RMI Risk Masters International LLC

Business Continuity Management for I.S. Auditors and Information Security Professionals

This is a two-day seminar, combining lecture with a hands-on, case-study based workshop that introduces I.S Auditors and Information Security Professionals to the principles and practice of Business Continuity Management (BCM). It includes standards, methodology, and audit and review techniques for both business and Information Technology resilience and recoverability.

Intended audience: I.S. Auditing managers and staff, Information Security managers and staff, Risk Managers, I.T. operations personnel, Internal Financial and Operational Auditors, Corporate Management, Chief Financial Officers and staff

Learning objectives: Participants in this seminar will learn:

- The business rationale for Business Continuity Management
- How to view and measure business continuity risk
- Widely accepted standards for Business Continuity Management
- The basic steps for the development of
    - A Business Continuity Plan
    - An I.T. Disaster Recovery Plan
    - A Crisis Management Plan
- Requirements for governance and oversight of a Business Continuity Management program
- An overview of tools and techniques for Business Continuity Planning
- An approach to auditing a Business Continuity Management program and the plans developed by such a program

Seminar outline:

A. The rationale for Business Continuity Management
    a. Strategic needs from the Senior Management viewpoint
    b. Responsiveness to business risk
    c. Tactical drivers from the operational viewpoint
B. Business continuity risk
    a. Business Continuity Management risk framework
    b. Risks at various stages
        i. During planning
        ii. Prior to an incident
        iii. Following an incident
    c. Justifying the investment in Business Continuity Management
C. An overview of Business Continuity Management standards
    a. BS 25999 – the global standard
    b. NFPA 1600 – the US standard
    c. ISO 27002 – the integration with Information Security

d. Practitioner guides (Disaster Recovery Institute International, Business Continuity Institute)

D. Developing a Business Continuity Plan
   a. Assessments of risk and current capabilities
   b. Business impact analysis (BIA)
   c. Strategy development
   d. Documentation of plans and procedures
   e. Continuous improvement and maintenance
   f. Beginning of case study workshop

E. Developing an I.T. Recovery Plan
   a. Integration with Business Continuity Planning
   b. The impact of integrated systems (ERP, CRM, etc.)
   c. Recoverability, availability and resilience
   d. Strategic and tactical alternatives
   e. Continuation of case study workshop

F. Developing a Crisis Management Plan
   a. Organization and structure of crisis management
   b. Emergency response
   c. Managing a crisis
      i. Communications
      ii. Deployment
      iii. Training and testing
   d. Continuation of case study workshop

G. Building a Business Continuity Management program
   a. Pre- and post-event governance
   b. Implementation
      i. Planning tools
      ii. Response tools and techniques
   c. Training
   d. Testing
   e. Continuation of case study workshop

H. Auditing the Business Continuity Management program
   a. Standards-based approach
   b. Effectiveness-based approach
   c. Quality assurance
   d. Compliance testing
   e. Completion of case study workshop

I. Conclusion

Seminar logistics: This is a two-day seminar (16 hours). Because of the intensive case study workshop, the seminar attendance should be limited to approximately 35 people.

Contact:

Steven Ross, Executive Principal,
stross@riskmastersinc.com, (917) 837-2484

Eric A. Beck, Principal,
erbeck@riskmastersinc.com, (732) 261-9555