



# Risk Management:

## The Core of Security Governance with ISO 27001

### TRAINING COURSE

The objective of this course is to provide attendees with the necessary skills to understand how to manage security risk in your corporate environment by using a solid framework and sound methodology based on ISO 27001 principles. Learn how to integrate people, processes and technology to provide a practical education on best practices for Information Security Management, IT Governance and other best practice models. Find out how to blend management, operations, and technology into the 27001 framework to align information security with the overall business objectives.

Gain knowledge of the methodology around 27001 compliance to address how you can manage regulatory compliance and best practices around security risk that face organizations daily. The methodology covers the keys to Building a Security Infrastructure, Proactive Planning (People, Process & Technology), insight in the certification process and continuous maintenance to monitor your plans. Address how management can use the tools to provide an overall approach to managing security risks in order to meet the business objectives. Get insight into the certification process for implementing a security program to ensure management is providing the proper due care and due diligence. Discover the framework of ISO 27001 & 27002, and how it works with CoBit, ITIL, PMBOK, Privacy, Security Techniques, and regulatory compliance. The course includes presentation of information plus practical exercises and workshop activities that enable participants to “learn by doing.” This will provide a valuable resource for participants when they return to the workplace.

#### Who should attend?

- Top Management representatives
- Security Professionals
- Risk Managers
- Staff responsible for compliance with laws and regulations
- Auditors (External and Internal)
- Information Security Officers
- IT Managers/Directors
- Privacy/Compliance Officers
- Legal counsel
- Human Resource Managers and staff involved

#### Benefits to Your Business

- Learn how to adopt Risk Management practices into your organization
- Take the knowledge and skills imparted during the training to increase and improve confidentiality, integrity and availability of information systems
- Improve customer and investor confidence
- Show due diligence and due care

Training by:





# Risk Management:

## The Core of Security Governance with ISO 27001

### TRAINING COURSE

#### Course Content -

The course is designed for people who have a reasonable awareness of Information Security Management.

#### Day 1

- **Global threats and vulnerabilities for networked organizations**
- **Identifying threats, vulnerabilities and impacts**
- **Why 27001 compliance?**
- **Business objective for security**
- **How to identify of information assets and information asset ownership**
  - Management, Operational & Technical
- **Security Baseline Metric**
- **Understanding the Technical & Non-Technical assessment**
- **Regulatory Compliance and Implications for Information Security with other standards**
  - Sarbanes Oxley
  - PCI Standard
  - HIPAA Compliance
  - GLBA Compliance
  - FFIEC
  - FISMA
  - Privacy Regulations
  - ITIL/ISO 20000
  - CoBit/COSO

#### Day 2

- **Risk Management analysis**
  - Commitment & Resources
  - Management, Operational , and Technical
  - Internal structure (audit)
  - Managements Review input/output
  - Improvement – Corrective/Preventative
- **General Requirements of PDCA**
  - Establishing the system with the ISMS

Training by:



- Implement and operating
- Monitor and Review with PDCA
  - Developing a Metrics & Measurement
- Documentation Requirements for the ISMS process
- Certification process of ISMS

### **Day 3**

- **Preparing for an ISO/IEC 27001 Audit**
  - Overview of the process
  - Parties involved
  - Certification
  - Post Certification requirements
  - Audit and Audit trails
    - Stage 1 and Stage 2
  - Surveillance
- **Risk Management project (Hands-on)** – Case Study and implementation

Training by:



## Duane Hopkins MLS, HISP, CIPP, IAM, IEM, CCE, CEH

Duane Hopkins is a Security subject matter expert in the area of Information Security Governance, Electronic Discovery, and Computer Forensics. His experience and knowledge has lead him to engage in projects dealing in Risk Assessment/Evaluations, Incidents Response, Computer Forensics, Business Continuity, Physical Security and Policy Development. Duane graduated with a Bachelors degree in Project Management, and holds a Masters Degree in Information Security from Eastern Michigan University, designated by NSA as a National Accredited and a Regional skills of excellence. Duane's education and experience in the Information Security field has lead him to consult and develop a concentration program at Lawrence Technological University. As a Professor he has developed courses in the following areas: High Tech Crime Cybercrime, Incident Response, Risk Management, Cyber Law, Computer Forensics methodology, Applications of Computer Forensics Tools and Corporate Fraud Examination. He has expertise's as a hybrid business information security and technical consultant with a holistic approach to the management of information security and regulatory compliance, as well as a subject matter expert on Information Security governance and compliance relating to regulatory standards. From his holistic approach to security he has experience and knowledge of organizational policies, processes and procedures against internationally accepted information security best practices ISO 27001, 27002, and HIPAA Security, Sarbanes-Oxley Act (Security), GLB Act, California SB-1386, NIST 800-53, FACT Act and PCI Data Security.

Duane is the Founder & Principal Security Consultant of Innovative Corporate Solutions, Inc., a Detroit, Michigan based Risk Management, Electronic Discovery and Computer Forensics Solutions Company founded in 2004. Duane founded Innovative-CSI on the holistic security approach to address the need to examine the big picture of information security. This approach has contributed to his involvement in the security community with speaking engagements and publications. He has established numerous valuable contacts nationwide and has name recognition in the information security, computer forensics, and regulatory compliance space.

He has successfully consulted organizations and the execution of information security projects, development, and implemented Information Security Governance. His knowledge in the commercial sector includes consulting engagements for clients, in the Manufacturing, Financial Services and Healthcare sector. In addition he has developed Corporate training courses in Information Security Governance, Electronic Discovery process, Risk Management – ISO 27001, Regulatory Compliance and Business Continuity. His work at Innovative CSI, branches from the detection work of computer forensics due to a breach of security to proactive consulting with clients on the implementation of risk management planning into their organization. He helps build the needed plans for organizations in Incident Response, Business Continuity and Disaster Recovery, Sarbanes-Oxley, and HIPAA to comply with their overall risk management plan. His creative and out of the box thinking leverages his process as one of the true innovators in the security field.

Training by:

