RMI Risk Masters International LLC

Data Privacy for I.T. Auditors and Information Security Professionals

This is a two-day seminar, combining lecture with a hands-on, case-study based workshop that introduces I.T. Auditors and Information Security Professionals to the principles, practices, legislation and governance of Personal Information Privacy. It includes standards, methodology and audit and review techniques for both business and Information Technology resilience and recoverability.

Intended audience: I.T. 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, Chief Privacy Officers and their staff, compliance personnel.

Learning objectives: Participants will gain a deep understanding of personal information including:

- What's privacy all about?
- What's driving privacy?
- What are the business benefits of privacy compliance?
- What are the risks of non-compliance?
- Dealing with multi-jurisdictional legislation and regulations
- Creating a privacy compliant organization
- Establishing privacy baselines
- Monitoring privacy initiatives
- Responding to a privacy breach
- Privacy reporting
- Sustainable compliance
- Addressing future privacy trends

Seminar outline:

A. The Privacy Imperative
    a. Approaching privacy
    b. Strategic and tactical drivers
    c. Privacy impacts
    d. Privacy legislation and regulation

B. Value-Based Privacy
    a. Stakeholders and customers
    b. Business drivers
    c. Making the business case for privacy

C. Assessing Privacy Compliance
    a. Identify privacy-relevant data assets
    b. Assess the current state of privacy protections
    c. Functional decomposition
    d. Case study

D. Design
    a. Strategic plan
    b. Tactical plan
    c. Organization and infrastructure
    d. Privacy policies
    e. Case study

E. Implement
    a. Remediation of systems (operational and technical)
    b. Awareness
    c. Chief Privacy Officer
    d. Case study

F. Monitor
    a. Compliance
    b. Reporting

G. Creating a Culture of Privacy
    a. Privacy in context
        i. Inhibitors and rewards
        ii. Methods to strengthen data privacy
    b. Pre-requisites
        i. Executive sponsor or champion
        ii. Positive and negative reinforcement
    c. Case Study

H. Generally Accepted Privacy Principles (GAPP)
    a. Ten principles defining privacy components
    b. 73 criteria
        i. Policies
        ii. Communications
        iii. Procedures
        iv. Controls
    c. Documentation
        i. Collection
        ii. Evaluation
        iii. Reporting
    d. Customizing GAPP

I. Privacy metrics
    a. Costs and benefits
    b. Monitoring and reporting

c. *Case study*

J. Privacy Maturity Model (PMM)
   a. Relationship with GAPP
   b. Using PMM data collection and assessment forms
   c. PMM reporting
   d. Case study

K. Privacy Data Breach Response Plans
   a. Preparation and Planning
   b. Breach Identification
   c. Breach Containment / Mitigation
   d. Breach Evaluation and Notification
   e. Breach Recovery (Critical Functions Restored)
   f. Breach Resumption (All Functions Restored)
   g. Breach Response Assessment and Lessons Learned

L. Auditing Privacy
   a. Tools and techniques
   b. Obtaining value from data privacy

M. 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:

Robert Parker, Advisory Consultant
rparker@riskmastersinc.com
(250) 658-0250

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