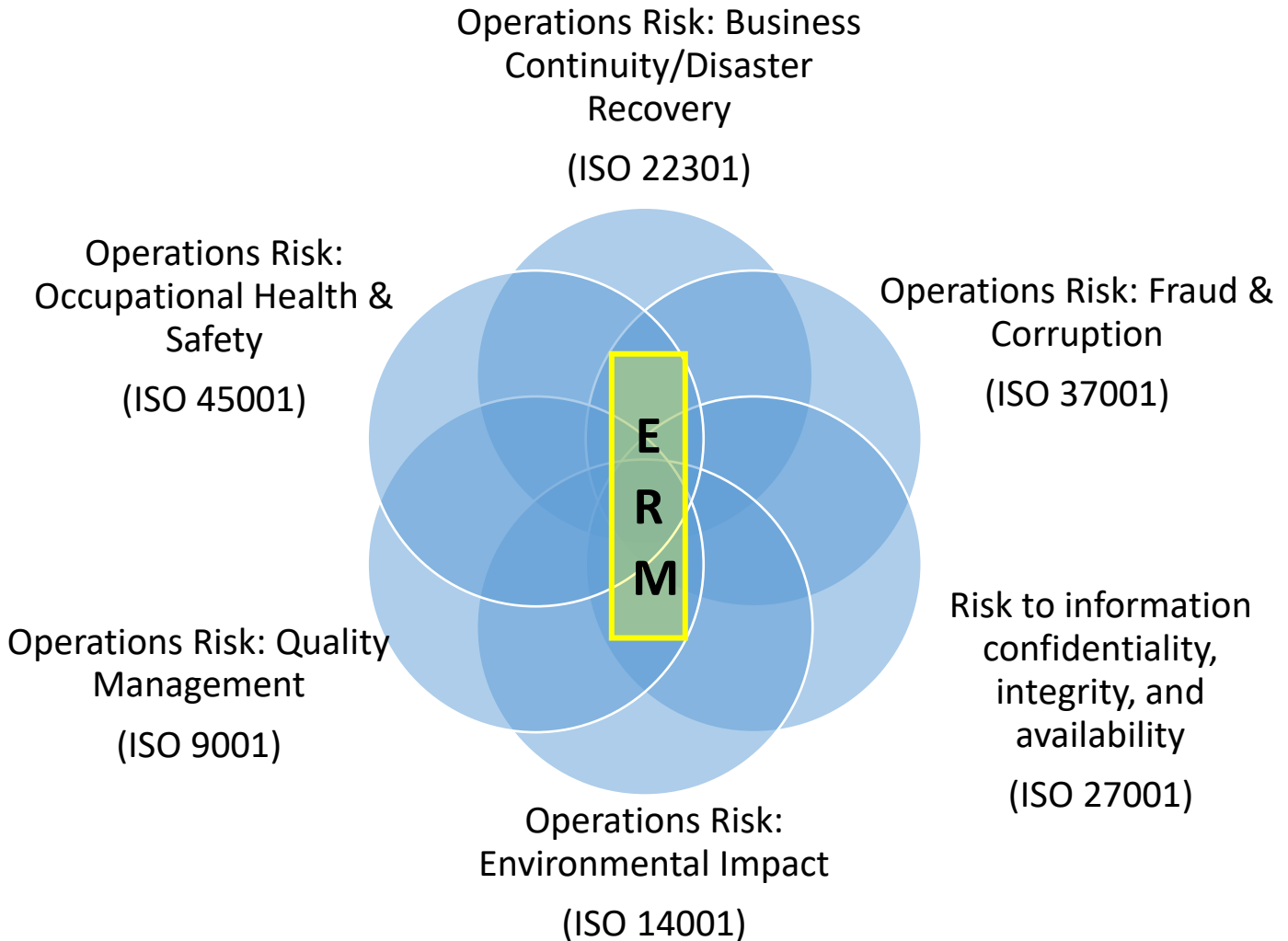
Our Caribbean customers include:



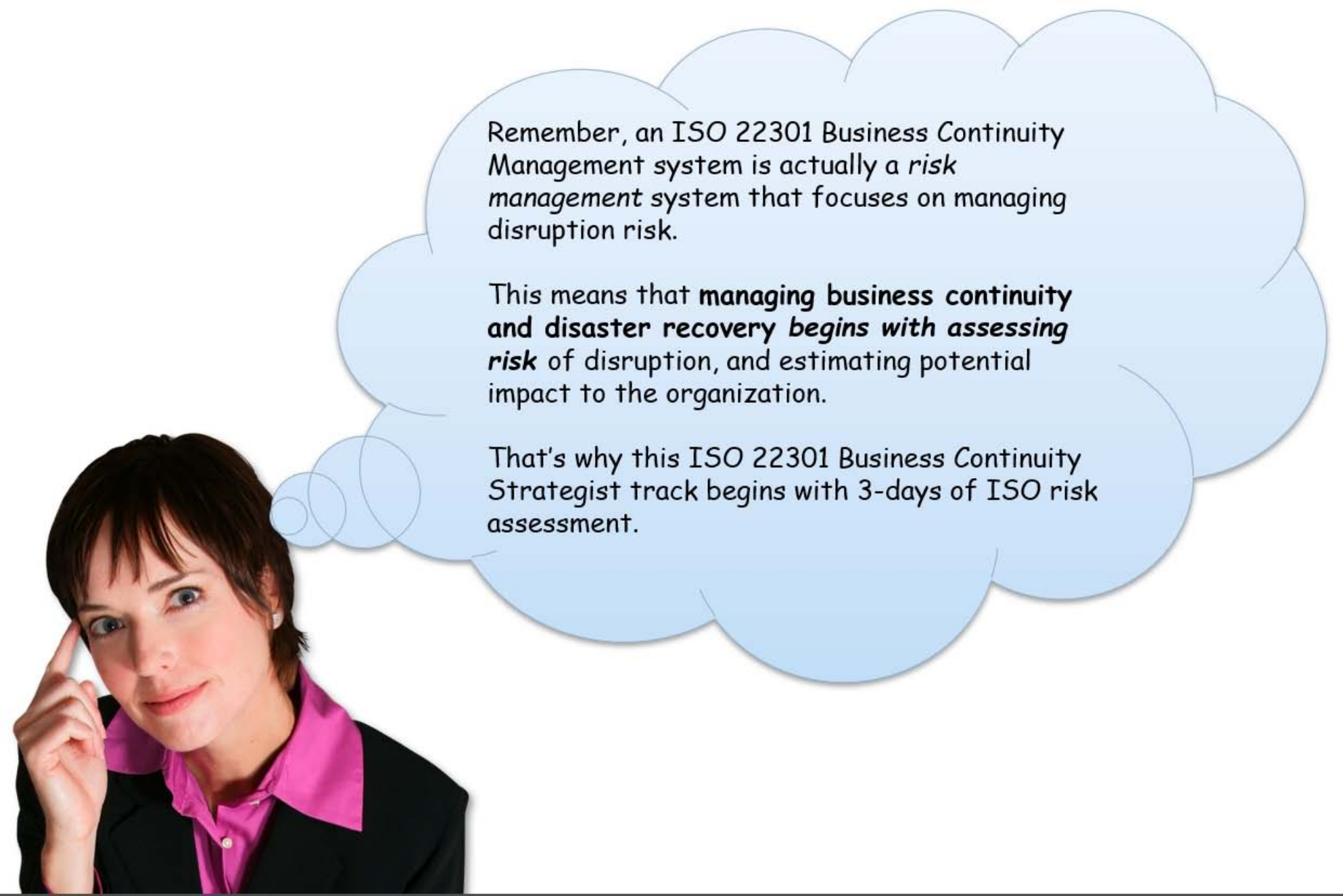
Angostura Distillers Ltd.
Anguilla Government
Aqualectra
Aruba Ministry of Finance
Atlantic LNG
Bahamas Development Bank
Bank of Jamaica
Barbados Department of Treasury
Barbados Light & Power Company
Republic Bank Barbados (Former BNB)
Barbados National Insurance Office
British Gas Group Trinidad
British Petroleum Trinidad
Butterfield Bank Limited
Cable & Wireless Caribbean Region
Cayman Islands Government
Cayman National Bank
Central Bank of Aruba
Central Bank of Barbados
Central Bank of Curaçao and Sint Maarten
Central Bank of Trinidad & Tobago
Civil Aviation Authority of Jamaica
Deloitte & Touche
Digicel
Eastern Caribbean Central Bank (ECCB)
Eastern Caribbean Financial Holding Co.
EOG Resources Limited
Ernst & Young
eTeck
Fidelity Bank
First Caribbean International Bank
First Citizen's Bank
GraceKennedy Ltd.
Jamaica Cooperative Credit Union League
Jamaica Deposit Insurance Corporation
Jamaica Ministry of Finance
Jamaica Financial Services Commission
Jamaica Ministry of Commerce and Tech.
Jamaica Ministry of Industry
Jamaica National Building Society
KPMG
Methanol Holding Company
Montserrat Ministry of Finance
National Bank of Anguilla Ltd.
National Bank of Barbados
National Bank of Dominica
National Commercial Bank (NCB)
National Gas Company of T&T
ORCO Bank
Office of Utilities Regulation (Jamaica)
PCS Nitrogen
Petrojam Limited
PLIPDECO
PowerGen of Trinidad & Tobago
PriceWaterhouseCoopers
Royal Bank of Canada (RBC)
Republic Bank
Royal Bank of Canada
Royal Montserrat Police Force
Sagicor
Scotia Bank
Sandy Lane Resort
St. Lucia Electric Company
St. Lucia Ministry of Finance & EA
St. Vincent Electricity Services, LTD.
Telem St. Maarten
Trinidad & Tobago Unit Trust
T&T Ministry of Public Administration
TSTT
United Telecommunication Services (UTS)
WASA
Wray & Nephew Distillers (Campari Group)

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

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



Enterprise Risk Management (ERM) guides and informs all other risk managing specialties, or silo’s, on how risk is to be uniformly measured, and to which tolerances (risk tolerance or risk appetite). ERM is essentially the core risk assessment, management, and communication framework at the heart of the organization’s other risk managing specialties including ISO 9001 quality management, ISO 22301 Business Continuity Management, ISO 14001 Environmental Management, ISO 45001 OHS, and even ISO 37001 anti-bribery & anti-corruption. As such, the Enterprise Risk Management framework, or program, should be designed and deployed prior to forming other risk managing specialties – *not after*.



Remember, an ISO 22301 Business Continuity Management system is actually a *risk management* system that focuses on managing disruption risk.

This means that **managing business continuity and disaster recovery begins with assessing risk** of disruption, and estimating potential impact to the organization.

That's why this ISO 22301 Business Continuity Strategist track begins with 3-days of ISO risk assessment.

CIS POLICY WORKSHOP SERIES: ISO 31000 ENTERPRISE RISK MANAGEMENT

3-Day Seminar

No pre-requisite training required.

CPE Credit Hours: 24

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

This course can be arranged as a private on-site training session at up to a 40% discount from public session fees.

*Copies of ISO standards are NOT included in this course, nor provided in class.

Learn Enterprise Risk Management, and how to leverage the ISO 31000 standard to establish and maintain an ERM program, and build-out the initial ISO 31000-conforming risk program policy right in class!

Why Enterprise Risk Management?

Risk management is an increasingly important business driver and stakeholders have become much more concerned about risk. Risk may be a driver of strategic decisions, it may be a cause of uncertainty in the organization or it may simply be embedded in the activities of the organization. An enterprise-wide approach to risk management enables an organization to consider the potential impact of all types of risks on all processes, activities, stakeholders, products and services. Implementing a comprehensive approach will result in an organization benefiting from what is often referred to as the "upside of risk".

A successful enterprise risk management (ERM) initiative can affect the likelihood and consequences of risks materializing, as well as deliver benefits related to better informed strategic decisions, successful delivery of change and increased operational efficiency. Other benefits include reduced cost of capital, more accurate financial reporting, competitive advantage, improved perception of the organization, better marketplace presence and, in the case of public service organizations, enhanced political and community support.

And since information security, business continuity/disaster recovery, environmental health and safety, and other critical management systems have the primary purpose of identifying and treating risk, it is essential that your organization establish a common platform and approach for managing risk.

What you and your colleagues will achieve

This 3-day training and workshop session provides a thorough overview on ISO 31000, as well as setting out advice on the implementation of an ERM initiative. This course:

- Describes the principles and processes of risk management;
- Provides a thorough overview of the requirements of ISO 31000 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

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 ISO 22301 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 obsolete 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.

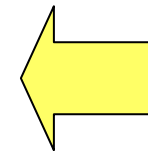
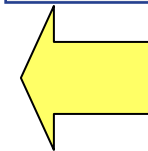
Policy Workshop: ISO 22301 Business Continuity Management:

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

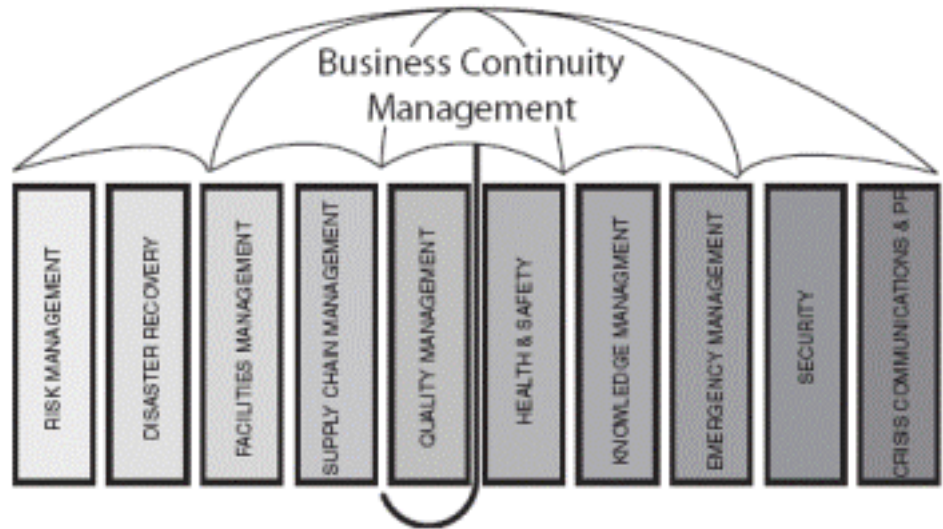
Best Practices to Develop, Exercise, and Certify a BCMS:

- 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



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

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



Certified ISO 22301 CBCS Training and Certification Workshop

CIS Policy Workshops: ISO 31000 Risk
+ CIS Policy Workshop: ISO 22301
Business Continuity Management
(5-Days)



CERTIFIED
Information Security[™]

Module I. Introduction

- A. Introduction to Enterprise Risk Management Concepts
 - 1. Overview of Enterprise Risk Management
 - 2. How does “Enterprise” Risk Management differ from “Risk Management”?
- B. Risk management drives business continuity management, information security, quality management, environmental health and safety, and even occupational health and safety
 - 1. Business drivers for risk management: Regulatory and other external requirements
 - a) [ISO 9001](#) Quality Management Systems
 - b) [ISO 14001](#) Environmental Management Systems
 - c) [ISO 27001](#) Information Security Management Systems
 - d) [ISO 22301](#) Business Continuity Management Systems
 - e) [ISO 45001](#) Occupational Health & Safety
 - f) [Sarbanes-Oxley Act](#)
 - 2. Leveraging ISO standards 31000, 31010, and 27005 to establish consistent, formal, and documented approach for risk management
- C. Risk Architecture & Strategy drives other Management Systems’ Architecture & Strategy
 - 1. Leadership (Mandate and Commitment) Requirements
 - 2. Typical senior leadership responsibilities
 - a) Risk Officer and the Risk Committee
 - b) Senior Executive Leadership
 - c) Top-Down Risk Management
 - d) Getting senior management buy-in and commitment
 - 3. How Enterprise Risk Management leadership transcends to automatically fulfil leadership requirements for Quality Management, Environmental Management, Information Security Management, Business Continuity Management, and Occupational Health and Safety
- D. Using the organization’s business context to develop fit-for-purpose Enterprise Risk Management, Quality Management, Environmental Management, Information Security Management, Business Continuity Management, and Occupational Health and Safety
 - 1. Corporate Governance
 - 2. ISO Requirements for “Context”

- a) ISO 9001:2015 Quality Management
 - b) ISO 27001:2014 Information Security Management
 - c) ISO 22301:2019 Business Continuity Management
 - d) ISO 14001:2015 Environmental Management
 - e) ISO 45001:2018 Occupational Health and Safety Management
3. Managing internal and external stakeholder input and collaboration
 - a) Procedure for Identification of ERM Project Requirements document (4-Page template provided)
 - b) Procedure for Identification of Statutory, Regulatory, and Contractual Requirements document (1-Page template provided)
- E. Governance and Management Roles & Responsibilities
1. Possible Organizational Structure for Establishing ERM
- F. How to Get Started in Establishing ERM

Module II. Risk Architecture and Strategy

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

G. Establishing the risk management policy

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

H. Enterprise risk management roles and responsibilities

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

I. Integration into organizational processes

J. Resource allocation

K. Communication and consultation program requirements

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

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

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

B. Risk Assessment

1. Risk Identification

a) Assets

b) Vulnerabilities

c) Threats

d) Controls

e) Consequence

2. Risk Analysis

a) Risk analysis techniques (procedures)

3. Risk Evaluation

Module IV. Risk Treatment

A. Calculating residual risk

B. Risk treatment alternatives

C. Risk treatment constraints

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

A. Risk Treatment Certification and Accreditation

B. Risk review (Risk communication and consultation)

C. Risk monitoring and review

Module VI. Using CIS' ISO 31000 Policy Document Toolkit

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

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

I. Introduction to Professional Business Continuity Management

A. What is business continuity management?

B. Relationship of BCM to Risk Management

C. Business Drivers

D. Benefits of BCM

E. Benefits of using ISO 22301 for BCM

F. ISO 22301 Methodologies Overview

1. Management systems approach with PDCA

2. The BCM life cycle

a) BCM program management

b) Understanding the organization

c) Determining business continuity strategy

d) Developing and implementing a BCM response

e) BCM exercising, maintaining and reviewing BCM arrangements

f) Embedding BCM in the organization's culture

G. Certifying the organization to ISO 22301 BCM

II. BCM Program and Policy Management

A. ISO 22301 BCM program requirements

1. Strategy requirements

2. Leadership requirements

3. Communication requirements

4. Roles and responsibilities

a) Organizational structure

b) Business Continuity Manager

- c) Disaster recovery teams
- d) Ongoing maintenance

B. Business Continuity Management System Policy

1. Policy development tutorial
 - a) Complete ISO 22301-conforming BCM Policy (29-Page template provided)
2. Scoping the BCM program
3. Resourcing the BCM program
4. Training and competency requirements
 - a) Program management
 - b) Policy and strategic development
 - c) Planning and document development
 - d) Document approval
 - e) Business impact analysis
 - f) Planning and incident response
 - g) BCM exercising and auditing
 - h) Media relations
 - i) Procedure for Training and Development Needs Analysis document (8-Page template provided)
5. Documentation requirements
6. BCM Program project kick-off document (9-Page template provided)
7. Procedure document for identification of statutory, regulatory, contractual, and other requirements (1-Page)

C. Establishing the business continuity strategic objectives

D. BCM Program project kick-off document (9-Page template provided)

III. Understanding the Organization and its Context

A. Introduction

1. Identifying the organization's objectives, stakeholder obligations, statutory duties and the environment in which the organization operates;
2. Identifying the activities, assets and resources, including those outside the organization, that support the delivery of these products and services;
 - a) Process mapping
3. Assessing the impact and consequences over time of the failure of these activities, assets and resources
4. Identifying and evaluating the perceived threats that could disrupt the organization's key products and services and the critical activities, assets and resources that support them

B. Requirements for business impact analysis (BIA)

IV. Developing Business Continuity Strategic Objectives

A. ISO 22301 requirements for BCM strategy

B. Aligning BCM strategy to organizational strategy

C. Establishing desired BCM outcomes and deliverables

1. Recovery time objectives
2. Recovery point objectives
3. Minimum Business Continuity Objective
4. Maximum Tolerable Period of Disruption
5. Using KPI's

D. Estimating continuity requirements for

1. People
2. Premises
3. Technology
4. Information

5. Supplies
6. Stakeholders
7. Civil emergencies

V. Planning for Embedding BCM into the Organization's Culture, Auditing, and Monitoring

A. Integrating BCM into business strategy, risk assessment, and processes

B. Raising BCM awareness

C. Maintaining the BCM program

D. Auditing the BCM program

1. Initial BCM program assessment class lab

E. Management review of the BCM program

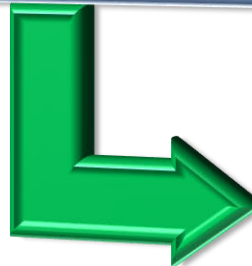
ISO 22301 Business Continuity Management Certification Path



- Start by completing your core risk assessment training and CICRA certification exam, #RM101



- Then complete your ISO 22301 business continuity strategy and policy training and CBCS Exam, #BCMS101



- Then complete your ISO 22301 business continuity deployment, exercising, and certification training and CBCM exam, #BCMS102

Certification Application and Endorsement Kit

ISO/IEC standards 31000, 31004, 31010, and 27005 provide guidelines for enterprise risk, information security risk, and business continuity risk management. These standards support the risk assessment and business impact assessment requirements of ISO/IEC 27001, and are designed to assist the satisfactory implementation of information security based on a risk management approach. These ISO standards are 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, these ISO standards can also ensure fulfilment of ISO 22301's requirements for such a risk management capability.

The CICRA credential by Certified Information Security certifies your understanding of how ISO/IEC standards 31000, 31004, 31010, and 27005 can be used to develop a custom risk management methodology that fulfils the requirements of ISO/IEC 9001:2015, 14001:2015, 27001, ISO 22301. It also helps fulfil the competence requirements of the certifications themselves. Upon completion of this training and certificate program, you will:

- be equipped with knowledge and skills required to develop, manage, monitor, and improve an Enterprise Risk Management System in line with the ISO 31000 standard of best practice;
- expand your risk management competency;
- increase your credibility through gaining international recognition; and
- improve your résumé and help to increase your earning potential.

Getting certified is easy. The CICRA™ certification is available to qualified candidates who:

1. **Are a member of CIS in good standing.** If you are not already an Associate member of the CIS certification student body, you must first become a member to pursue the CICRA credential. Please see www.certifiedinfosec.com/about/becoming-a-member for further details.
2. **Attend the required CIS approved curriculum courses.** Seminars may be attended at **live instructor-led sessions, online**, or a combination of both.
 - CIS Policy Workshop: *ISO 31000 Enterprise Risk Management*
3. **Pass the CICRA Exams.**
For CICRA certification by CIS, candidates must pass the CIS online exam RM101. CIS exams are administered online and can be taken at your convenience at your home or work through the CIS Learning Center, where your progress and score are monitored and recorded centrally. Your exam results are provided to you automatically upon completion of your exam.

Becoming a Certified ISO 31000 Internal Controls Risk Analyst (CICRA)

Start here.

- Become a CIS member.



Get your training.

- CIS Policy Workshop: ISO 31000 Enterprise Risk Management



Take your exam.

- CICRA Exam #RM101



Submit your endorsements.



Certified!

CERTIFIED
INTERNAL CONTROLS

Risk AnalystTM
ISO 31000

Certification Application and Endorsement Kit

Since Business Continuity Management is more important than ever in today's risk conscious business environment, and because ISO Standard 22301 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 ISO 22301 certification, it needs evidence of appropriate training and competence to fulfil the certification requirements of the standard itself.

CBCS™ Certification

ISO 22301 advocates that the business process of business continuity and disaster recovery management should begin with the development of a clear continuity strategy establishing what the organization needs to accomplish with its BCM program based upon thorough risk analysis and evaluation by the proper risk decision-makers within the organization.

The *Certified Business Continuity Strategist* (CBCS) certification by CIS validates 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:

- determine and guide 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;
- deliver solutions for continuation of business within the recovery time and/or recovery point objectives, whilst maintaining the organization's critical functions;
- develop, coordinate, and evaluate plans and procedures to communicate with internal stakeholders during incidents; and
- provide of post-incident support and guidance for employees and their families.

Upon completion of this training and certificate program, you will also:

- expand your risk management and business continuity competency in line with internationally recognized standards of best practice;
- increase your credibility through gaining international recognition; and
- improve your résumé and help to increase your earning potential.

Becoming a Certified ISO 22301 Business Continuity Strategist

