RMI Risk Masters International LLC

IT Disaster Recovery: A Master Class

This is a two-day seminar, combining lecture with a hands-on, case-study based workshop that presents the most current trends and methods for IT Disaster Recovery. The purpose of the class is to provide those responsible for planning, executing and maintaining IT resilience and Disaster Recovery Plans with the skills and techniques to do their jobs *better*. It is assumed that participants have basic Business Continuity Management and IT Disaster Recovery knowledge. This class starts from there and goes deeper into the actual challenges facing Disaster Recovery planners today.

Intended audience: IT Disaster Recovery planners, IT operations personnel, IT Auditing managers and staff, IT-knowledgeable Risk Managers, Information Security managers and staff, experienced Business Continuity managers and staff

Learning objectives: Participants in this seminar will learn:

- The foremost challenges facing IT functions with regard to Disaster Recovery
- How to avoid the pitfalls and take advantage of the latest technologies
- The elements of a Disaster Recovery architecture
- DR consolidation and diversification
- The risks and advantages of moving from the "tried and true" to the "leading edge"
- How to (re)develop a Disaster Recovery Plan to keep pace with changing technologies
- Managing the risks and resources of complex Disaster Recovery projects
- Adapting Disaster Recovery planning to the changing needs of the business

Seminar outline:

A. Welcome to Tomorrow: The Current Challenges of Disaster Recovery Planning
    a. Changing operating technologies
    b. Changing economics for backup and recovery
    c. Changing threat environment
        i. Cyberattacks
        ii. Remote data center staffing
        iii. Climate change
        iv. Vendor failure
    d. The non-data center data center
        i. The cloud
        ii. Software Defined Data Center
    e. Organizational issues
        i. Keeping up with the business
        ii. Mergers and divestitures

B. Mergers and Divestitures
    a. Multiple dimensions, compressed timeframe
    b. Data center consolidation
        i. Challenges and opportunities

ii. Keeping the big(ger) picture in sight
c. Data center separation
i. What (and who) goes where?
ii. Splitting applications and infrastructure
d. Transition initiatives
e. Transformation
i. Program management
ii. Facilities transformation
iii. Technology transformation
iv. Operational transformation
f. Case study

C. Managing Complex Disaster Recovery Planning Projects
a. Characteristics of complex Disaster Recovery Planning projects
b. Adding value by managing risk
c. QRM – Quality and Risk Management
d. Empowering the Disaster Recovery Manager

D. Frameworks and Standards
a. NFPA
i. 1600
b. ISO Standards
i. 27001/2
ii. 27031
c. NIST standards
i. 800-34
ii. Cybersecurity Framework

E. Data Center Risk, Resilience and Sustainability Assessment
a. Physical architecture
b. Power
i. IDUs
ii. UPS
iii. Generators
c. Cooling
i. HVAC
ii. Chillers
d. MEP (Mechanical, Electrical and Plumbing)
e. Downtime analysis
f. Case study

F. Disaster Recovery Architecture
a. What is an architecture?
b. Business drivers and operational requirements
c. Architectural elements
i. Facilities
ii. Storage
iii. Backup and recovery
iv. Computing platforms
v. Transport
vi. Applications

vii. Staffing
d. Putting the pieces together
i. Solution analysis
1. Internal strategies
2. External strategies
ii. One-stop shopping vs. best of breed
iii. Cost comparison
e. Case study

G. Comprehensive Disaster Recovery Plans
a. Functional Plan
i. Roles and responsibilities
ii. Mobilization
iii. Progress reporting
iv. Restoration
b. Technical Plan
i. Preemptive vs. reactive planning
ii. Resource requirements
iii. Data backup
iv. Recovery steps
c. Case study

H. Cloud-based Recovery (DRaaS)
a. Advantages and limitations
b. Market analysis
c. Cost

I. Cyber-recovery
a. RTO vs. MTTR (mean time to repair)
b. Trusted images
c. Isolated recovery environment
d. Re-architecture
e. CyberCERT
f. Recovery time calculation
g. Case Study

J. Third Party Recoverability
a. Internet connectivity
b. Assurance
i. Right to audit
ii. Third party assessments
iii. Service level agreements
c. Alternatives
d. Case study

K. Recovery for Distributed Systems
a. Centralized and decentralized models
b. Timeframes and data loss expectations
c. Work at home issues and solutions
d. Case study

L. 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@riskmastersintl.com, (917) 837-2484

Stacy Olewiler, Associate Principal, solewiler@riskmastersintl.com, (717) 368-6256