Building Blocks

Course Outline

This four day intermediate level Information Systems Security Officer (ISSO) course expands upon the principles and concepts learned in the ISSO Orientation course by delving deeper into detail regarding the people, process and technology aspects of an ISSO's role. This course sets the stage with an accelerated review of entry level security principles and concepts that quickly moves to more detailed security topics, discussions, demos, and hands-on exercises utilizing open source security tools.

Lecture material is further reinforced via individual and group exercises that include using tools that will demonstrate the capability of popular open source security tools used by many security professional today as a function of their role.

Audience

Unit ISSO's who have completed introductory training regarding information security principles and practices; experienced ISSO's seeking an intermediate level of instruction and exercises; or for those needing to advance their skills and knowledge in managing site and/or system security at the Junior to Intermediate level of experience in IT Security.

You will learn how to:

- Understand the importance of understanding the needs of the business to effectively implement reasonable and effective security controls and safeguards
- Understand the importance of security policy and associated documents and practices that support an effective security program
- Understand the relationship between people, process and technology processes supporting security implementations at the administrative, technical and physical perspectives
- Understand the importance of layering security implementations of controls and safeguards that support preventive, detective, response and recovery processes
- Make use of some of the security tools via demo's, and hands-on exercises to reinforce the presentation of information during class

Buiding Blocks Technologies, Inc. • 170 Laurier Avenue West, Suite 810 • Ottawa, Ontario K1P 5V5 • T: 613.230.6255 • F: 613.599.0859 • www.bblockstech.com

Building Blocks

Course Topics

ISSO Foundations Review

1. Course Introduction
2. The ISSO Role
3. Disclaimer
4. ISSO Readiness Recommendations
5. IT Security Foundational Principles and Concepts
6. Information Security Trends You Need to Know
7. IT Governance and the Security Program
8. Physical and Logical Security Controls and Safeguards

Overview of Government Security Policies, Directives, Standards and Guidelines

1. GoC Policy on Government Security
2. CSEC – Canada's National Security Policy
3. DND Policies and Security Orders
4. Treasury Board MITS Operational Standard
5. Assets and Information Classification Processes (Sensitivity and Criticality)
6. Group exercise

Evaluation Methodologies Overview

1. Understanding Common Criteria and Questions to Consider
2. Evaluation Methodologies including Common Criteria
3. Security Program Compliance processes
4. Group exercise

Network Security Need to Know

1. What you need to know and why
2. Network Primer, Models, and Layers
3. OSI Model
4. TCPIP Architecture
5. Defense in Depth (Prevention, Detection, Reaction, Recovery)
6. Access Controls, Method and Procedures
7. Hands-On activities using security tools

Media Security and Handling

1. Counter Measures and Labeling
2. Hardcopy Media
3. Fax, Phone and Voicemail, Printers
4. Magnetic Media
5. Optical Media
6. Communications Media
7. Copper
8. Fibre
9. RF Wireless communications
10. Demo on Wireless Sniffing and information reconnaissance

Risk Management

1. Overview of Risk Management for ISSO Officers
2. Risk Management Methodologies
3. Threats and Vulnerabilities
4. Threat Agents, Vectors and Exploits
5. Threat Risk Assessments and the TBS Harmonized TRA methodology
6. Group exercise

Incident Management, eDiscovery and Forensics

1. Procedures for Incident Handling
2. Incident Handling and Investigations
3. Security breaches and high technology crimes
4. Information Warfare and National Security
5. Computer Crimes
6. Criminal activity preparedness
7. Hands-on exercise

Configuration Management, Business Continuity Planning and Crisis Management

1. Definitions of CM, BCP and Crisis Management
2. Configuration and Change Management
3. Continuous Risk Services and Continuity of Critical Assets
4. Nature and Human-Made Crises and Availability of Critical Services
5. Group exercise

Certification and Accreditation

1. A Walk-Through of a service's Certification and Accreditation Process - condensed (Group exercise)

Buiding Blocks Technologies, Inc. • 170 Laurier Avenue West, Suite 810 • Ottawa, Ontario K1P 5V5 • T: 613.230.6255 • F: 613.599.0859 • www.bblockstech.com