Developing of an Information Security and Risk Management Program Strategy

Overview

Information security has become a critical issue within organizations, and a key success factor for businesses. In order to effectively maintain the integrity and security of an organization’s information infrastructure an information security and risk management strategy and program must be developed and implemented. This workshop will introduce the concepts of developing an information security and risk management strategy, structure of an information security program, threat and vulnerability management, and metrics for effective information security governance. This workshop will highlight the key functional areas, processes and methodologies, and organizational concepts that should be included in order to implement and maintain an effective information security strategy and program. Key functional areas will be discussed in depth and will be highlighted for their importance to the strategy, activities that they will perform, and their associated key performance indicators (KPI’s). This workshop will utilize interactive discussions and case studies to highlight operationally capable models and solutions.

Syllabus

• Why is Strategy Important to Information Security and Risk Management
  • Current Business Conditions
  • Risk Profile
  • Budget Availability
  • Annual vs. Rolling Three Year Plan
  • Point of Arrival
  • Staff Availability
  • Cultural Awareness
  • Operational Components Yes or No?
  • Reporting Structure
  • Competency Models
  • Sourcing Plans
  • Industry Standard Alignment
  • Key Performance Indicators
  • Global Considerations
  • Compliance and Risk
  • Consequence Management
  • Oversight and Reporting
  • Organizational Interactions
  • Communication and Awareness
  • Cultural Change – Security vs. Risk Management
• Introduction of an Information Security Program
  • Functional elements of an Information Security Program
  • Organizational Structure of Information Security Program
  • Key dependencies and linkage points
• Key Performance Indicators (KPI’s) of key functional areas
• Key competencies and staffing models
• Case studies of Information Security Program Deployments
• Individual Element Exploration
• Threat and Vulnerability Management
  • Overview of Threat and Vulnerability Management Programs
  • Asset Identification
  • Threat Analysis Who, What, When, Where, and How
  • OSI+ Methodology
  • Intelligence Gathering and Assessment
  • Vulnerability Management
  • Risk Mitigation Strategies
  • Countermeasure and Control Development
• Developing Metrics for Effective Information Security Governance
  • Defining the Measurement
  • Business Goal Alignment
  • Baseline Framework of Metrics
    • Organizational and Performance Metrics
    • Operational Metrics
    • Technological Metrics
    • Business Process Metrics
    • Business Metrics
    • Compliance Metrics
  • Meaningful Reporting
  • Benchmark Reporting
• Final Thoughts

Who Should Attend

  o Individuals who have the responsibility to provide data security and privacy service within their organization
  o Business executives and who have the responsibility of designing, implementing, and operating information security programs within their organization
  o Business executives who would like to understand how to implement an effective information security program within their organization
  o Information security auditors who are responsible for providing oversight to enterprise information security solutions

Prerequisites

  o Familiarity with basic information security technologies, concepts, policies, procedures, and techniques. No security background or technical background required.

Presentation Time
1 or 2 Days (2 Day Includes extended case studies and student projects)

**Instructor**

John P. Pironti is the President of IP Architects, LLC. He has designed and implemented enterprise wide electronic business solutions, information security and risk management strategy and programs, enterprise resiliency capabilities, and threat and vulnerability management solutions for key customers in a range of industries, including financial services, energy, government, hospitality, aerospace, healthcare, pharmaceuticals, media and entertainment, and information technology on a global scale. Mr. Pironti has a number of industry certifications including Certified in the Governance of Enterprise IT (CGEIT), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified in Risk and Information System Control (CRISC), Information Systems Security Architecture Professional and (ISSAP) and Information Systems Security Management Professional (ISSMP). He is also a published author and writer, highly quoted and often interviewed by global media, and a award winning frequent speaker on electronic business and information security and risk management topics at domestic and international industry conferences.