

Certified Information Security Manager (CISM)

9th - 13th October 2011 Abu Dhabi UAE

Price: USD 2,695 /Per Delegate

Registration is available online log in to www.invention-i.com

5 Days Course outline

Day 1 – CISM Boot Camp Information Security Governance

(Corresponds to Domain 1 of the CISM exam – 23%)

Description

Data is an essential asset of any organization and these assets require continual monitoring and protection. Information Security Governance (ISG) is a subset discipline of Corporate Governance, the focus of which is on information security systems and their performance and overall risk management.

Just having security policies and then simply concentrating on securing your network, is impractical and incomplete. To fully vest security within business processes, all organizations must have a robust information security strategy and mechanism that map to its business drivers, legal and regulatory requirements, as well as its threat profile.

Information security governance is therefore, all of the software, hardware, personnel, infrastructure, and business processes that ensure that security is functionally capable to assist an organization in meeting its strategic objectives. ISG, is simply how technology coupled with security are used and managed so that business needs and goals are supported.

This course provides an overview into the specific criteria, steps and actions necessary to implement and sustain a quality Information Security Governance program.

Learning Objectives: After completing this session, the participant will be able to:

1. Gain further knowledge and understanding about the essential components of a viable information security governance program.
2. Identify the essential differences between corporate governance and IT governance, when and how to apply each.
3. Understand how to build a business case for a comprehensive Information Security Governance (ISG) program
4. Assess specific regulatory requirements and their potential business impact from an information security standpoint
5. Evaluate third party relationships and their impact on information
6. Define the roles, responsibilities and general organizational structure of a comprehensive Information Security Governance (ISG) program

Session Outline

- Components of an information security strategy
- Concepts of corporation and information security governance
- Budgetary planning strategies and reporting methods
- Developing the business case for a comprehensive Information Security Governance (ISG) program
- Regulatory requirements and their potential business impact from an information security standpoint (HIPAA, GLB, SoX, Basel II, etc.).
- Liability management strategies and insurance options (e.g. crime or fidelity insurance, business interruptions)
- Third party relationships and their impact on information (e.g., outsourcing, SLAs, etc.).
- Establishing and operating an information security steering group
- Roles, responsibilities and general organizational structure of a comprehensive Information Security Governance (ISG) program
- Generally accepted international standards for information security management

Summary

- Audience Participation Activities

Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

- Additional Resources To Be Provided (a.k.a. Take-aways)

Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

Day 2 – CISM Boot Camp Information Risk Management

(Corresponds to Domain 2 of the CISM exam – 22%)

Description

In today's global economy, every organization has a mission. In this digital era, as organizations critically depend upon information technology (IT) systems to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT-related risk.

An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence.

Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.

This course provides an overview into the specific criteria, steps and actions necessary to implement and sustain a comprehensive Information Risk Management program.

Learning Objectives: After completing this session, the participant will be able to:

1. Define and implement an information asset and data classification schema
2. Document the relevant components of information ownership schema
3. Identify threats, vulnerabilities and exposures to organizational data assets
4. Explain and utilize risk assessment and analysis methodologies
5. Select specific methods to determine sensitivity and criticality of information resources
6. Assess information security controls and countermeasures and their effectiveness
7. Develop risk mitigation strategies for critical organizational information resources
8. Utilize Gap and Cost-benefit analyses as means to analyze and mitigate risk to a management acceptable level

Session Outline:

1. Establishing an information asset and data classification schema
2. Identification of the relevant components of information ownership schema
3. Information threats, vulnerabilities and exposures
4. Information resource valuation methodologies
5. Risk assessment and analysis methodologies
6. Determining risk reporting frequency and requirements
7. Methods used to determine sensitivity and criticality of information resources (quantitative and qualitative)
8. Baseline modeling and risk-based assessments of control requirements
9. Information security controls and countermeasures and their effectiveness
10. Risk mitigation strategies for information resources
11. Gap analysis (end state vs. current state) and the relationship to ISM
12. Cost benefit analysis - mitigating risks to acceptable levels
13. Risk management principles and practices

Summary

- Audience Participation Activities

Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

- Additional Resources To Be Provided (a.k.a. Take-aways)

Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

Day 3 – CISM Boot Camp Developing an Information Security Program

(Corresponds to Domain 3 of the CISM exam – 17%)

Description

Information is one of an organization's most important assets. Protection of information assets is necessary to establish and maintain trust between the organization and its customers, maintain compliance with the law, and protect the reputation of the organization. Timely and reliable information is necessary to process transactions and support organization and customer decisions. An organization's earnings and capital can be adversely affected if information becomes known to unauthorized parties, is altered, or is not available when it is needed.

Information security is the process, by which an organization protects and secures its systems, media, and facilities that process and maintain information vital to its operations.

Organizations often inaccurately perceive information security as the state or condition of controls at a point in time. Security is an ongoing process, whereby the condition of an organization's controls is just one indicator of its overall security posture. Other indicators include the ability of the organization to continually assess its posture and react appropriately in the face of rapidly changing threats, technologies, and business conditions.

The purpose of an information security program is to:

1. Establish an organization-wide approach to ensure the accuracy, security and protection of information in the organization's custody, regardless of format.
2. Prevent and protect against any anticipated threats and hazards to the security or integrity of organizational information.
3. Ensure organization-wide compliance to applicable laws, regulations, policies and practices.
4. Prevent and protect against the unauthorized access to or use of organization information, including confidential and personal information.

This session addresses the ways and means of developing an information security program that enables an organization to meet its business objectives by implementing business systems with due consideration of information technology (IT)-related risks to the organization, business and trading partners, technology service providers, and customers.

Learning Objectives: After completing this session, the participant will be able to:

1. Breakdown information security management strategies into manageable and maintainable plans for implementing information security policies and procedures.
2. Identify activities associated with a vibrant information security program.
3. Recognize needed information security controls
4. Design applicable information security controls, as warranted by the operational environment
5. Construct appropriate tests of selected information security controls
6. Evaluate logical and physical information security architectures
7. Produce information security policies, guidelines, procedures.
8. Assess the integration of information security requirements into organizational processes
9. Understand and recognize appropriate information security metrics
10. Assist in developing a business case for implementation of a viable information security program, across the enterprise

Session Outline

- Interpreting ISM strategies into manageable and maintainable plans for implementing information security policies and procedures
- Information security program – general associated activities
- Managing the implementation of the information security program
- Planning, designing, developing, testing and implementing information security controls
- Methods used to align information security program requirements with those of other assurance functions
- Identifying internal and external resources and skills requirements supporting the ISM function
- Logical and physical information security architectures
- Security technologies (hardware, software) and controls (monitoring tools)
- Information security awareness - training and education of enterprise personnel, vendors, etc.
- Identification, development, implementation and maintenance of ISM policies, standards, procedures, guidelines
- Integration of information security requirements into organizational processes (e.g. change control, mergers and acquisitions)
- Enterprise contracts (e.g., SLAs, contractors, suppliers, VANs, trading partners, joint ventures, etc.) – managing risk and addressing ISM issues
- Information security metrics – identification, design, development and implementation
- Information security controls (e.g. vulnerability testing, assessment tools) - effectiveness and applicability
- Information security awareness, training and education - effectiveness and relevancy to enterprise operations
- Growing the information security program across the enterprise

Summary:

- Audience Participation Activities

Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

- Additional Resources To Be Provided (a.k.a. Take-aways)

Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

Day 4 – CISM Boot Camp Managing an Information Security Program

(Corresponds to Domain 4 of the CISM exam – 24%)

Description

Management controls involve those safeguards and countermeasures that manage the security of data and the information systems which process those data, along with the associated risk to organization assets and operations.

The overall objective of an information security management program is to ensure that risks to an organization's data assets are correctly identified and effectively and efficiently managed. This emphasizes that information security is a management issue and as such, includes the proper assessment, evaluation and oversight of people, policies and processes. It is not merely a technical or operational issue.

Identification and assessment of the main risks to an organization's data assets, enables suitable management objectives, essential policies and individual roles and responsibilities to be established. This process provides the foundation for a viable information security governance framework, and the proper management of an information security program.

This session examines the frameworks and processes required to effectively manage an organization's information security program.

Learning Objectives: After completing this session, the participant will be able to:

1. Interpret, design, and advocate information security policies.
2. Recognize and construct process and procedures for effective organization-wide information security management.
3. Evaluate effectiveness of third-party relationships in their contribution to achieving both IT and organization strategic objectives.
4. Assess SLAs, TPAs, vendor relationship management with respect to achieving information security goals and objectives.
5. Define and monitor security requirements in service level agreements.
6. Evaluate the effectiveness of the information security program investment, through the use of applicable metrics.
7. Develop testing and validation methods to assess the effectiveness of information security controls.
8. Measure the effectiveness of change and configuration management activities as a critical process within the organization's information security management function.
9. Evaluate the feasibility, cost benefits and risk, associated with the use of external assurance providers to conduct information security reviews.
10. Perform assessment reviews for compliance to accepted standards for managing and controlling access to information.

Session Outline

1. Interpreting and Implementing information security policies
2. Administrative processes and procedures for effective ISM (e.g., access controls, identity management, remote access)
3. SLAs, contractors, suppliers, VANs, trading partners, joint ventures, security services providers, etc., enterprise contracts - managing information security issues
4. Right to audit, confidentiality, nondisclosure, non-compete – managing information security related contract provisions
5. Defining and monitoring security requirements in service level agreements (SLA)
6. Continuous monitoring enterprise-wide infrastructure and business applications security activities
7. Validating the information security program investment – applicable metrics (e.g., data collection, periodic review, key performance indicators)
8. Testing the and validating the effectiveness and applicability of information security controls (e.g. penetration testing, password cracking, social engineering, assessment tools)
9. ISM - change and configuration management activities
10. Pros vs. Cons of employing internal/external assurance providers to conduct information security reviews
11. Due diligence activities, reviews and related standards for managing and controlling access to information
12. Third-party sources - identifying potential impacts on information security in applications and infrastructure (e.g., pen-testing)
13. Security base lining - changes effecting information security program elements
14. Problem management – resolving information security issues

Summary

- Audience Participation Activities

Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

- Additional Resources To Be Provided (a.k.a. Take-aways)

Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

Day 5 – CISM Boot Camp Incident Response & Management - Response, React, Recover

(Corresponds to Domain 5 of the CISM exam – 14%)

Description

The objective of a viable incident management strategy is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters, and to ensure the timely resumption of these critical processes. A workable incident response process must be established to minimize the impact on the organization and recover from loss of information assets, to an acceptable level, through a combination of preventive and recovery controls.

It is essential that a managed process be developed and maintained for business continuity throughout the organization that addresses the information security requirements critical for sustaining the organization's ongoing business mission.

This session addresses the processes and procedures vital to establishing the critical and required elements of an organization-wide, information incident management plan.

Learning Objectives: After completing this session, the participant will be able to:

1. Identify the essential elements of a disaster recovery plan (DRP), business continuity plan (BCP), incident management plan (IMP).
2. Define and assist in developing practices, policies and procedures for information security incident management.
3. Participate in validating the effectiveness of DRP/BCP/IMP.
4. Identify containment methods applicable to effective incident response planning.
5. Develop incident notification and escalation processes as part of a viable incident response plan.
6. Establish methods and means for critical and essential crisis communications.
7. Establish basic requirements for equipping incident response teams.
8. Document the incident response process.
9. Establish post-incident review practices and investigative methods.
10. Prepare damage estimations, assisting in quantifying an incident's business impact
11. Recognize and use appropriate incident management metrics.

Session Outline

1. What is Incident Management?

- Types of Incidents
- Incident Indicators

2. What is an Incident?

- The Objectives of Incident Management

3. What is Incident Response?

- Goals of Incident response
- The Objectives of Incident Response
- Benefits Of Having An Incident Response Capability
- Compliance with laws, regulations, and policy
- Incident Response and data loss prevention
- Incident Management Challenges

4. What is Business Continuity Management?

- Objective of Business Continuity Management
- Incident Response Plan (IRP)
- Business Impact Assessment (BIA)
- Key Business Recovery Objectives
- What Is Incident Handling?
- 5. Risk in Incident Response
- IR Risk Management

6. Incident Response Organization Services

- Enterprise Response, Analysis and Discovery (ERAD)
- Policies Governing Incident Response
- What Services Does The Incident Response Team Provide?

7. Incident Response Planning

- Intrusion Detection System (Host- and Network- based)

8. Achieving the Objectives of Incident Response

9. Components of an Effective, A Good Incident Management System

10. Metrics for IR

- Recovery Time Granularity (RTG)
- Recovery Object Granularity (ROG)
- Recovery Event Granularity (REG)
- Recovery Consistency Characteristics (RCC)
- Recovery Location Scope (RLS)
- Recovery Service Scalability (RSS)
- Maintenance Point Objective (MPO)
- Total Cost of Recovery (TCR)
- Annualized Loss Expectancy (ALE)

11. Performance Measurements for IR

12. Six Steps to Handling An Incident Most Effectively

- Choosing a Containment Strategy

13. Evidence Gathering and Handling

14. Incident Management Deployment Phases

Summary

- Audience Participation Activities

Attendees will be encouraged to actively participate in responding to questions posed regarding the subject matter and presented.

- Additional Resources To Be Provided (a.k.a. Take-aways)

Attendees will be provided with several articles written by the presenter on the subject and several industry whitepapers addressing the presentation topic.

Your Trainer

Albert J. Marcella Jr., Ph.D., CISA, CISM

Albert J. Marcella Jr. is an internationally recognized public speaker, researcher, workshop and seminar leader with over 30 years of experience in IT audit, security and assessing internal controls, and an author of numerous articles and 32 books on various IT, audit and security related subjects.

Dr. Marcella's book Cyber Forensics: Collecting, Examining, and Preserving Electronic Evidence An Auditor's Field Manual, second edition, focuses on issues, tools, and control techniques designed to assist audit, law enforcement, and info security professionals in the successful investigation of illegal activities perpetrated through the use of information technology.

Professor Marcella is a tenured, full-professor at Webster University in Saint Louis, MO, where he is responsible for teaching information technology management courses in the University's graduate and doctoral programs.

Dr. Marcella is the Institute of Internal Auditors Leon R. Radde Educator of the Year, 2000, Award recipient. Dr. Marcella has taught IT audit seminar courses for the Institute of Internal Auditors (IIA), continues to teach for the Information Systems Audit and Control Association (ISACA), and has been recognized by the IIA as a Distinguished Adjunct Faculty Member.

DR. MARCELLA BELONGS TO THE FOLLOWING PROFESSIONAL ORGANISATIONS:

1. Information Systems Audit and Control Association (ISACA)
2. Institute of Internal Auditors (IIA)

DR. MARCELLA HAS EARNED THE FOLLOWING U.S. UNIVERSITY ACADEMIC CREDENTIALS:

- Ph.D. (Information Management)
- MBA (Finance)
- B.S. (Information Technology)
- B.S. (Management)

ORGANIZED BY INVENSION INTERNATIONAL

Registration for CISM is available online:

log in to www.inversion-i.com

Price : USD 2,695 / Per Delegate

OR you may wish to contact the person in-charge:

Abdul Qadeer

Tel: +603 2162 8485

Fax: +603 2162 7485

Email. qadeer.h@inversion-i.com