ManTech

TRAINING
COMMERCIAL PRICELIST
MANTECH INTERNATIONAL CORPORATION
January 2020

ManTech

TABLE OF CONTENTS

ManTech

MANAGEMENT TRAINING COURSE DESCRIPTIONS AND PRICES

Course Description	Course Length (hours)	Customer Site		ManTech Site (per student)
		Base Price	Individual Fee (per student)	
Using DISC Personality Diagnostics to Communicate	4	$3,000	---	$245
Situational Leadership II	4	$3,000	$100	$295

Number of attendees is unlimited
An additional charge of $5 applies for each copy of materials
Travel charges are not included in this pricing and will be negotiated on a case-by-case basis.

Using DISC Personality Diagnostics to Communicate:

Participants will be exposed to the DISC personality diagnostic instrument in an effort to understand their communication and behavior patterns. Further, each personality type will be examined to assist each participant in understanding how to interact and communicate with individuals of different personalities. At the conclusion, each participant should have a basic understanding of how and why interactions with others are affected by personality. During this presentation, the use of video clips and PowerPoint slides are used to reinforce the conceptual framework of the course.

Situational Leadership II:

Using Ken Blanchard's Situational Leadership Model II as a basis, participants will develop a basic understanding of their managerial and leadership role and responsibility in directing, coaching, supporting and delegating to their employees, dependent on their employees developmental and readiness level to assume additional duties and responsibilities. A further discussion of the correlation of DISC personality diagnostic will be related to situational leadership. Course materials will be provided through the Ken Blanchard Company. During this presentation, the use of video clips and PowerPoint slides are used to reinforce the conceptual framework of the course. This course contains the basic information and one diagnostic.

To register, please contact:
Karen Gardner, Executive Director, Training and Organizational Development
Email: Karen.Gardner@ManTech.com
Direct Dial: (703) 218-6074
Fax: (571) 748-6450

ManTech

INFORMATION SYSTEMS SECURITY TRAINING COURSE DESCRIPTIONS AND PRICES

Course Title	Course Cost	Course Location
Risk Management Framework (RMF) Open Enrollment	$1,950.00	Various Locations
Program Security Fundamentals (PSF) Open Enrollment	$1,950.00	Various Locations
Information Systems Continuous Monitoring (ISCM) Open Enrollment	$2,990.00	Various Locations
Risk Management Framework (RMF) Onsite (Max 24 Students)	$27,500.00	Customer Location
Program Security Fundamentals (PSF) Onsite (Max 24 Students)	$27,500.00	Customer Location
Information Systems Continuous Monitoring Onsite (Max 20 Students)	$35,000.00	Customer Location
Windows 7 Security Audit Onsite (Max 16 Students)	$37,500.00	Customer Location
Introduction to Linux Security Onsite (Max 16 Students)	$37,500.00	Customer Location

We accept Visa, MasterCard, American Express, checks and purchase orders.

Registration:
Tammy Delesky, Technical Training Manager
Email: Tamara.Delesky@ManTech.com
Direct Dial: (703) 610-9297
Mobile: 540-604-8245
Fax: (571) 297-9584

CANCELLATION POLICY: All payment arrangements (credit card, check or purchase order) must be received and finalized by the designated payment deadline to secure a confirmed reservation.

Cancellation fees are as follows:

- Up to 30 days prior to class start date — No cancellation fee
- 30 to 21 days prior to class start date — Eligible for 50% refund of course tuition
- 21 to start of class — Forfeit of 100% of course tuition

Requests for refund due to emergency situations will be considered on a case by case basis and must be approved by the ManTech Security & Mission Assurance Training Center Director.

ManTech

ManTech Advanced Systems International

Risk Management Framework Course

Course Outline

1. **The history and transformation of Risk Management Framework**
    a. By the end of this module you should be able to:
        i. Understand Transformation Strategic Vision and Goals
        ii. Explain how the C&A process is transitioning to align with the RMF process
        iii. Explain the RMF Roles and Functions
        iv. Discuss Committee for National Security Systems (CNSS) policies and instructions; National Institute of Standard and Technology (NIST) Special Publications; and Joint SAP Implementation Guide (JSIG)
        v. Explain the Security Authorization Artifacts required to achieve system authorization

2. **Managing Risk Within the SAP Information Environment**
    a. By the end of this module you should be able to:
        i. Understand the basic concepts of Risk Management
        ii. Understand how to manage risk within the SAP information Environment
        iii. Define risk management factors, to include the risk analysis questions to be considered
        iv. Implement the Risk Management Framework and process in support of:
            1. NIST SP 800-37
            2. NIST SP 800-39
            3. NIST SP 800-30
        v. Understand the importance of Risk Management within the System Development Lifecycle

3. **Step 1 – Categorizing the System**
    a. By the end of this module you should be able to:
        i. Discuss Risk Management Framework Step 1 – System Categorization
        ii. Understand the initial Risk Assessment
        iii. Understand essential elements of Information and expectations for a System Security Plan (SSP)

4. **Step 2 – Selecting Security Controls**
    a. By the end of this module you should be able to:
        i. Explain the Risk Management Framework Step 2 – Selecting Security Controls
        ii. Gain awareness of the SAP Communities combined use of CNSS & NIST guidelines for NSS as process for Control Selection
        iii. Complete a Security Control Selection Exercise
        iv. Review and understand a Security Control Traceability Matrix (SCTM)

5. **Step 3 – Implementing Security Controls**
    a. By the end of this module you should be able to:
        i. Explain the Risk Management Framework Step 3 – Implementation of Security controls

ii. Gain Awareness of the Special Access Program (SAP) community's combines use of NIST guidelines for NSS and Community Best Practices for Implementing Security Controls
iii. Discuss Best Practices to assist in implementing security controls

6. **Step 4 – Assessing Security Controls**
   a. By the end of this module you should be able to:
      i. Explain the Risk Management Framework Step 4 – Assessment of Security Controls
      ii. Gain awareness of the Special Access Program (SAP) community's combined use of NIST guidelines for NSS and Community Best Practices for Assessing Security Controls
      iii. Discuss NIST SP 800-53A and Assessment Cases
      iv. Review Security Assessment Report Essential Elements of Information
      v. Discuss methods to assist in assessing Security Controls

7. **Step 5 – Security Authorization**
   a. By the end of this module you should be able to:
      i. Explain the Risk Management Framework Step 5 – System Authorization
      ii. Understand Plan of Action and Milestones (POA&M) Artifact
      iii. Understand types of system authorization

8. **Step 6 – Information Security Continuous Monitoring**
   a. By the end of this module you should be able to:
      i. Apply Risk Management Framework Step 6 – Continuous Monitoring
      ii. Describe SAP Information Security Continuous Monitoring Requirements and Implementation
      iii. Gain awareness of Configuration Management
      iv. Describe a Security Impact Analysis (SIA); Ongoing Controls Assessment; Reporting

9. **Best Practices and Tools**
   a. By the end of this module you should be able to:
      i. Share and discuss IA Best Practices
      ii. Understand various government and industry sites that can provide IA guidance and support
      iii. Various tools to assist the ISSM / ISSO
      iv. Discuss the use of various automated tools

Students will receive: Book with course slides, hard copy of latest JSIG, JSIG templates book, the DAAPM, PM RMF Handbook, and a reference CD

Maintaining Your 8570 Certification Requirements:

Risk Management Framework & Information Security Continuous Monitoring
CompTia CEU's: 32 hours towards A+, Network+, and Security+
ISC (2): CPU's: 32 hours towards CAP, CISSP, and SSCP

ManTech Advanced Systems International

Information Systems Continuous Monitoring (ISCM)

Course Outline

1. **Cybersecurity Vulnerabilities & Threats to Information & Information Systems**
    a. By the end of this module you should be able to:
        i. Discuss common vulnerabilities, threats and trends
        ii. Understand and discuss system exploits
        iii. Understand basic concepts of Risk
        iv. Understand Continuous Monitoring and Risk Management
        v. Discuss the Insider Threat
        vi. Define risk management factors, to include the risk analysis questions to be considered
        vii. Implement the Risk Management Framework and process in support of JSIG

2. **Introduction to Information Security Continuous Monitoring**
    a. By the end of this module you should be able to:
        i. Describe SAP Information Security Continuous Monitoring requirements and implementation
        ii. Be familiar with key documents and terms
        iii. Understand the roles and responsibilities
        iv. Understand why Continuous Monitoring and the way forward

3. **Testing & Assessing Controls**
    a. By the end of this module you should be able to:
        i. Discuss various technical controls
        ii. Understand the techniques for assessing controls
        iii. Understand the importance of proper control implementation to support assessment and continuous monitoring steps
        iv. Test and document the security configuration
        v. Discuss security assessment plan

4. **Monitoring Controls Within the Security Automation Domains**
    a. By the end of this module you should be able to:
        i. Discuss the eleven security automation domains that support continuous monitoring and the controls they monitor
        ii. Discuss what and how we monitor various security controls
        iii. Discuss the development of a continuous monitoring strategy
        iv. Discuss and use tools to monitor the various controls within the security automation domains

5. **ISCM Documentation Creation**
    a. By the end of this module you should be able to:
        i. Discuss and provide sample plans
        ii. Discuss the frequency selection
        iii. Be familiar with various document creation and assistance tools

6. **ISCM Best Practices & Reference Sources**
    a. By the end of this module you should be able to:
        i. Share and discuss IA Best Practices
        ii. Understand various government and industry sites that can provide IA guidance and support
        iii. Various tools to assist the ISSM / ISSO
        iv. Discuss the use of various automated tools

Maintaining Your 8570 Certification Requirements:

Risk Management Framework & Information Security Continuous Monitoring
CompTia CEU's: 32 hours towards A+, Network+, and Security+
ISC (2): CPU's: 32 hours towards CAP, CISSP, and SSCP

ManTech Advanced Systems International / Logos Secure

Windows 7 Security Audit Course (Onsite Course Only)

Course Outline

1. **Audit Method and Policy**
   a. By the end of this module you should be able to:
      i. Understand Audit Method and Policy
      ii. Discuss CNSS, NIST, NISPOM, PCI, HIPAA, FISMA
      iii. Understand when and how to use different methods for auditing
      iv. Discuss Best Practices for implementing audit method and policy

2. **What's New and Security Features**
   a. By the end of this module you should be able to:
      i. Understand Windows 7 / Server 2008R2 New and Improved Audit Security Features
      ii. Discuss the applicable security features to be implemented
      iii. Summarize the intent of required security features
      iv. Explain the importance of proper configuration in order to conduct auditing relative to Policy Confirmation and/or Violation

3. **Even Logs and EVTX**
   a. By the end of this module you should be able to:
      i. Understand how to examine the new structure of even logs
      ii. Explain how to Note the addition of log types
      iii. Understand how to research the underlying technology of the new format and implications
      iv. Explain how to use the updated Event Viewer for viewing the new format and take advantage of queries

4. **Audit Infrastructure**
   a. By the end of this module you should be able to:
      i. Understand Audit Infrastructure
      ii. Identify preliminary concerns to accomplish collection with integrity
      iii. Understand how to analyze event logs
      iv. Discuss how to assess "your" situation and make determinations of "your" environments

5. **Native Commands and Power Shell**
   a. By the end of this module you should be able to:
      i. Review and understand Native Windows commands
      ii. Understand how to use important tools for Event Log Management
      iii. Gain awareness of how to use Power Shell

6. **Event Categories**
   a. By the end of this module you should be able to:
      i. Understand the Windows Audit Policy
      ii. Describe the various Event Types
      iii. Identify the different Event Codes
      iv. Review the Event Log and attempt to find out what it is telling us
      v. Approach the information with RAM in mind to help us prepare for Queries

7. **Tools / Log Parser**
   a. By the end of this module you should be able to:
      i. Gain awareness of LogParser as a utility for audit reduction
      ii. Understand how to create tools to make LogParser easier to use
      iii. Discuss Windows 7 capabilities

8. **VS Audit Framework**
   a. By the end of this module you should be able to:
      i. Understand VS Audit Framework

ii. Explain how VS simplifies the challenges of using a Query Tool for less technical
iii. Explain VS Rapid Query Development
iv. Understand how to organize and practice our radical audit method
v. Discuss how VS provides for more advanced solutions

9. Query Eye for the Security Guy

a. By the end of this module you should be able to:
   i. Explain how to analyze the reference data and apply the tools, methods and new knowledge
   ii. Discuss current issues and Best Practices within the community

ManTech Advanced Systems International

Program Security Fundamentals Course

Course Outline

1. **Information Security**
   a. By the end of this module you should be able to:
      i. Understand original and derivative classification for collateral and SAP information
      ii. Understand classification levels and categories
      iii. Apply appropriate classification markings
      iv. Maintain a Top Secret Accountability System
      v. Understand the function of the Document Control Center (DCC)
      vi. Properly handle security incidents and infractions

2. **Operational Security (OPSEC)**
   a. By the end of this module you should be able to:
      i. Identify the five parts of the OPSEC process, describe the specific activities involved in each part and explain ways to successfully accomplish these activities
      ii. Describe a number of associated OPSEC activities and explain how they relate to and facilitate accomplishment of the OPSEC mission
      iii. Apply what's been learned to a practical exercise

3. **Personnel Security (PERSEC)**
   a. By the end of this module you should be able to:
      i. Understand different types of security questionnaires
      ii. Understand the different levels of security clearances
      iii. Become familiar with the agencies involved in the PERSEC process
      iv. Review form submission for completeness and accuracy
      v. Understand Program Access Requests (PAR's)
      vi. Describe reporting requirements

4. **Physical Security**
   a. By the end of this module you should be able to:
      i. Comprehend, interpret, and identify Special Access Program Facility (SAPF) and Sensitive Compartmented Information Facility (SCIF) basic construction requirements
      ii. Create and process associated accreditation documentation for a new SCIF/SAPF
      iii. Discuss and consult with other physical security professionals about related topics, interface with technical teams, and process related documentation for Program Security Officer approvals

5. **Industrial Security**
   a. By the end of this module you should be able to:
      i. Identify, interpret, and explain Industrial security elements as they pertain to the government and industry partnership for operating in a Special Access Program (SAP) environment
      ii. Determine contractual security requirements and author a Contract Security Classification Specification, DD Form 254

6. **Information Systems Security**
   a. By the end of this module you should be able to:
      i. Comprehend, review and evaluate documentation necessary to assist in the operations of Information Systems and Information Assurance within a Special Access Program Facility (SAPF) and Sensitive Compartmented Information Facility (SCIF)

ii. Gain working knowledge that will enable the collaboration with Information Assurance Managers (IAM) and Information Assurance Officers (IAO) to ensure Information Systems meet operational requirements

7. Other Program Security Topics, Duties and Responsibilities

a. By the end of this module you should be able to:

i. Create and implement a comprehensive security education and training program
ii. Appreciate a very contemporary topic – Insider Threat!
iii. Apply basic planning principles to a variety of program security planning requirements
iv. Acquire a basic understanding of the Freedom of Information Act and how it impacts special access programs
v. Apply various special security processes to the acquisition security arena
vi. Manage inspection programs and perform special access security self-inspections

Maintaining Your SPeD Certifications

Program Security Fundamentals (PSF)
You may claim 45 PDU's under category 2A when you attend this course.
The hours will be reflected on your attendance certificate

ManTech Advanced Systems International / LOGOS Secure

Introduction to Linux Security (Onsite Course Only)

The Introduction to Linux Security course is an intensive 2.5-day training experience led by seasoned Information System Security and Technology professionals. This course provides practice in advanced Information Systems Security skills to support the protection of information and information systems within an ICD 503/JSIG/RMF for DoD IT environment. During the course of instruction, the student will be able to apply Linux security features in order to adhere to requirements for Confidentiality, Integrity, and Availability. Each student will have the opportunity, through practical exercises and hands-on labs, to configure a Linux workstation to comply with ICD 503/JSIG/RMF for DoD IT technical security requirements.

The hands-on Introduction to Linux Security course addresses the array of government requirements faced by today's ISSO/ISSM and System Administrators. The student leaves the class armed with the knowledge and tools required to ensure that their information system operates at an acceptable level of risk.

Course Content

The hands-on Introduction to Linux Security course addresses the array of government requirements faced by today's IAO and System Administrators. The student leaves the class armed with the knowledge and tools required to ensure that their information system operates at an acceptable level of risk.

Topics discussed include:

- Risk Management Framework Overview
- Operating System and Root Account Security
- Linux Identification and Authentication Methods and Common Threats
- Use of Pluggable Authentication Modules
- Linux Resource and Session Control issues
- Methodology for Object Access and Discretionary Access Control
- Configuring and Conducting Auditing within a Linux Environment

INTELLIGENCE PROFESSION EDUCATOR COURSE DESCRIPTIONS AND PRICES

Fully Cleared Instructional Design Executive Consulting

Price: $500 per hour

Accomplished professional in developing learning solutions for government and higher education clients. Ability to meld vision with reality using goal-oriented and measurable instructional design. Significant and progressive curriculum development experience in these areas:

- Basic and advanced investigative techniques
- Interviewing and debriefing
- Operationalizing intelligence (targeting)
- Surveillance detection
- Certification courses for certain intelligence community career tracks
- E-learning and blended solutions

General Guidelines

The compensation system of ManTech International Corporation and its subsidiaries is designed to pay equitably and fairly for services rendered in a manner which aids in attracting, retaining and motivating competent employees without regard to race, sex, age, national origin, religion, or physical ability while providing appropriate control of overall compensation costs.

Price Deviation: Concessions, discounts or other deviations are addressed on a case-by-case basis and are subject to approval by executive level management.

Travel and Accommodations and Other Direct Costs are handled on an order-by-order basis and are subject to open market prices.

Contact Information

For any questions or for additional information, please contact CW Etzler at (703) 218-6320.

Email correspondence may be sent to CW.Etzler@ManTech.com

2251 Corporate Park Drive
Herndon, VA 20171