**NIST 800\_16 Revision 3: A Role-Based Model for Federal Information Technology/ Cybersecurity Training**

Kirkpatrick model

Graphical user interface, text, application, letter, email

Description automatically generated

Role Based Training

<https://csrc.nist.gov/CSRC/media/Publications/sp/800-16/rev-1/draft/documents/sp800_16_rev1_3rd-draft.pdf>

Learning is a continuum; it starts with awareness, builds to training, and evolves into education. The  
Cybersecurity Learning Continuum provides context and the relationship between Security Awareness,  
Cybersecurity Essentials, Training and Education. The Learning Continuum demonstrates that  
Awareness and Cybersecurity Essentials form the fundamental baseline required for all individuals  
involved with the management, operation, maintenance, development or use of IT systems, information  
technology and cybersecurity. It also demonstrates that the training and education levels are more  
selective, based on a role and responsibility.

Diagram

Description automatically generated

**NIST 800-50: Building an Information Technology Security Awareness and Training Program**

**Needs assessment**

The matrix is organized by six role categories – or functional specialties – relative to three fundamental training content categories – or training areas (i.e., laws and regulations, security program, and system life cycle security). The six role categories or functional specialties are:

* Manage – This category is for individuals who manage IT-based functions in an organization.
* Acquire – This category is for those individuals who are involved in the acquisition of IT products and/or services (e.g., serve on a source selection board to evaluate vendor proposals for IT systems). This is especially important for those who serve as a contracting officer’s technical representative (COTR).
* Design and Develop – This category is for those individuals who design and develop systems and applications.
* Operate – This category is for those individuals who operate (administer) IT systems (e.g., webservers, e-mail servers, file servers, LANs, WANs, mainframes).
* Review and Evaluate – This category is for individuals who review and evaluate (audit) IT functions as part of an organization’s internal controls program, internal review, or an external audit program (e.g., inspector general).
* Use – This category is for individuals who access IT resources and/or use IT to do their jobs.

**Training Plan**

* Existing national and local policy that requires the awareness and training to be accomplished;
* Scope of the awareness and training program;
* Roles and responsibilities of agency personnel who should design, develop, implement, and maintain the awareness and training material, and who should ensure that the appropriate users attend or view the applicable material;
* Goals to be accomplished for each aspect of the program (e.g., awareness, training, education,professional development [certification]);
* Target audiences for each aspect of the program;
* Mandatory (and if applicable, optional) courses or material for each target audience;
* Learning objectives for each aspect of the program;
* Topics to be addressed in each session or course;
* Deployment methods to be used for each aspect of the program;
* Documentation, feedback, and evidence of learning for each aspect of the program;
* Evaluation and update of material for each aspect of the program
* Frequency that each target audience should be exposed to material.

**Establishing Priority**

Following roles should be addressed in terms of any special training needs:

* Executive Management – Organizational leaders need to fully understand directives and laws that form the basis for the security program. They also need to comprehend their leadership roles in ensuring full compliance by users within their units.
* Security Personnel (security program managers and security officers) – These individuals act as  
  expert consultants for their organization and therefore must be well educated on security policy and accepted best practices.
* System Owners – Owners must have a broad understanding of security policy and a high degree of understanding regarding security controls and requirements applicable to the systems they manage.
* System Administrators and IT Support Personnel – Entrusted with a high degree of authority over  
  support operations critical to a successful security program, these individuals need a higher degree of technical knowledge in effective security practices and implementation.
* Operational Managers and System Users – These individuals need a high degree of security  
  awareness and training on security controls and rules of behavior for systems they use to conduct business operations.

**Developing Awareness Training Material**

“What behavior do we want to reinforce?” (awareness); and  
“What skill or skills do we want the audience to learn and apply?” (training).

Awareness Topics

* Password usage and management – including creation, frequency of changes, and protection
* Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions
* Policy – implications of noncompliance
* Unknown e-mail/attachments
* Web usage – allowed versus prohibited; monitoring of user activity
* Spam
* Data backup and storage – centralized or decentralized approach
* Social engineering
* Incident response – contact whom? “What do I do?”
* Shoulder surfing
* Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
* Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization)
* Personal use and gain issues – systems at work and home
* Handheld device security issues – address both physical and wireless security issues
* Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance
* Laptop security while on travel – address both physical and information security issues
* Personally owned systems and software at work – state whether allowed or not (e.g., copyrights)
* Timely application of system patches – part of configuration management
* Software license restriction issues – address when copies are allowed and not allowed
* Supported/allowed software on organization systems – part of configuration management
* Access control issues – address least privilege and separation of duties
* Individual accountability – explain what this means in the organization
* Use of acknowledgement statements – passwords, access to systems and data, personal use and gain
* Visitor control and physical access to spaces – discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity
* Desktop security – discuss use of screensavers, restricting visitors’ view of information on screen (preventing/limiting “shoulder surfing”), battery backup devices, allowed access to systems
* Protect information subject to confidentiality concerns – in systems, archived, on backup media, in hardcopy form, and until destroyed
* E-mail list etiquette – attached files and other rules.

**Training Material Delivery**

Techniques for effectively delivering training material should take advantage of technology that supports  
the following features:

* Ease of use (e.g., easy to access and easy to update/maintain);
* Scalability (e.g., can be used for various audience sizes and in various locations);
* Accountability (e.g., capture and use statistics on degree of completion);
* Broad base of industry support (e.g., adequate number of potential vendors, better chance of  
  finding follow-on support).

**Feedback and Success Indicators**

* Monitoring compliance
* Diagram

  Description automatically generated
* Program Success indicators