RMI Risk Masters International LLC

Building the Resilient (Enough) Enterprise:
A Seminar/Workshop for Risk and Control Professionals

This is a two-day seminar/workshop, combines lecture with a hands-on, case-study continues through the entire course. It presents a proactive approach to determining the degree to which businesses need to keep their operations running under any and all circumstances. Resilience at the appropriate level needs to be built into the design, implementation and operation of business and technology processes. Based on known best practices and globally-accepted standards, this course addresses resilience in many forms: business operations, information systems, telecommunications, supply chains and customer service. The seminar/workshop involves participants in both the tactical and strategic decision-making and design processes that lead to never-fail enterprises.

Intended audience: Information Security managers and staff, Risk Managers, Business Continuity Managers and staff, I.T. and Financial Auditors managers (internal and external), I.T. operations personnel, Technical engineers and architects

Learning objectives: Participants in this seminar/workshop will learn:

- Determining the necessity for Enterprise Resilience…or Business Continuity at a lesser level
- Lessons learned from organizations that kept going through potential disruptions...and those that did not
- Assessing the risk of disruption and downtime
- Justifying the investments in resilience
- Developing resilient organizational structures
- Going beyond Business Continuity Planning
- How Cloud processing contributes to Resilience
- Building resilient networks
- Managing vendor resilience
- Serving customers through disruptions

Seminar outline:

A. Resilience as an Enterprise Policy
    a. Definition of Enterprise Resilience
        i. Resilience, business continuity and recoverability
        ii. Possibilities and limitations
    b. Standards for resilience and their broader application
        i. Construction
        ii. Power
        iii. Banking
    c. Business drivers for resilience
        i. Customer expectations
        ii. The consequences of disruption
        iii. Taking advantage of technology
    d. Case study #1

B. Determining the Need for Resilience
    a. Implementation of Policy
        i. Can the business tolerate any downtime? Some?
        ii. Are there acceptable causes?
    b. Risk
        i. Determining potential causes for disruption
            1. External threat assessment
            2. Internal vulnerability assessment
    c. Impact
        i. Business Impact Analysis techniques
        ii. Is a BIA necessary?
    d. Cost
    e. Return on investment
    f. Case study #2

C. Business Resilience
    a. Strongest and weakest links
    b. Continuity of operations
    c. Continuous operations
    d. Acceptable downtime
    e. Case study #3

D. Personnel Resilience
    a. Planning for absenteeism
        i. Remote working
        ii. Staff distribution
        iii. Cross-training
        iv. Collaboration
    b. Resilience in normal times and in emergencies
    c. Lessons Learned from Covid-19
    d. Assessing Personnel Resilience
    e. Case study #4

E. Data Center Resilience
    a. Uptime Institute Tier levels
    b. Mechanical, electrical and plumbing (MEP)
        i. Power
        ii. Cooling
        iii. Security
    c. Sustainability
    d. Trends affecting data center resilience
        i. Containers and pods
        ii. Software defined data center (SDDC)
    e. On-premises, colocation and the Cloud
    f. Assessing Data Center Resilience
    g. Case study #5

F. Cyber Resilience
    a. Resilience in the face of cyberattacks
    b. Backup and recovery
    c. Distributed architectures

d. Virtualization and mobility
e. Infrastructure as a Service (IaaS)
f. Assessing Cyber Resilience
g. Case study #6

G. Supply Chain Resilience
   a. Third, fourth and nth parties
   b. Certification and validation
   c. Collaboration with vendors
   d. Internal Audit's role
   e. Industry associations' role
   f. Case study #7

H. Putting the Pieces Together
   a. Building a resilient culture
   b. Resilience as a design criterion
   c. Learning how to be resilient
   d. Staying resilient

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@riskmastersintl.com, (917) 837-2484

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