A Role-Based Model for Federal Information Technology/Cyber Security Training

FISSEA Conference
March 19, 2014

Pat Toth
Computer Security Division
Information Technology Laboratory

Penny Klein
Systegra
Background

- NIST SP 800-16 “Information Technology Security Training Requirements: A Role- and Performance-Based Model” April 1998

- NIST SP 800-16 Rev 1 DRAFT March 2009
Document Development

• Landscape Analysis
• Draft Development
  – 2nd Public Draft October 2013
  – 3rd Public Draft March 2014
    • Comments due April 30
• Final Publication
  – June 2014
Purpose

Provide a comprehensive, yet flexible, training methodology for the development of role-based training courses or modules for personnel who have been identified as having significant IT/cybersecurity responsibilities within Federal Organizations.
Relationships

• SP 800-50 *Building an Information Technology Security Awareness and Training Program*

• FIPS)200 *Minimum Security Requirements for Federal Information and Information Systems*

• NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations*

• NIST SP 800-53 *A Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
Management

• Understand the necessity of role-based training

• Plan for the development, implementation and evaluation of role-based training

• Understand how roles with security related responsibilities are identified within their organization
Using SP 800-16

• IT/Cybersecurity Specialist
  – Subject Matter Expert (SME)
  – Identify training courses and training
  – Identify training gaps and needs
  – Develop baseline
Using SP 800-16

• Training Professionals
  – Understand IT security requirements and knowledge/skills required
  – Evaluate course quality
  – Obtain the appropriate courses and materials
  – Develop or customize courses/materials
  – Tailor their teaching approach to achieve the desired Learning Objectives.
Cybersecurity Proficiency

- Competency
- Knowledge and Skills
- Cybersecurity Essentials
Cybersecurity Essentials

- Technical underpinnings of cybersecurity and its taxonomy, terminology and challenges;
- Common information and computer system security vulnerabilities;
- Common cyber attack mechanisms, their consequences and motivation for use;
- Different types of cryptographic algorithms;
- Intrusion, types of intruders, techniques and motivation;
- Firewalls and other means of intrusion prevention;
- Vulnerabilities unique to virtual computing environments;
- Social engineering and its implications to cybersecurity; and
- Fundamental security design principles and their role in limiting point of vulnerability.
Organizational Responsibilities

- Organization Head
- CIO
- SAISO
- CLO
- Managers
- Training Developer
- Personnel with Significant IT/Cyber security responsibilities
- Users
Cybersecurity Learning Continuum

- Security Awareness
- Cybersecurity Essentials
- Role-Based Training
- IT Security Specialist & Professionals

Increasing Knowledge and Skills
Competency Levels

- Level I: skill requirements are basic and are usually obtained during the first few years in that role.
- Level II: skill requirements are considered intermediate, and are those skills that have obtained and honed during more years in that role.
- Level III: skill requirements are considered expert, and are those skills that can only be obtained after many years in the role.
Competency Levels

Competency in a Role

Competency Level I
Basic

Competency Level II
Intermediate

Competency Level III
Expert

Time in a Particular Role
Training in a Particular Role
Experience in a Particular Role
Functional Perspectives

• Manage
  – Program or technical aspect of a security program
  – Overseeing the lifecycle of a computer system, network or application;
  – Responsibilities for the training of staff

• Design
  – Scoping a program or developing procedures, process and architecture
  – Design of a computer system, network or application;

• Implement
  – Putting programs, processes, polices into place;
  – Operation/maintenance of a computer system, network or application

• Evaluate
  – assessing the effectiveness of any of the above actions.
Overview

- Chap 6 Worked Example
- Chap 7 Evaluation Methodology
- Appendices
  - Appendix A: Functions
  - Appendix B: Knowledge and Skills Category
  - Appendix C: Roles
  - Appendix D: Sample Evaluation Forms
  - Appendix E: Glossary
  - Appendix F: Acronyms
  - Appendix G: References
Appendix A: Functions

- Functions and roles should be identified as candidates for role-based training
  - **Function Area**: Identifies a security function area;
  - **Roles Areas**: Identifies various roles that are covered by the function. These roles are guidelines and may exist under different names within a particular Agency;
  - **Definition**: Provides a definition of the function; and
  - **Outcome(s)**: Identifies the various outcomes that the training module should strive to meet for each of the functions and their associated roles.
Appendix B: Knowledge and Skills Category

- **Knowledge unit and the associated knowledge and skills**

<table>
<thead>
<tr>
<th>INDUSTRIAL CONTROL SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICS-1</td>
</tr>
<tr>
<td>ICS-2</td>
</tr>
<tr>
<td>ICS-3</td>
</tr>
<tr>
<td>ICS-4</td>
</tr>
<tr>
<td>ICS-5</td>
</tr>
<tr>
<td>ICS-6</td>
</tr>
<tr>
<td>ICS-7</td>
</tr>
</tbody>
</table>
Appendix C: Roles

- Competency/knowledge unit and associated Knowledge and Skills required by a particular role
  - Function Area: This area corresponds with Appendix A: Function Area.
  - Role Area: This describes the overall role;
  - Roles: Identifies various roles that are covered by the function
  - Responsibility: Defines the activities, tasks and/or responsibilities of that particular role;
  - Knowledge Unit: Identifies the competencies associated with the role.
  - Corresponding Knowledge and Skills Table: Functional perspectives for tailoring.
    - Manage – responsible for management (e.g., managers, team leads, project managers)
    - Design – responsible for design activities (e.g., system developers, engineers)
    - Implement – execute implementation (e.g., system administrators, network administrators)
    - Evaluate – evaluation activities (e.g., testers, security analysts)
- Flexibility is required for most role-based training
Appendix D: Sample Evaluation Forms

• The forms that will assist in the evaluation of the training are located within this appendix

• Important to the overall process
Appendix E, F and G

- These appendices are the glossary, acronyms and references
- Glossary and Acronyms do not include all Federal Organization – will have to tailor to your organization
- References provide NIST, FIPS and NICE documents that can provide additional guidance
Worked Example
Step 1

• Conducting the Agency-Wide Needs Assessment
  – Identify any gaps in the current training program, and/or identify those roles which require training
  – Federal Organization to use their own process
  – NIST SP 800-50 to provide guidance
For example, the Needs Assessment of Organization X determined that the contracting individuals have not been trained in security areas.

This would be a training gap.
Worked Example

Step 2

• Identify the functions, using Appendix A
• Outcomes are also listed in Appendix
  – Learning Objectives(s) should be in the forefront
• Important: Just because a function or role is listed within the appendices; it does not mean that a training course or module must be built for that role.
Function Area: **Oversight, Management and Support**

Role Areas:
- Legal Advice and Advocacy
- Strategic Planning and Policy Development
- Awareness, Education and Training
- Privacy
- Management
- Procurement
- Personnel Security
- Physical and Environmental Security
- Security Program Management

**Definition** — Provides oversight and support so that others may effectively conduct Cybersecurity work.

**Learning Objectives** — An individual should be able to successfully complete one or all of the following, depending on the role(s):

- Provide legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain.
- Advocate legal and policy changes and make a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.
- Apply knowledge of priorities to define an entity’s direction, determine how to allocate resources, and identify programs or infrastructure that are required to achieve desired goals within domain of interest.
- Develop policy or advocate for changes in policy that will support new initiatives or required change/enhancements.
- Conduct training of personnel within pertinent subject domains.
- Develop, plan, coordinate and evaluate training courses, methods, and techniques as appropriate.
- Oversees the security baseline and associated activities of an information system in or outside the network environment.
- Provides contractual, procurement and/or acquisition support for IA purchases.
- Manage IT/cybersecurity implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, policy enforcement emergency planning, security awareness, and other resources.
- Ensures that privacy impact assessments are conducted and appropriate controls are implemented.
- Ensures physical controls are correctly implemented.
- Provides personnel security policies, implements security controls and handles all personnel issues.
Worked Example
Step 3

• Annotate the associated training outcomes and learning objectives
• Appendix C will provide some associated role areas and roles and help shape the learning objectives
• Using the appropriate role, the corresponding knowledge and skills can be identified using Appendix B
Worked Example
Step 3 - Continued

• Role is identified in Appendix C – Tailor to organization

• Role tasks that the employee executes determine the level to which he/she needs to be trained.
  – Contracting Officer has 10 years of experience in contracting, but has only within the last two years moved into IT/Cybersecurity contracting. Therefore, with only two years in IT/Cybersecurity contracting, the employee is at a Competency Level I.

• This competency level determines the Knowledge Units that will be used to develop the training module.
Worked Example
Step 3 - Continued

• Knowledge Unit is based on the competencies identified for that role and the knowledge and skills required to successfully execute the activities associated with the role.

• In addition to the Competency levels, the functional perspective of the role must be considered. There are four (4) functional perspectives: Manage, Design, Implement and Evaluate.
**Function Area:** Oversight, Management and Development

**Role Area:** Procurement

**Roles:**
- Authorizing Official
- Acquisition Official
- Procurement Officer
- Management
- Contracting Officers
- System Owner
- Mission/Business Owner
- Program Manager
- Project Manager
- Budgeting Officer

**Responsibility** – Procures resources as needed. Develops and executes contracts to include security controls. Ensures deliverables are compliant with Federal and Organizational security control requirements.

**Knowledge Units:**
- Procurement
- Management
- Compliance

<table>
<thead>
<tr>
<th>Knowledge Unit</th>
<th>All</th>
<th>Manage</th>
<th>Design</th>
<th>Implement</th>
<th>Evaluate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement</td>
<td>PROC 1 - 2</td>
<td>PROC 6 - 9</td>
<td>PROC-11 - 12</td>
<td>N/A</td>
<td>PROC-3 - 9</td>
</tr>
<tr>
<td>Management</td>
<td>PM-37</td>
<td>PM-1 - 4</td>
<td>PM-8</td>
<td>PM-10</td>
<td>PM-12</td>
</tr>
<tr>
<td>Compliance</td>
<td>COMP-1</td>
<td>COMP-3 - 5</td>
<td>COMP-7</td>
<td>COMP-2 - 5</td>
<td></td>
</tr>
</tbody>
</table>
Worked Example
Step 3 - Continued

• After the function and role area have been identified, review Appendix B

• Using our example, PROC-6 means that the training module should provide the employee with knowledge about how to execute secure acquisitions.
<table>
<thead>
<tr>
<th>PROC</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROC-1</td>
<td>Knowledge of applicable business processes and operations of customer organizations</td>
</tr>
<tr>
<td>PROC-2</td>
<td>Knowledge of capabilities and requirements analysis</td>
</tr>
<tr>
<td>PROC-3</td>
<td>Knowledge of system software and organizational design standards, policies, and authorized approaches relating to system design</td>
</tr>
<tr>
<td>PROC-4</td>
<td>Skill in conducting capabilities and requirements analysis</td>
</tr>
<tr>
<td>PROC-5</td>
<td>Skill in interpreting and translating customer requirements into operational cyber actions</td>
</tr>
<tr>
<td>PROC-6</td>
<td>Knowledge of secure acquisitions</td>
</tr>
<tr>
<td>PROC-7</td>
<td>Knowledge of Export Control regulations and responsible Federal Organizations for the purposes of reducing supply chain risk</td>
</tr>
<tr>
<td>PROC-8</td>
<td>Knowledge of critical IT procurement requirements</td>
</tr>
<tr>
<td>PROC-9</td>
<td>Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes)</td>
</tr>
<tr>
<td>PROC-10</td>
<td>Skill in evaluating the trustworthiness of the supplier and/or product</td>
</tr>
<tr>
<td>PROC-11</td>
<td>Knowledge of processes to allocate resources in business process planning</td>
</tr>
<tr>
<td>PROC-12</td>
<td>Skill in ensuring the proper allocations of resources in business process planning</td>
</tr>
</tbody>
</table>
Worked Example
Step 4

• Tailor the training module to the appropriate level of expertise for the audience.
• Tailor also for your particular organization

Now the training modules can be developed
Worked Example
Step 4 - Continued

• The employee is trained specifically to his/her role as well as the corresponding responsibilities of that role.
  – Keep in mind the competency level

• Remember, as the training module is developed, these knowledge and skills must be included with the outcome as defined for the function.
Worked Example

Evaluations

• Appendix D provides samples forms to assist with evaluating the training
• Any areas of training that were confusing or did not provide the desired outcome can be identified through the evaluation process
• Areas identified need to be improved prior to the next training session
<table>
<thead>
<tr>
<th>Evaluation Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Levels of Evaluation Student</td>
</tr>
<tr>
<td>Type of Training</td>
</tr>
<tr>
<td>Training</td>
</tr>
<tr>
<td>Education</td>
</tr>
</tbody>
</table>
Sample Questionnaire — Level 1 Evaluation Training Assessment by Student

1. Indicate your highest level of education:
   - High School graduate or less
   - Bachelor's Degree
   - Some college/technical school
   - Master's Degree
   - Associate degree or technical certification
   - Doctorate

2. Indicate the total number of courses you have completed in subject areas related to this training:
   - 0
   - 1-4
   - 5-10
   - 11-15
   - More than 15

3. Indicate how long it has been since you took a course in the subject area of this training:
   - This is my first course in this subject
   - Less than 1 year
   - 1-3 years
   - 4-6 years
   - More than 6 years

4. Indicate the extent of your work experience in the general subject areas of this training:
   - None
   - Less than 1 year
   - 1-3 years
   - 4-6 years
   - More than 6 years

5. For my preparation and level of knowledge, the training was:
   - Too elementary
   - Somewhat elementary
   - Somewhat difficult
   - About right
   - Too difficult

6. The pace at which the subject matter was covered was:
   - Too slow
   - Somewhat slow
   - Somewhat fast
   - About right
   - Too fast

7. For what I got out of this training, the workload was:
   - Light
   - About right
   - Heavy

8. Considering my previous experience with this subject matter, the course content was:
   - Out of date
   - Somewhat current
   - Current
Tailoring

• Concentrate the training on the skill and knowledge areas that are harder to grasp
• Concentrate on those areas that have been identified as weak
• Use organizational terms
• Adjust skills/knowledge as needed to meet specific organizational roles
• The purpose is to keep the audience engaged in the training.
Participate

Public Review and Comment
March 14 – April 30, 2014

– csrc.nist.gov/publications/drafts
– sp80016-comments@nist.gov
Contact Information

Pat Toth
(301) 975-5140
patricia.toth@nist.gov