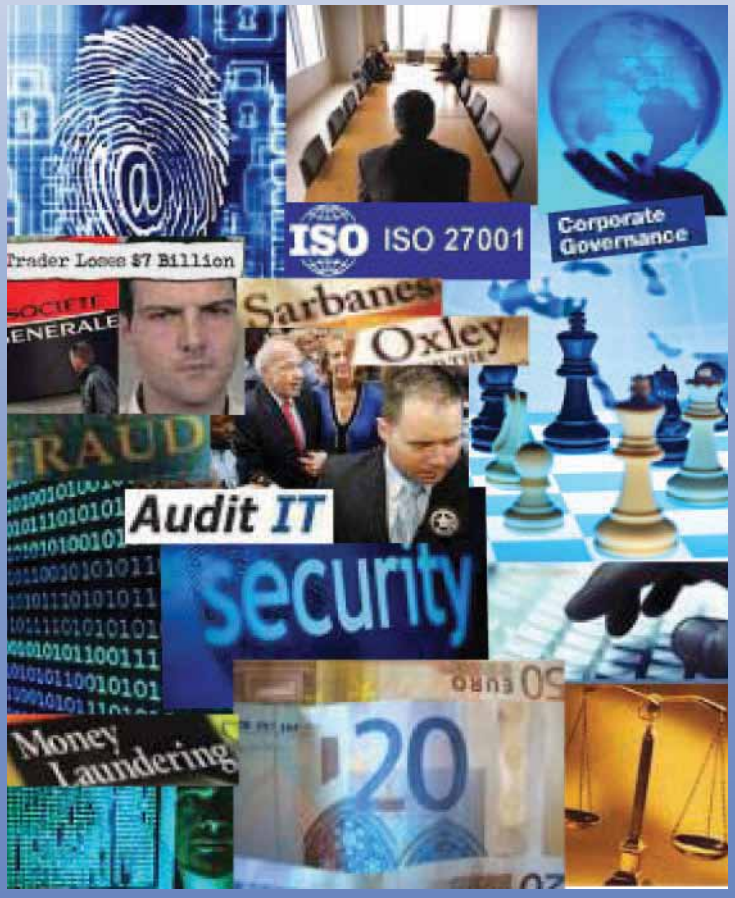
WORLD CLASS CORPORATE GOVERNANCE & COMPLIANCE TRAINING

CERTIFIED Information Security™

2020 SEMINAR CATALOG



- ISO 31000 ENTERPRISE RISK MANAGEMENT
- ISO 45001 OCCUPATIONAL HEALTH & SAFETY MANAGEMENT
- ISO 27001 INFORMATION SECURITY MANAGEMENT
- ISO 22301 BUSINESS CONTINUITY & DISASTER RECOVERY MANAGEMENT
- ISO 37001 ANTI-BRIBERY & ANTI-CORRUPTION MANAGEMENT
- FRAUD PREVENTION, DETECTION, & INVESTIGATION

www.certifiedinfosec.com

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

Our business is training you to improve your business.

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

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

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

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

Allen Keele, President & CEO

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.

CISA CISM CISSP

CERTIFIED INTERNAL CONTROLS Risk Analyst ISO 31000

CERTIFIED INTERNAL CONTROLS Architect ISO 27001

CERTIFIED FRAUD CONTROL Manager

CERTIFIED BUSINESS CONTINUITY Manager ISO 22301

© Copyright 2003 -2016 Certified Information Security (Ce – www.certifiedinfosec.com. All rights reserved.

Our customers include:

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

3-Day Seminar

Prior attendance of ISO 31000 or ISO 27005 risk management training is encouraged, but not 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.

CERTIFIED NIST CYBERSECURITY FRAMEWORK LEAD IMPLEMENTER

Get trained as an expert in planning, deploying and managing cybersecurity according to the NIST Cybersecurity Framework

The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States and around the world can assess and improve their ability to prevent, detect, and respond to cyber attacks. It has been translated to many languages, and is used by the governments of Japan and Israel, among others.

The NIST CSF is now the go-to playbook for countless organizations for building a robust data protection strategy. It's structured along five core functions — Identify, Protect, Detect, Respond and Recover — each of which captures and curates the essential goals and actions that should be prioritized across the cybersecurity lifecycle.

What does NIST CSF deliver for an organization?

The CSF helps make sense of what to do before, during, and after an incident: from shedding light on your data ecosystem and where the vulnerabilities lie; to locking down sensitive data and remediating known risks; to detecting malicious activity and meeting the threat with consistent and repeatable processes; to finally recovering through the quarantine of corrupted data, monitoring of ongoing threat activity, protocol adjustment and related steps.

The beauty is that all this guidance and wisdom comes in the form of a few strategic guidelines that are intuitive and accessible to a wide range of practitioners. Of course, not everything about NIST is voluntary for all organizations (U.S. government contractors, for example, must demonstrate security compliance under NIST 800-171 or risk losing their contracts), and regulations are always changing. That's why the CSF is still the roadmap to drive your organization toward the most secure data and architectures possible.

Become a NIST CSF Lead Implementer

CERTIFIED Lead Implementer™ NIST CSF

The Certified NIST CSF LI certification certifies your ability to implement the formal structure, governance, and policy of a robust cybersecurity framework following internationally recognized and respected NIST best practices and standards. Get trained and certified as an expert in devel loping, implementing, and managing a robust cybersecurity program according to internationally adopted NIST CSF governance and management best practices.

Upon completion of this training and certificate program, participants will:

- Be equipped with knowledge and skills required to manage, monitor, and improve NIST Cybersecurity Framework policy and program in line with the NIST CSF 1.1 and related standards of best practice;
- Expand your cybersecurity competency;
- Be prepared to integrate a robust NIST Cybersecurity program into an ISO 27001 Information Security Management System (ISMS); and
- Increase your credibility through gaining international recognition.

Course Content Details

1. **Framework Core Functions**
   - Identify
   - Protect
   - Detect
   - Respond
   - Recover
2. **Framework Implementation Tiers (Cyber Security Risk Management)**
3. **Framework Profiles**
4. **Converging the CSF Framework into an ISO 27001 Information Security Management System**
5. **Establishing the CSF Framework Policy documents (soft-copy template included)**

Establish a firm program starting point by NISTS's CSF 1.1 to build out the initial cybersecurity component of an overall Information Security Policy core policy. Throughout the class, our expert instructor will convert NIST CSF concepts and requirements into a real NIST CSF-conforming cybersecurity policy.

Who should attend

- Policy Approvers / Strategy Decision Makers
- Chief Information Officer (CIO / CISO)
- Information security / cybersecurity professionals
- IT Managers
- Risk managers
- Business continuity managers
- Facilities managers
- Operations department heads (business unit managers)
- Auditors