Building an IT Security Awareness & Training Program

Mark Wilson, CISSP

Computer Security Division, ITL

National Institute of Standards and Technology

- March 6, 2003 -

mark.wilson@nist.gov

(301) 975-3870 (voice) (301) 948-1233 (fax)

http://csrc.nist.gov/

Cornerstones for Success

- Policy
- Roles and Responsibilities
  - CIO
  - IT Security Program Manager
  - Managers (and Their Contractors)
  - Users
- Budget
- Management Support . . . Commitment

A Life-cycle Approach

- Design
- Develop
- Implement
- Maintain

What Do We Mean By . . . ?

- Awareness is Not Training; Training is Not Awareness!
  - The purpose of **awareness** presentations is *simply to focus attention on security . . . allow individuals to recognize IT security concerns and respond accordingly . . . change attitudes and behavior.*
  - **Training** strives to *produce relevant and needed security skills and competencies.*

What Do We Mean By . . . ?

- In awareness activities the learner receives information; in training the learner has a more active role.
- Awareness relies on reaching broad audiences with a single message (or several messages); training is more formal, with a goal of building knowledge and skills to facilitate job performance.

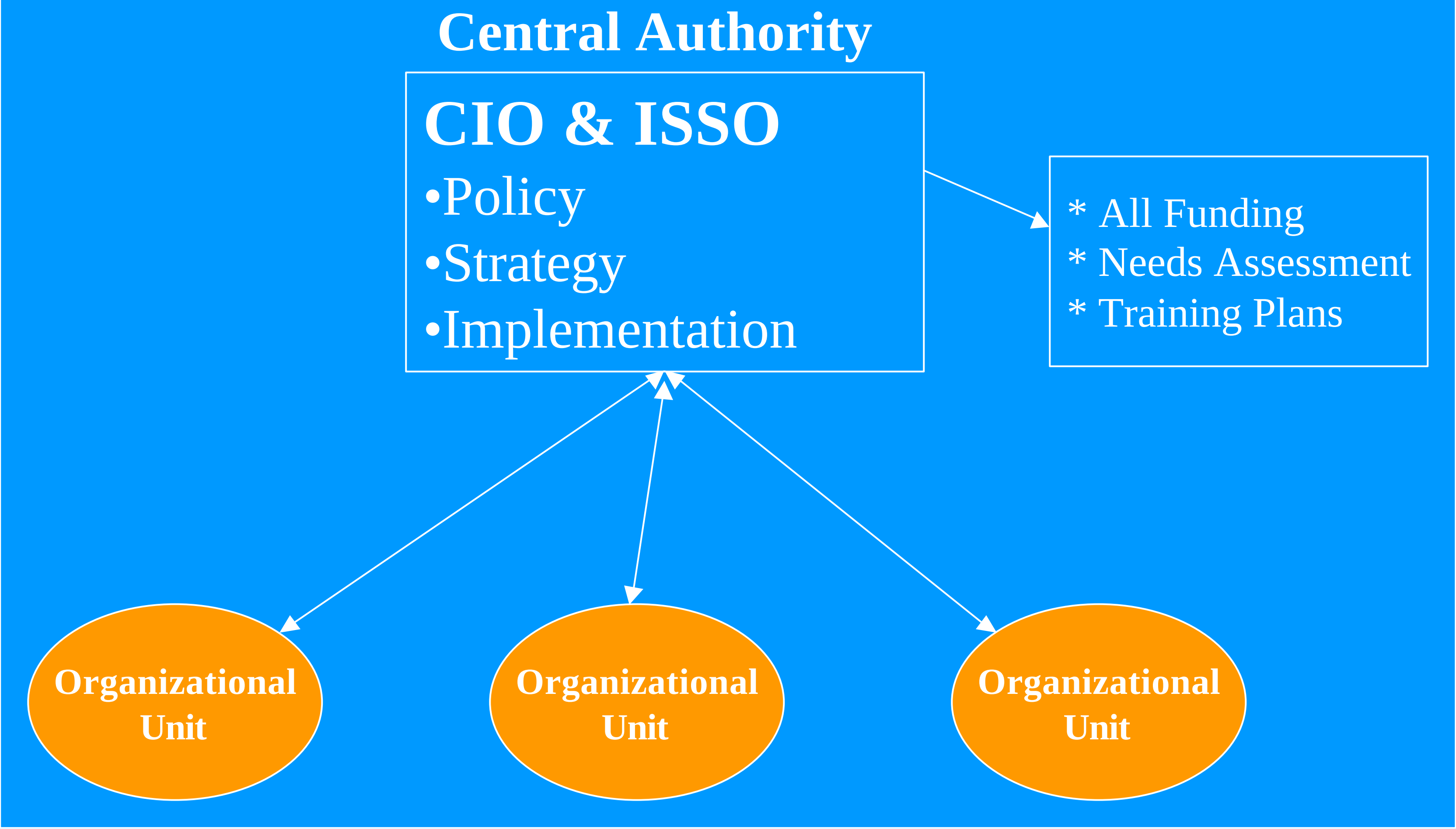
Designing Your Awareness & Training Program

- Determine Organization’s Needs
  - – Needs Assessment
  - – Incorporating Results of Program Reviews
- Build a Strategy
- Develop an Awareness and Training Plan
  - – Identify Audiences; Scope Needs; Establish Priorities; Set the Bar; Get Mgmt/Org Buy-in!

Designing Your Awareness & Training Program

- Strategy Depends on Agency’s Structure and Management Model
- Some Common Models or Approaches
  - Centralized Program Management Model
  - Partially Decentralized Program Management Model
  - Fully Decentralized Program Management Model

Centralized Program Management Model



Central Authority

CIO & ISSO

- Policy
- Strategy
- Implementation

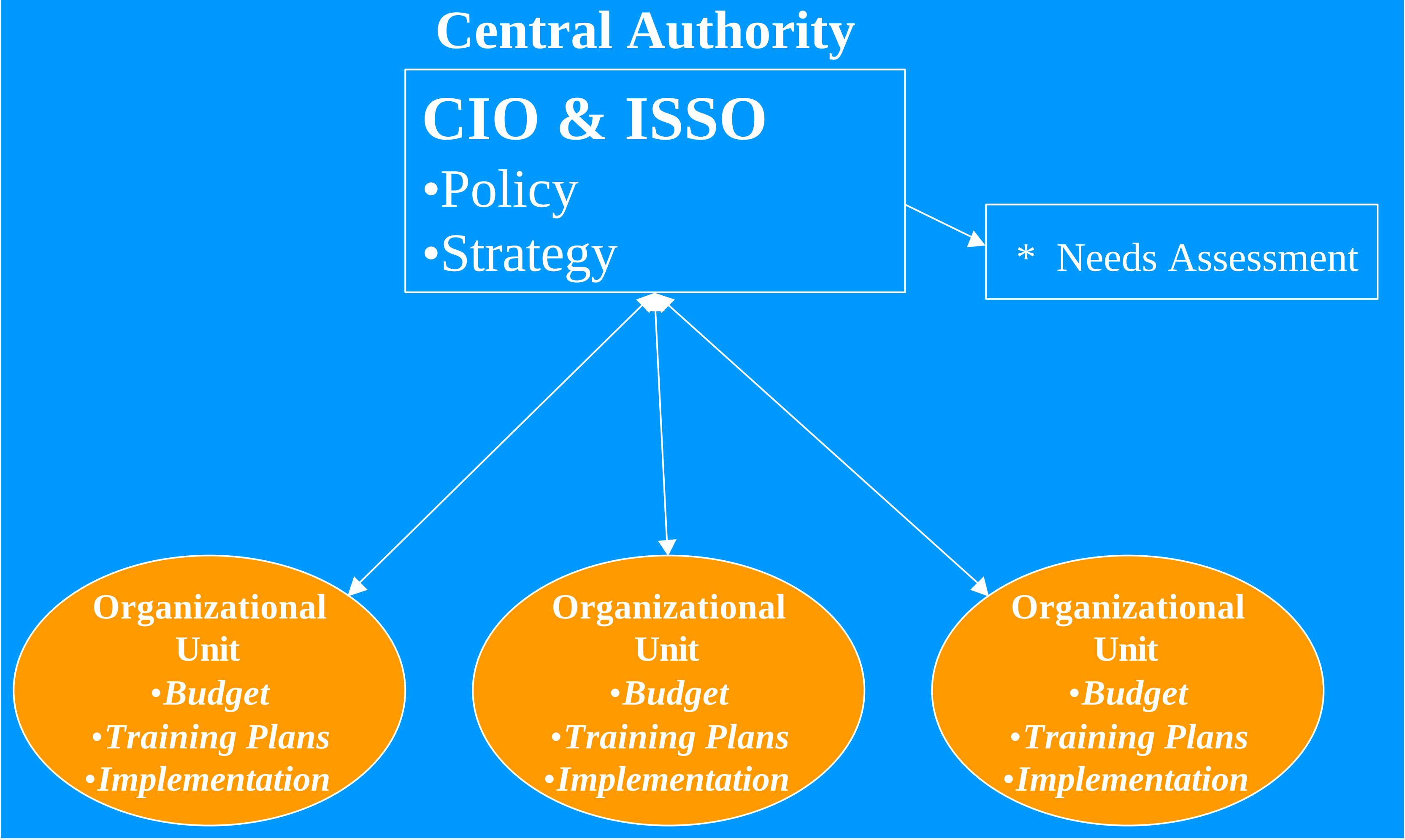
* All Funding
* Needs Assessment
* Training Plans

Organizational Unit

Organizational Unit

Organizational Unit

Partially Decentralized Program Management Model



Central Authority

CIO & ISSO

- Policy
- Strategy

* Needs Assessment

Organizational Unit

- ***Budget***
- ***Training Plans***
- ***Implementation***

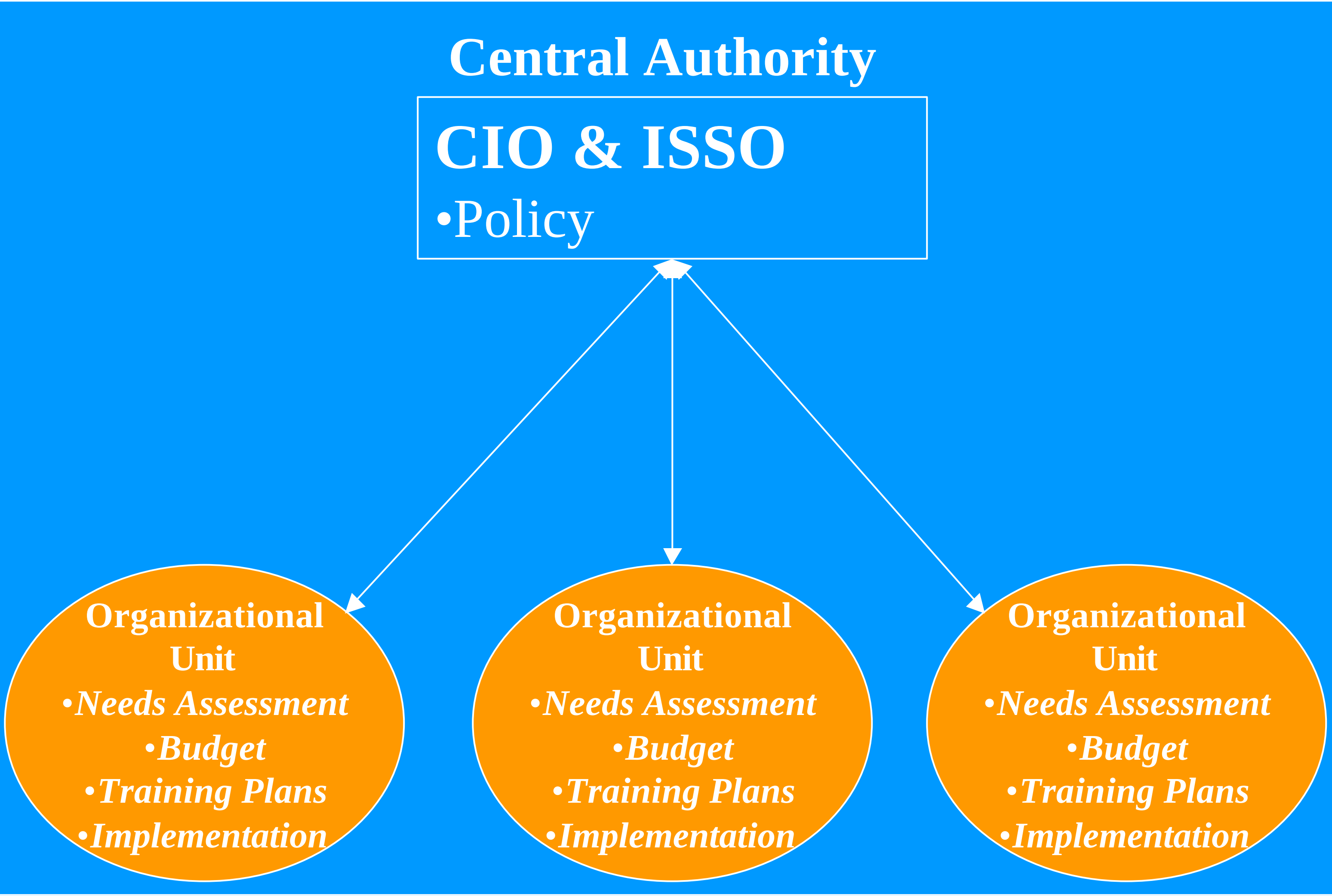
Organizational Unit

- ***Budget***
- ***Training Plans***
- ***Implementation***

Organizational Unit

- ***Budget***
- ***Training Plans***
- ***Implementation***

Fully Decentralized Program Management Model



Central Authority

CIO & ISSO

- Policy

Organizational Unit

- ***Needs Assessment***
- ***Budget***
- ***Training Plans***
- ***Implementation***

Organizational Unit

- ***Needs Assessment***
- ***Budget***
- ***Training Plans***
- ***Implementation***

Organizational Unit

- ***Needs Assessment***
- ***Budget***
- ***Training Plans***
- ***Implementation***

Designing Your Awareness & Training Program

- Model or Approach is Dependent on:
  - Organization Size
  - Defined Roles and Responsibilities
  - Budget Allocations and Authority

Developing Your Awareness & Training Material

- Policy and Guidance Issues
  - Your Program is Dependent on Policy
  - Computer Security Act
  - OMB Circular A-130, Appendix III
  - FISMA
  - Department & Agency Policy
  - NIST Guidelines - http://csrc.nist.gov

Developing Your Awareness & Training Material

- Developing Awareness Material: Samples
  - Password Usage/Creation/Changes
  - Protection From Viruses - Scanning and Updating
  - PDA Security Issues
  - Laptop Security While on Travel
  - Personal Use and Gain Issues
  - Software Patches & Security Settings on Client Systems
  - Software License Restriction Issues
  - Social Engineering

Developing Your Awareness & Training Material

- Developing Awareness Material: Sources
  - E-mail Advisories
  - On-line IT Security Daily News Websites
  - Periodicals
  - http://csrc.nist.gov/ATE
  - http://csrc.nist.gov/fissea
    - Previous Conference Presentations
    - Future Repository of Awareness and Training Material

Developing Your Awareness & Training Material

- Developing Training Material: Sources
  - In-house
  - Contractors/Vendors
  - Mix of In-house and Contractor Support
  - http://csrc.nist.gov/ATE . . .
  - NIST Special Publication 800-16
  - DoD/DISA

Implementing Your Awareness & Training Material

- Messages on Trinkets: e.g., Key Fobs, Post-it Notes, Notepads, First Aid Kits, Clean-up Kits, Diskettes With a Message, Frisbees, “Gotcha” Cards
- Posters
- Access (to My PC) Lists
- “Do and Don’t” Lists
- Screensavers, Warning Banners/Messages

Implementing Your Awareness & Training Material

- Newsletters
- Desk-to-desk Alerts
- Organization-wide E-mail Messages
- Videotapes
- Web-based Sessions
- Organization’s IT Security Homepage
- Computer Security Day

Implementing Your Awareness & Training Material

- Computer-based Sessions
- Teleconferencing Sessions
- In-person, Instructor-led Sessions
- “Brown Bag” Seminars
- Rewards Programs - Plaques, Mugs, Letters of Appreciation . . . All-hands Meetings (Public Humiliation) ;-)

Maintaining Your Awareness & Training Program

- Monitoring Success - Use of Evaluation and Feedback
  - Evaluation Forms (Classroom)
  - Web- and Computer-based Evaluations
  - Pre- and Post-testing
  - Feedback From Management and Users

Maintaining Your Awareness & Training Program

- Managing Change
  - Technological
  - Architectural
  - Organizational
- Raising the Bar

Common Themes in Successful Programs

- Budget = Successful Program
- Defined Roles = Successful Program
- Web-based Material is Very Popular
- Keep Material Interesting and Current
- Movement Toward Professionalization
- Training Plans = Your Program Strategy
- Mix of Awareness and Role-based Training

Questions?

Mark Wilson, CISSP

NIST

mark.wilson@nist.gov

(301) 975-3870 (voice)

(301) 948-1233 (fax)

http://csrc.nist.gov/

http://csrc.nist.gov/ATE

http://csrc.nist.gov/fissea