

NIST Role-based Training Guideline: SP 800-16, Rev. 1 It's a Draft; It's Alive!

Mark Wilson, CISSP
Computer Security Division
National Institute of Standards and Technology

- March 24, 2009 -

mark.wilson@nist.gov

(301) 975-3870 (voice)

<http://csrc.nist.gov/>

Awareness and Training Policy Drivers

- FISMA (Federal Information Security Management Act) [2002]
- OMB Circular A-130 Appendix III [2000]
- OPM 5 CFR Part 930 [June 2004]
- Computer Security Act of 1987

Document Drivers

- Two Audiences: Information Security and Training Development (Instructional Design) Professionals
- “Harmonization” Efforts:
 - NSA’s CNSS training standards
 - DHS’ Essential Body of Knowledge
 - OPM’s 2210 Series Training Topics/Competencies
 - CIO Council’s IT Workforce Committee (Matrix)
 - DOD’s 8570 Training and Certification Program
 - Intel. Community’s Cyber Security Training Program
 - ISS LOB Tier 2 Role-based Training Initiative
 - CNCI Cyber Education Efforts

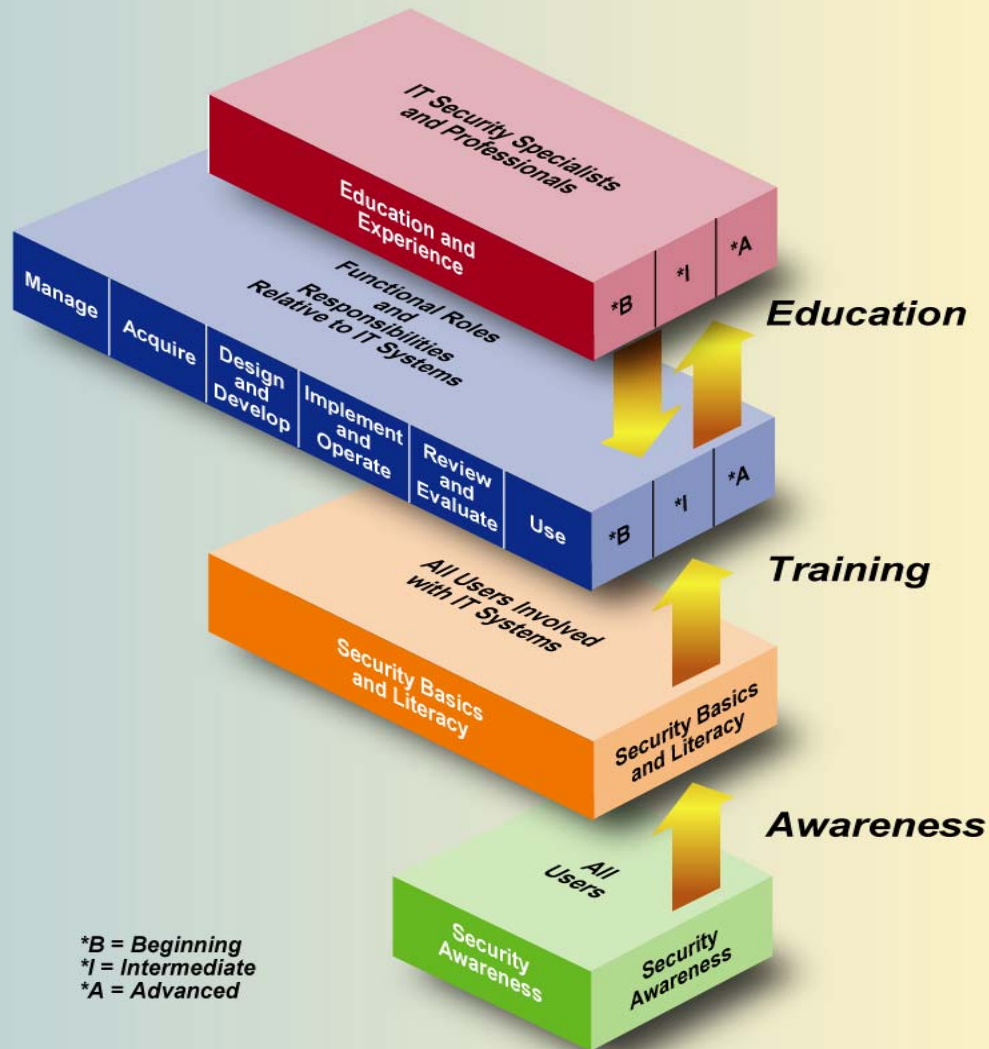
Training Requirements Vs. Options

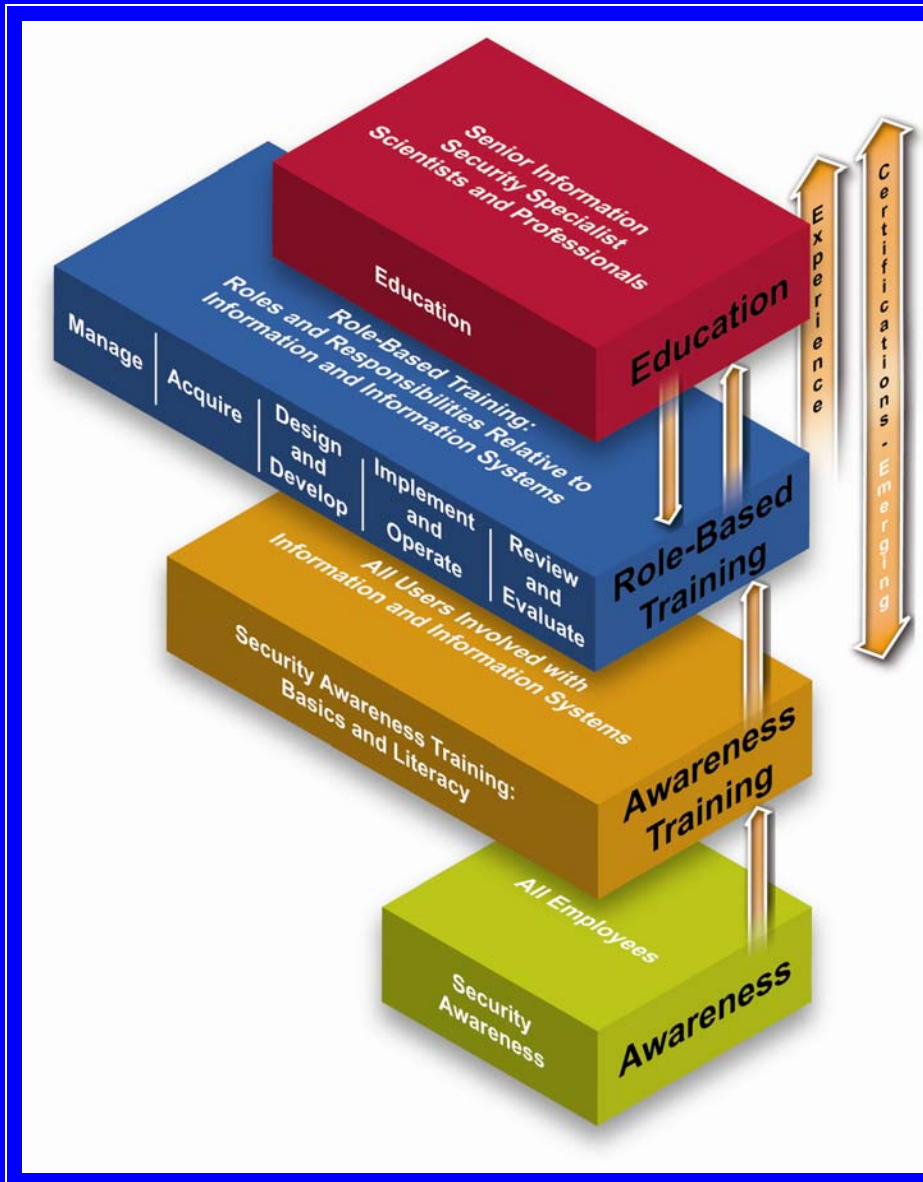
- Requirements:
 - Identify people with significant responsibilities for information security
 - Train them
- Options:
 - Number of roles to use
 - Build a course or module
 - Presentation mode (e.g., instructor-led, technology-based, incorporate avatars)
 - Order of content in course or module
 - Topics and elements

The Rules

- Rule #1: Identify people with significant responsibility for information security
- Rule #2: Do not open SP 800-16, Rev. 1 until organization has identified people with significant responsibility for information security
- Rule #3: The list of roles in SP 800-16, Rev. 1 is a catalog; use what you need and do not use what you do not need

The NIST Model Used In SPs 800-50, 800-100





The Learning
Continuum
(aka, The
NIST Model)
In Draft
Special
Publication
800-16,
Rev. 1




A New Look: “Awareness” Versus “Awareness Training”

- In current NIST guidelines: “awareness” equals “awareness training”
- In Draft SP 800-16, Rev. 1:
 - “Awareness” is limited to . . .
 - “Awareness training” equals “Basics and Literacy”
- Impact of OMB’s ISS LOB Tier 1 Awareness Training Initiative

Awareness and Training Relationships



Awareness and Training Relationships

Role-Based Training:	Role-Based Training:	Role-Based Training:	Role-Based Training:	Role-Based Training:	Role-Based Training:
Truck Driver	Cab Driver	Bus Driver	Indy Car Racer	Drag Racer	Road Racer
					

Driver Education (Driver Training): Basics and Literacy
Target Audience = All Vehicle Drivers

Driving Safety Awareness: Target Audience = All Citizens
Use Seat Belts, Look Both Ways Before Crossing The Street

Rev. 1 Key Thoughts/Goals

- Role matrices are starting points, not mandatory
- Rev. 1 to be supported by follow-on web-based “reference model” [on our CSRC]
- Initial course outline on web = a starting point
- “Scoping guidance”
 - Needs assessment
 - Job task analysis
 - ADDIE Model
 - Tailor role matrices, topics and elements to meet your organization’s and audiences’ needs

Questions? Comments?
- Thank You -

Mark Wilson, CISSP
Computer Security Division
National Institute of Standards and Technology
mark.wilson@nist.gov
(301) 975-3870 (voice)