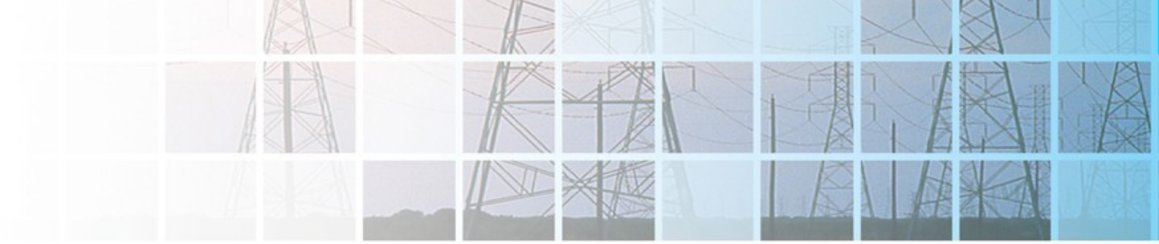


gridSMART℠
from American Electric Power

Addressing Security Issues for the Smart Grid Infrastructure

UCA International Usersgroup

Entergy THE POWER OF PEOPLE™

UtilityAMI

AMI-SEC Task Force Meeting
June 25, 2008
New Orleans, Louisiana

Neil Greenfield, CISSP, CISA
IT Security Engineering

AEP AMERICAN ELECTRIC POWER

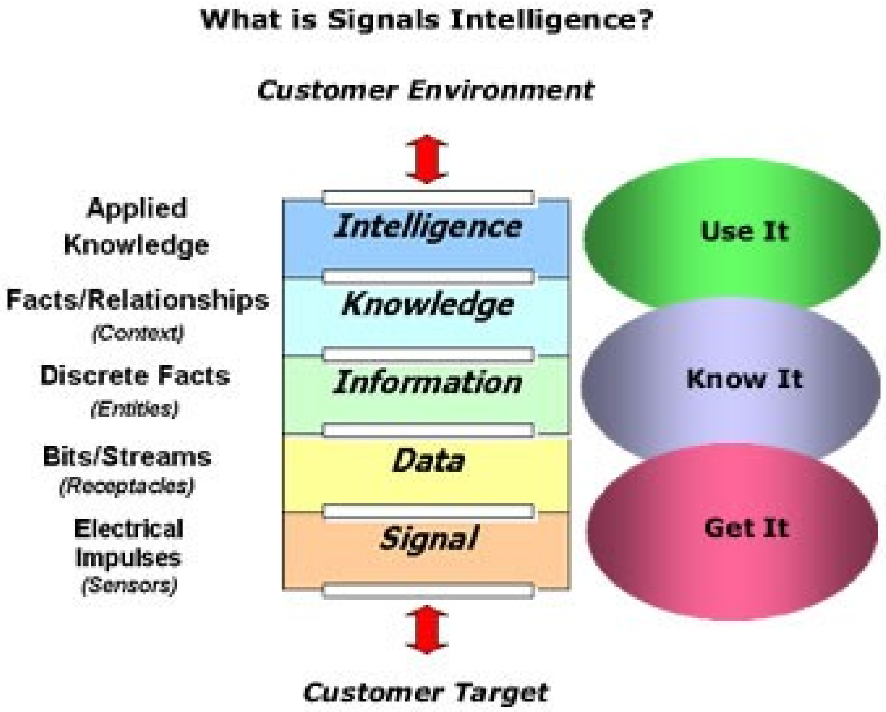
Definition - U.S. Critical Infrastructures

- "...systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters."

  -- USA Patriot Act (P.L. 107-56)

Defense in Depth Focus Areas

- Defend the network and infrastructure
  - Backbone network availability
  - Wireless network security
  - System interconnections
- Defend the enclave boundary
  - Network access protection
  - Remote access
  - Multilevel security
- Defend the computing environment
  - End-user environment
  - Application security
- Supporting infrastructures
  - Key Management Infrastructure
  - Detect and respond


What is Signals Intelligence?
Customer Environment
Applied Knowledge
Facts/Relationships (Context)
Discrete Facts (Entities)
Bits/Streams (Receptacles)
Electrical Impulses (Sensors)
Intelligence
Knowledge
Information
Data
Signal
Use It
Know It
Get It
Customer Target

Security Pieces & Parts

People	Process	Technology
Identity & access management	Information risk management	Network
Information security organization	Policy and compliance framework	Endpoints
Training awareness & personnel	Information asset management	Database
	Business continuity and DR	Application infrastructure
	Physical and environment sec	Systems
	Incident & threat management	Messaging and content
	Systems dev. & ops management	Data

Security Truisms

- **Protection** – Configuring our systems and networks as correctly as possible

- **Detection** – Identify when the configuration has changed or that some network traffic indicates a problem

- **Reaction** – Identify problems quickly, respond to any problem and return to a safe state as rapidly as possible

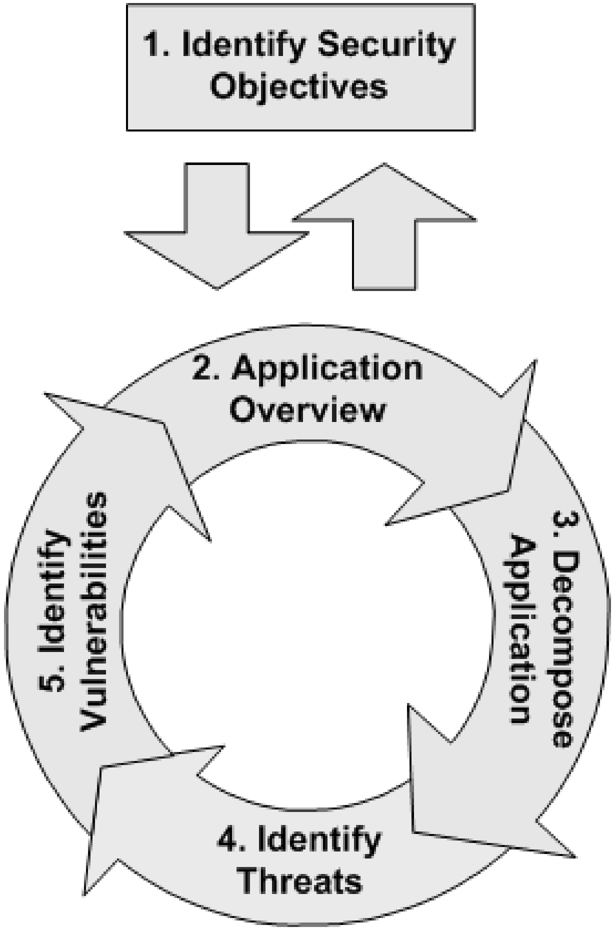
Security Challenges

Reconfigurability and wireless nature may enable:

- Jamming (DoS)
- Device spoofing, configuration of a malicious device (DoS, Tampering)
- Violation of regulatory constraints (DoS)
- Invalid configuration (DoS)
- Eavesdropping, insecure software download (Disclosure, Tampering)
- Exhaustion of system resources (DoS)
- Improper software functionality (Tampering)

Security Threats

- Blunders, errors, and omissions
- Fraud and theft, criminal activity
- Disgruntled employees, insiders
- Curiosity and ignorance, recreational and malicious hackers
- Industrial espionage
- Malicious code
- Foreign espionage and information warfare



Security Mechanism Examples

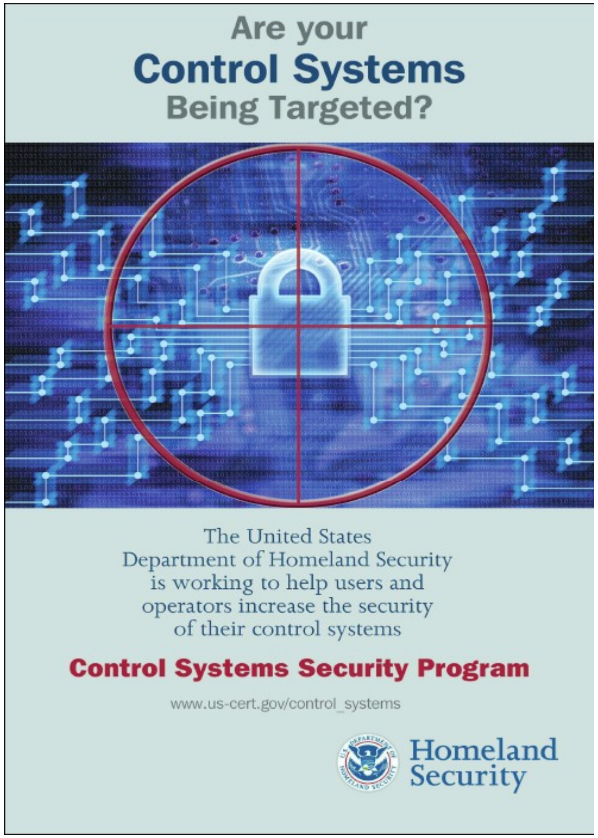
- Jamming – agile spectrum allocation
- Eavesdropping – communication channel encryption
- Internet attacks – firewalls on connection to public network, strong user authentication
- Device spoofing, malfunctioning device, violation of regulatory constraints – secure configuration, remote attestation

Security Requirements

- Prevent loading, installation, instantiation of unauthorized software
- Verify downloaded software from trusted vendor
- Ensure confidentiality and integrity of over-the-air software download and stored data
- Ensure the terminal operates within allowed frequency bands and power levels specified by regulators and power operators
- Provide trusted configuration information to substations on request

DOH – Vision Statement

The Energy Sector envisions a robust, resilient energy infrastructure in which continuity of business and services is maintained through secure and reliable information sharing, effective risk management programs, coordinated response capabilities, and trusted relationships between public and private security partners at all levels of industry and government.



Are your
Control Systems
Being Targeted?

The United States
Department of Homeland Security
is working to help users and
operators increase the security
of their control systems

Control Systems Security Program

www.us-cert.gov/control_systems

Homeland
Security

- National Infrastructure Protection Plan – Energy Sector, 2007

Security Standards Guidelines

- **ANSI/ISA–99.00.01–2007** – Security for Industrial Automation and Control Systems
- **IEC TS 62351** – Power Systems Management and Associated Information Exchange – Data and Communications Security
- **ISO/IEC 13335** – Information technology — Security techniques — Management of information and communications technology security
- **ISO/IEC 21827** – Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM)
- **ITU-T Recommendation X.805** – Security Architecture for Systems Providing End-to-End Communications
- **NIST Special Publication 800-27** – Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- **NIST Special Publication 800-53** – Recommended Security Controls for Federal Information Systems
- Many others………….

Security Tools – More Than Just a Firewall

Management, Audit, Measurement, Monitoring, and Detection Tools

•Log Auditing Utilities
•Virus and Malicious Code Detection Systems
•Intrusion Detection Systems
•Vulnerability Scanners
•Forensics and Analysis Tools (FAT)
•Host Configuration Management Tools
•Automated Software Management Tools

Authentication and Authorization Technologies

•Role-Based Authorization Tools
•Password Authentication
•Challenge/Response Authentication
•Physical/Token Authentication
•Smart Card Authentication
•Biometric Authentication
•Location-Based Authentication
•Password Distribution and Management Technologies
•Device-to-Device Authentication

Filtering/Blocking/Access Control Technologies

•Network Firewalls
•Host-based Firewalls
•Virtual Networks

Physical Security Controls

•Physical Protection
•Personnel Security

Encryption Technologies and Data Validation

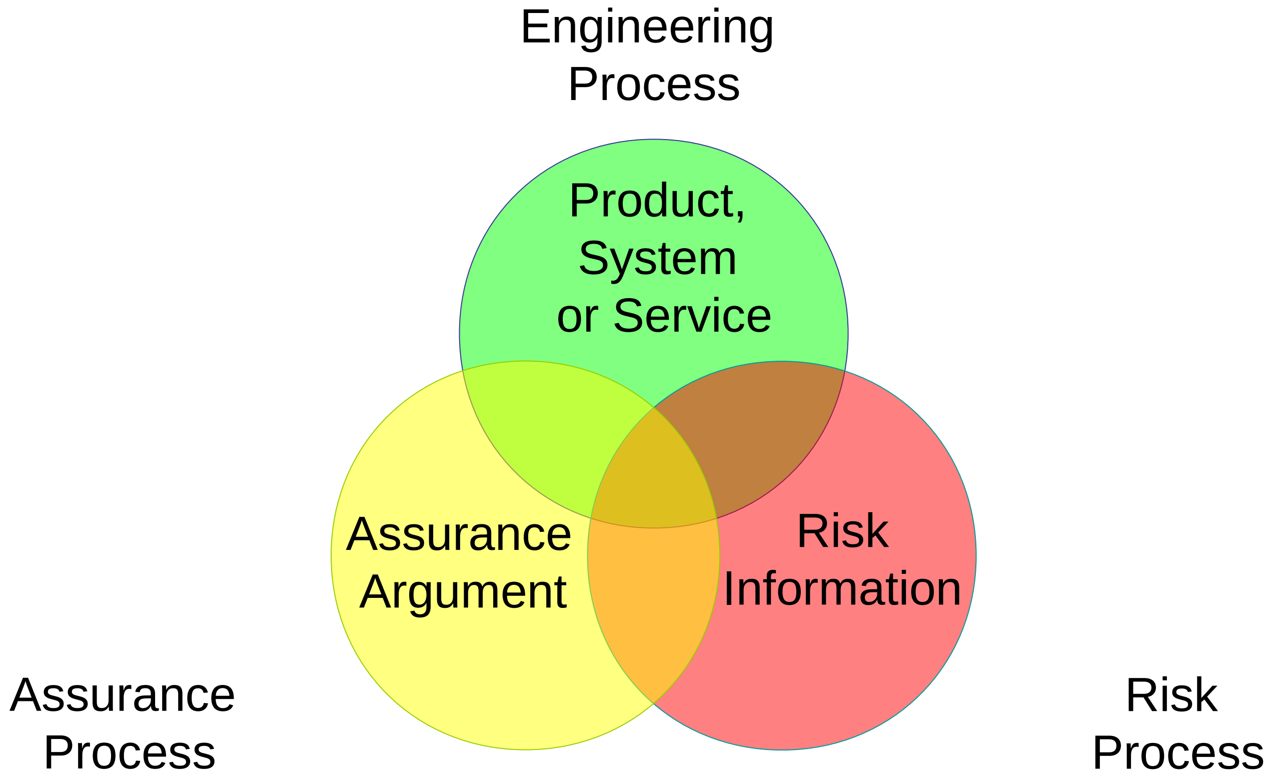
•Symmetric (Secret) Key Encryption
•Public Key Encryption and Key Distribution
•Virtual Private Networks (VPNs)

Industrial Automation and Control Systems Computer Software

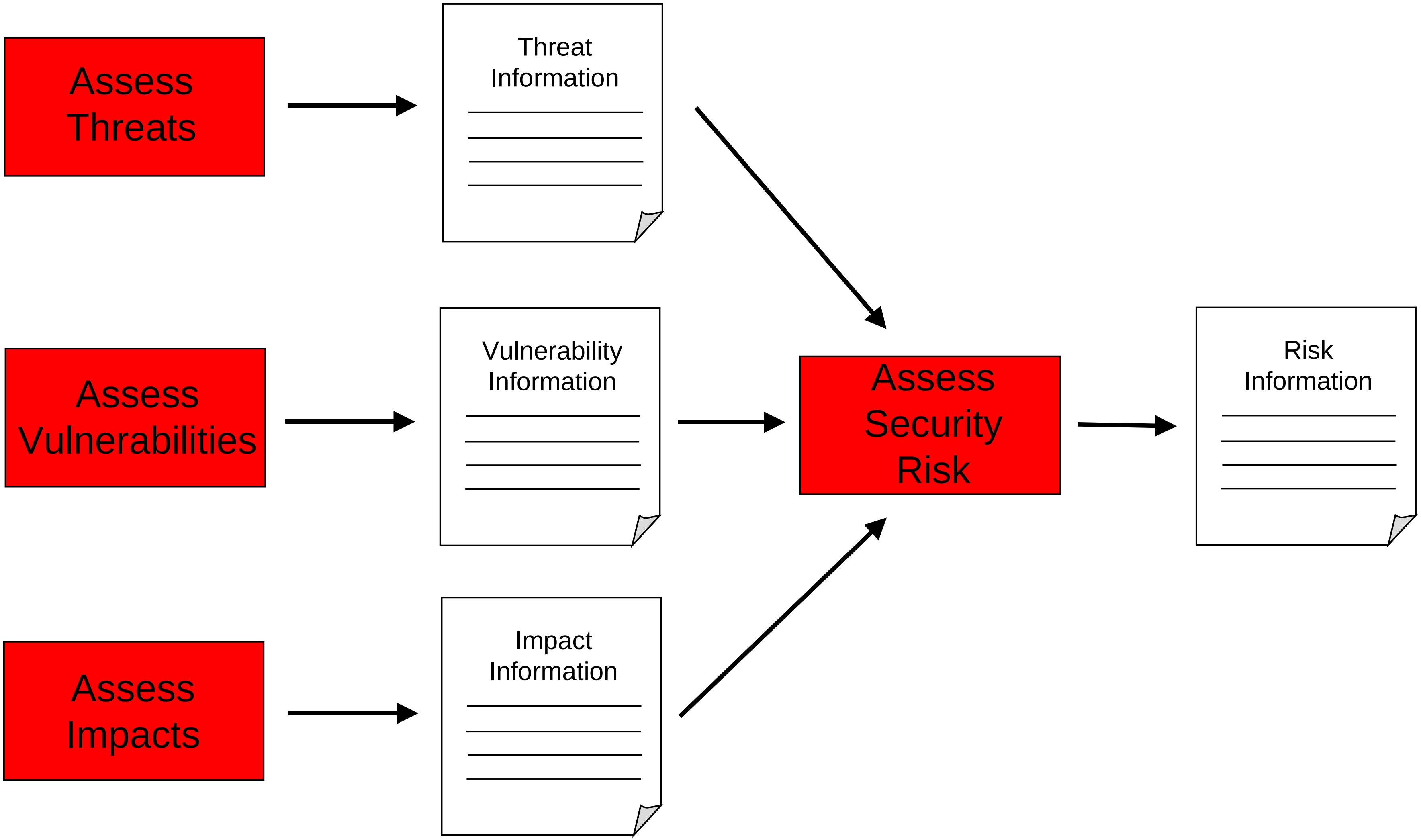
Server and Workstation Operating Systems
Real-time and Embedded Operating Systems
Web Technologies

ISO/IEC 21827 SSE-CMM

International Standard for Systems Security Engineering – Capability Maturity Model (SSE-CMM)



SSE-CMM & Risk Process



Assess Threats

Threat Information

Assess Vulnerabilities

Vulnerability Information

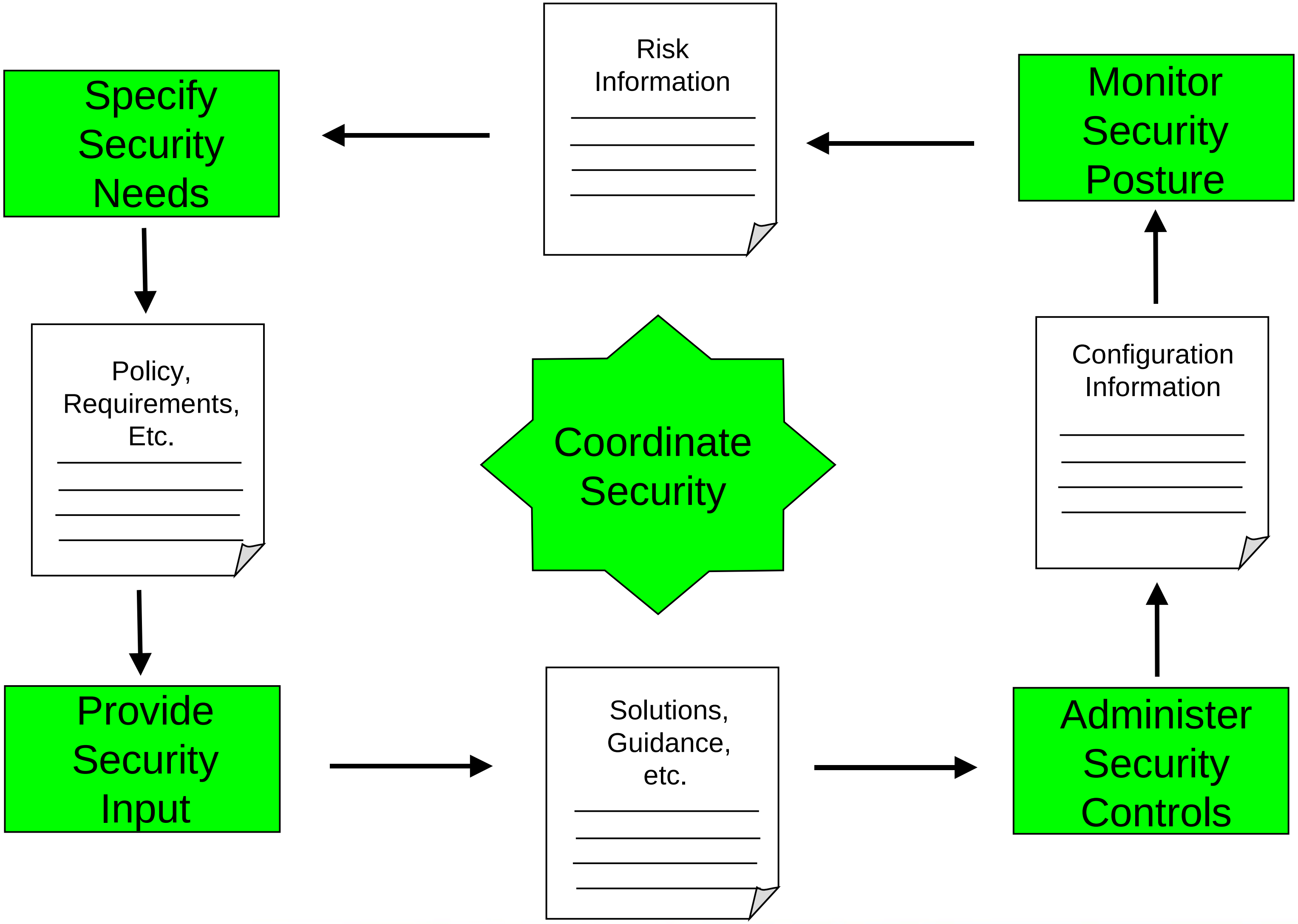
Assess Impacts

Impact Information

Assess Security Risk

Risk Information

SSE-CMM & Engineering Process



Specify Security Needs

Risk Information

Monitor Security Posture

Policy, Requirements, Etc.

Coordinate Security

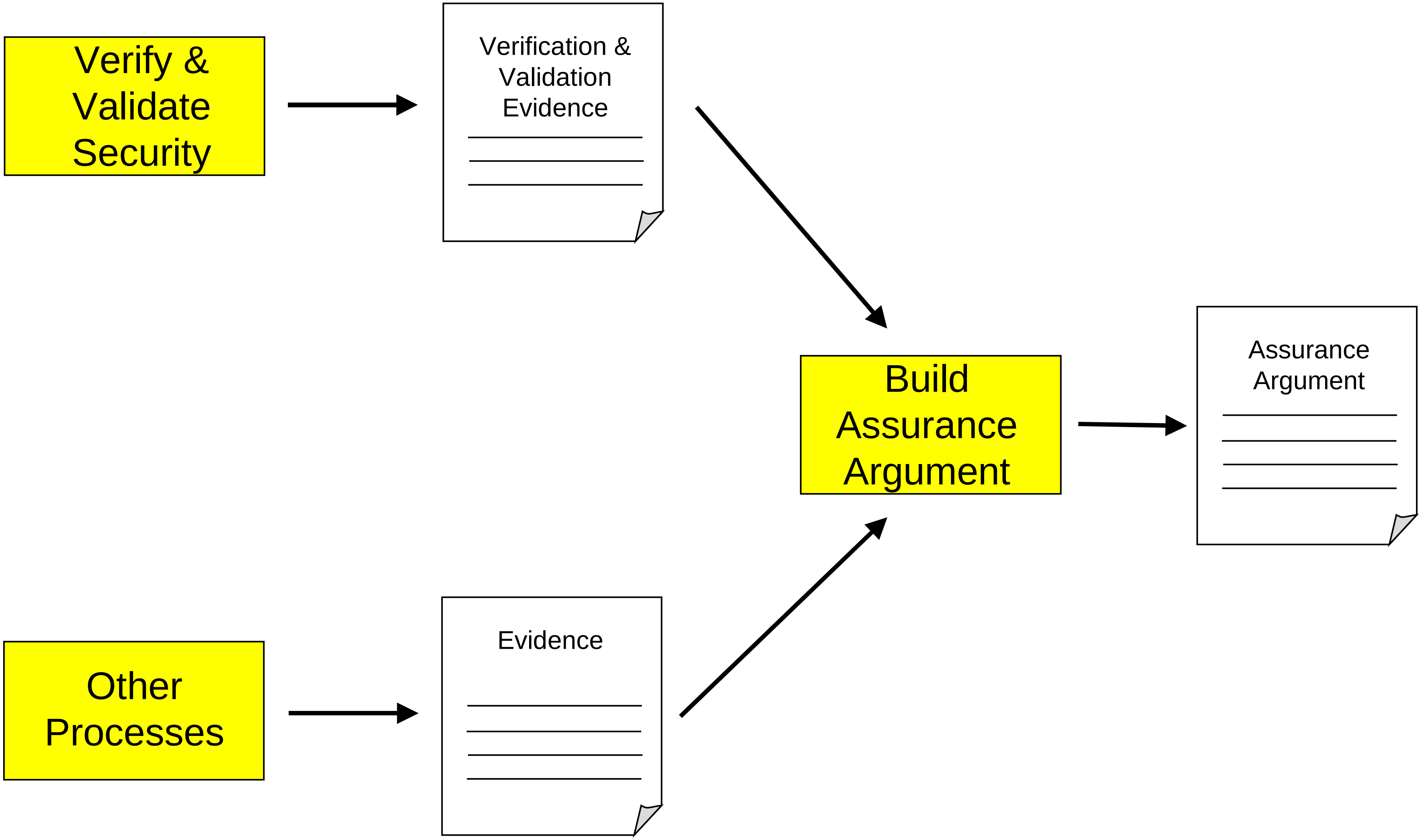
Configuration Information

Provide Security Input

Solutions, Guidance, etc.

Administer Security Controls

SSE-CMM & Assurance Process



Verify & Validate Security

Verification & Validation Evidence

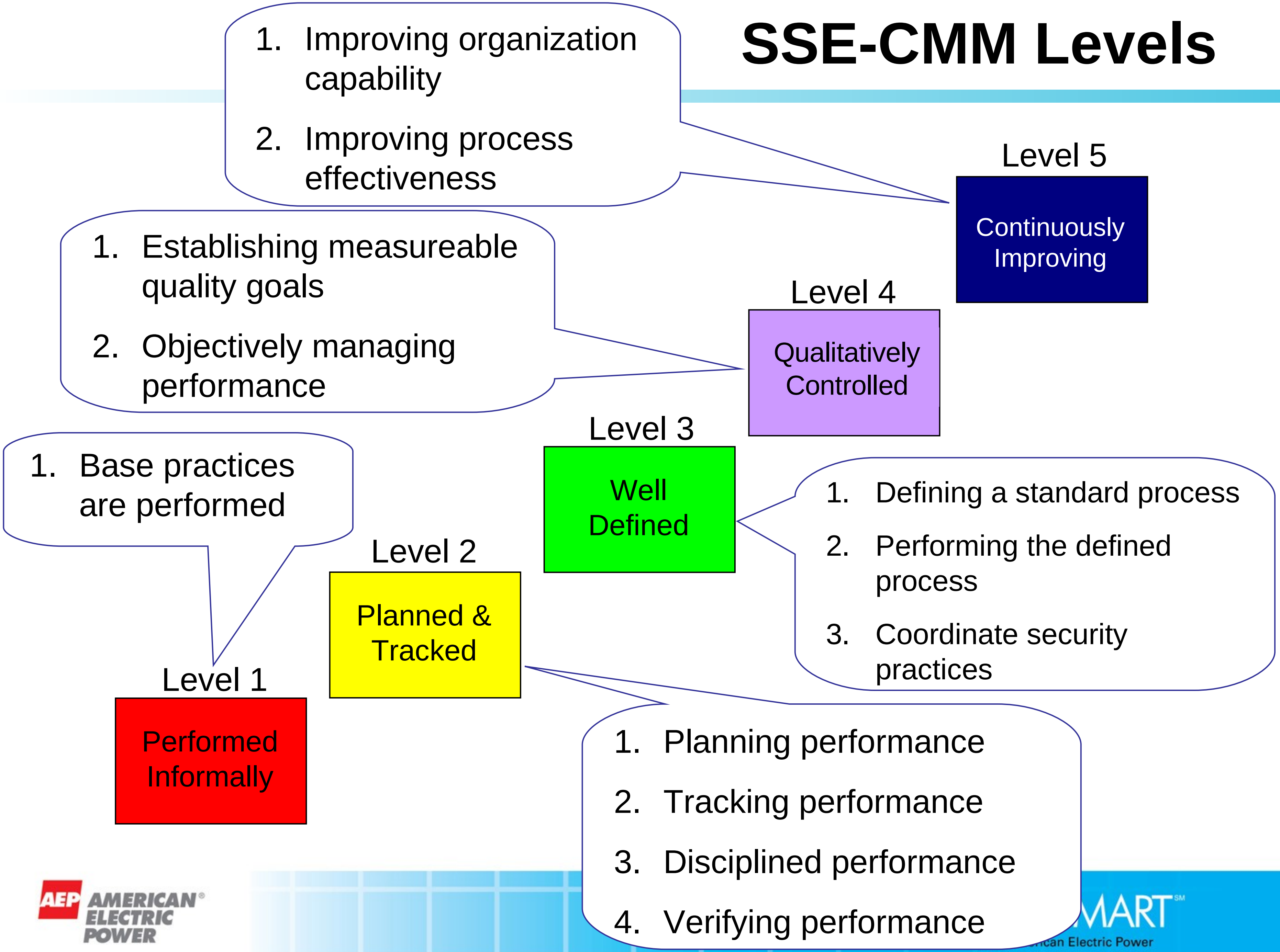
Build Assurance Argument

Assurance Argument

Other Processes

Evidence

SSE-CMM Levels



Level 1

Performed Informally

1. Base practices are performed

Level 2

Planned & Tracked

1. Planning performance
2. Tracking performance
3. Disciplined performance
4. Verifying performance

Level 3

Well Defined

1. Defining a standard process
2. Performing the defined process
3. Coordinate security practices

Level 4

Qualitatively Controlled

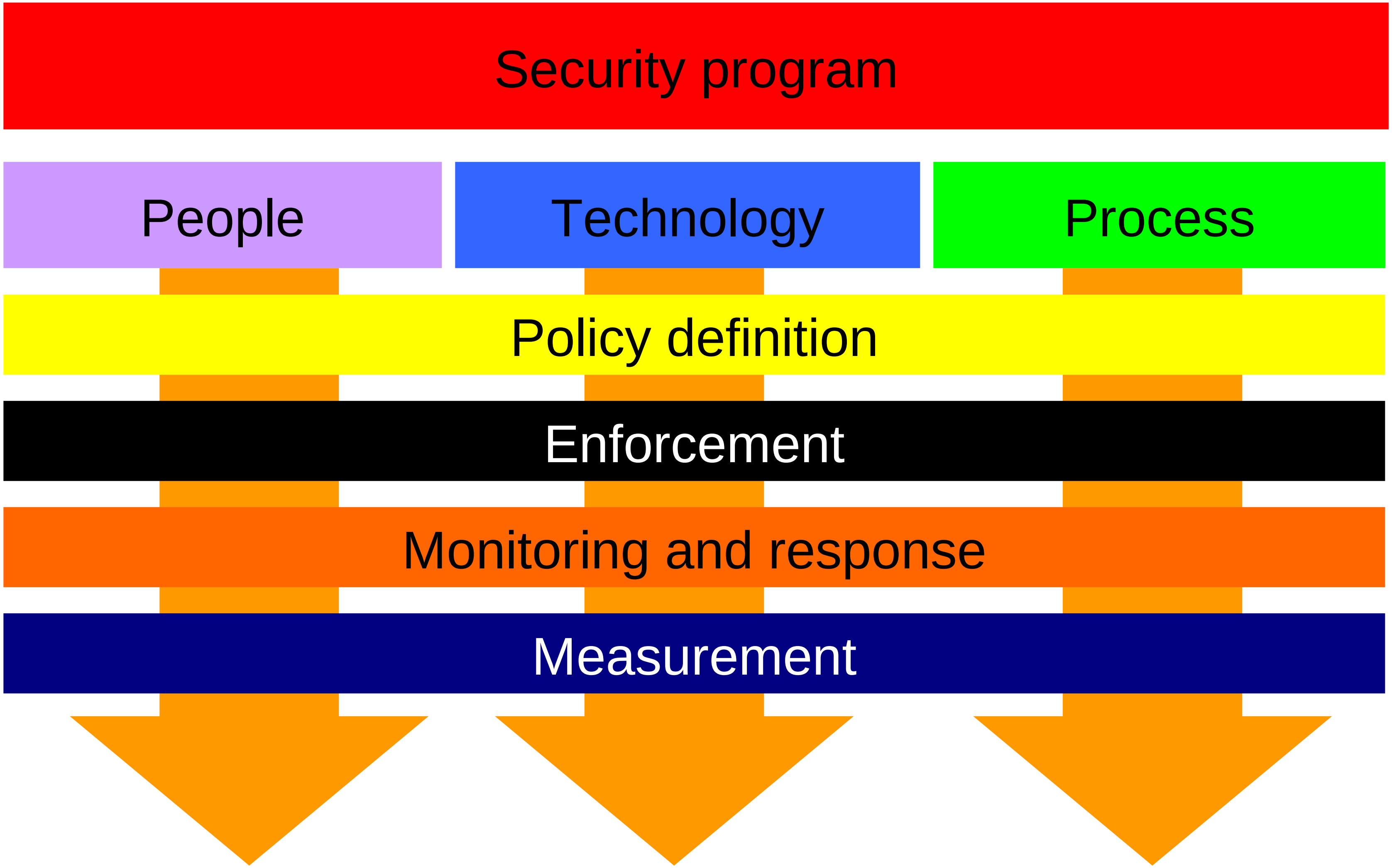
1. Establishing measureable quality goals
2. Objectively managing performance

Level 5

Continuously Improving

1. Improving organization capability
2. Improving process effectiveness

Security Program



Security program

People

Technology

Process

Policy definition

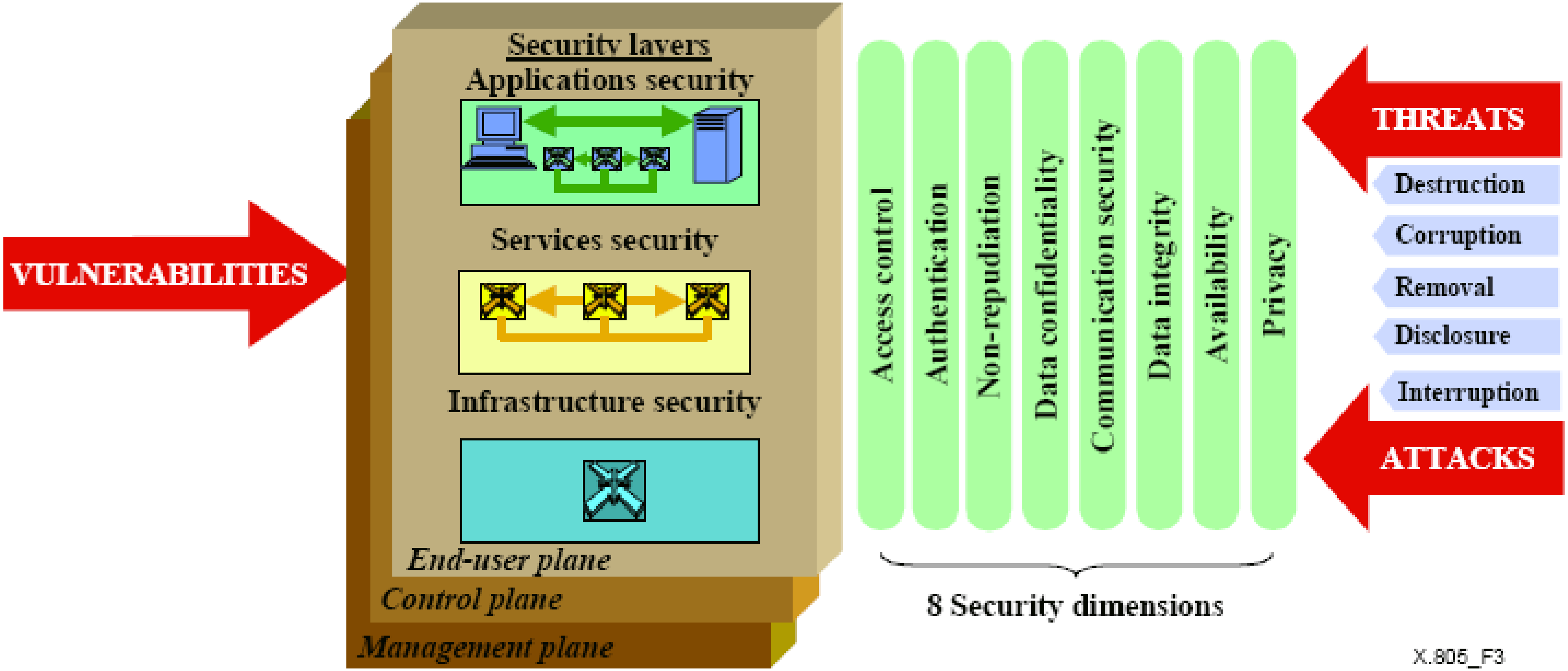
Enforcement

Monitoring and response

Measurement

ITU-T Recommendation X.805

Security architecture for end-to-end network security



Security architecture for end-to-end communications

ITU-T Recommendation X.805 addresses three essential questions:

1. What kind of protection is needed and against what threats?

1. What are the distinct types of network equipment and facility groupings that need to be protected?

1. What are the distinct types of network activities that need to be protected?

Cyber Security Requirements – High Level

Functional Requirements

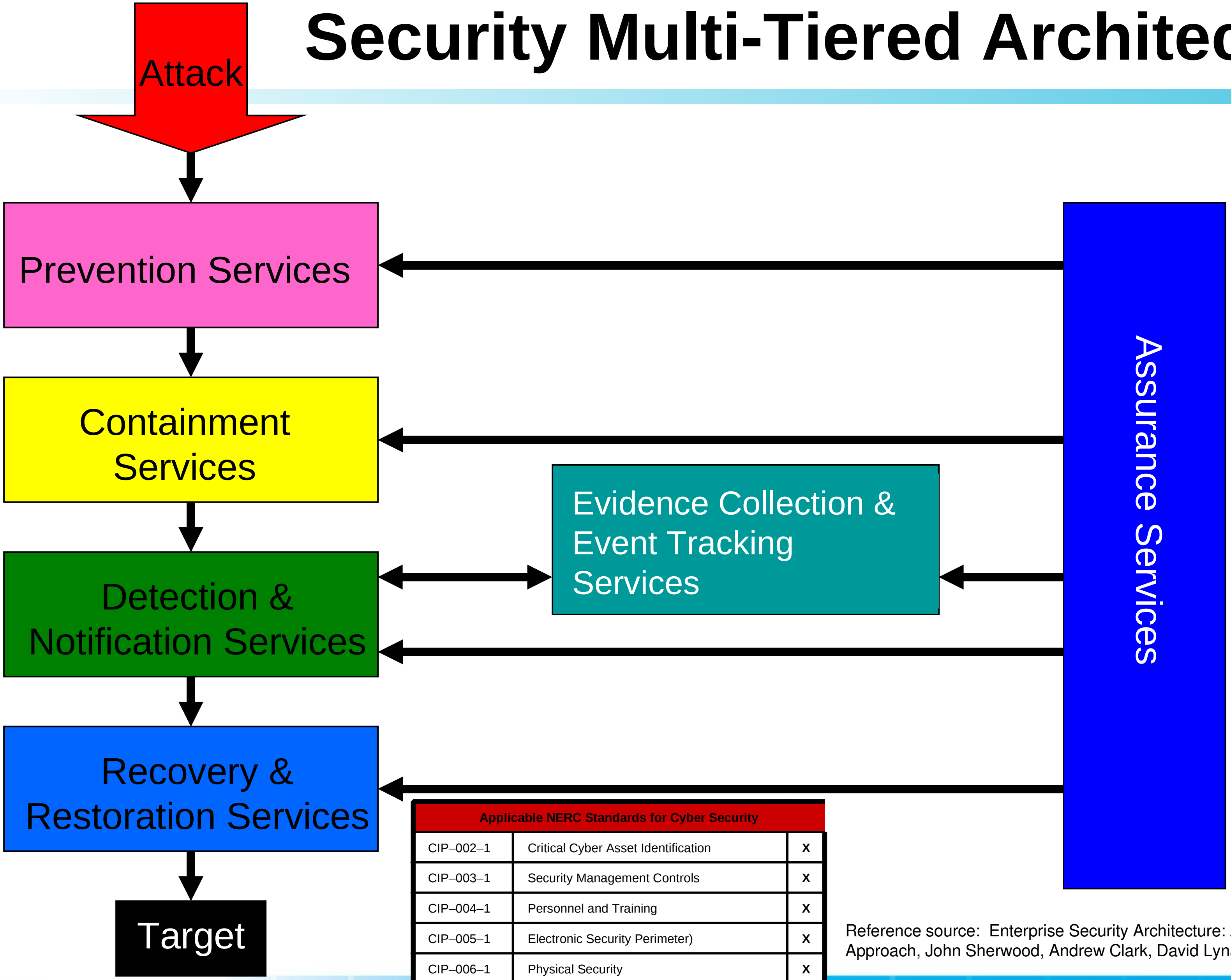
- Auditing
- Cryptographic Support
- User Data Protection
- Event Monitoring
- Identification & Authentication
- Functional Management
- Security Event Monitoring
- Physical Protection
- System Configuration
- Resource Utilization
- Trusted Path/Channels

Assurance Requirements

- Configuration Management
- Delivery & Operation
- Guidance Documents
- Life Cycle Support
- Security Awareness
- Operation & Maintenance
- System Architecture
- Testing
- Vulnerability Assessment
- Assurance Maintenance

Applicable NERC Standards for Cyber Security		
CIP–002–1	Critical Cyber Asset Identification	X
CIP–003–1	Security Management Controls	X
CIP–004–1	Personnel and Training	X
CIP–005–1	Electronic Security Perimeter)	X
CIP–006–1	Physical Security	X
CIP–007–1	Systems Security Management	X
CIP–008–1	Incident Reporting and Response Planning	X
CIP–009–1	Recovery Plans for Critical Cyber Assets	X

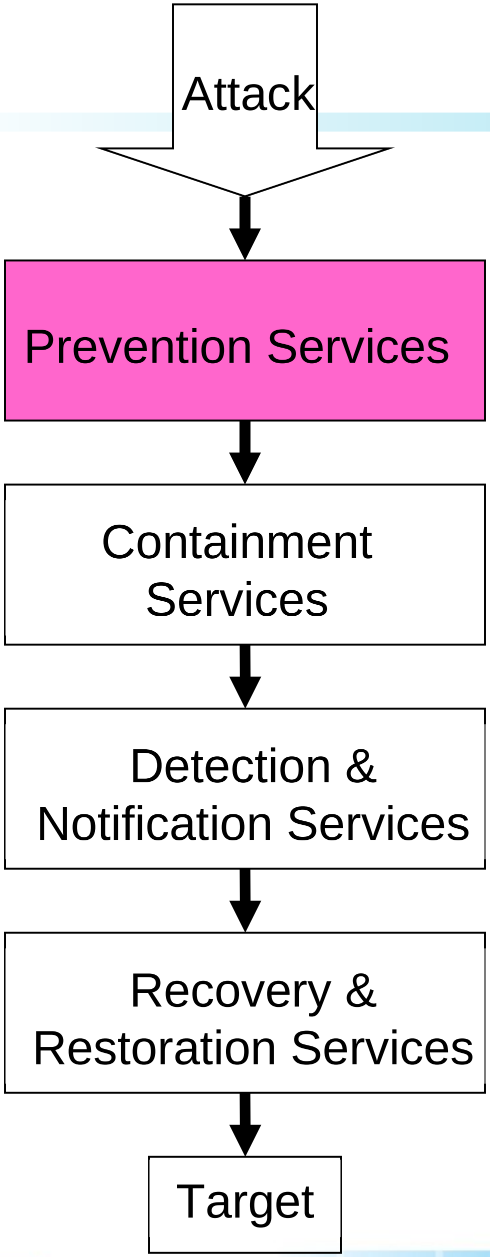
Security Multi-Tiered Architecture


Attack
Prevention Services
Containment Services
Detection & Notification Services
Recovery & Restoration Services
Target
Evidence Collection & Event Tracking Services
Assurance Services

Applicable NERC Standards for Cyber Security		
CIP–002–1	Critical Cyber Asset Identification	X
CIP–003–1	Security Management Controls	X
CIP–004–1	Personnel and Training	X
CIP–005–1	Electronic Security Perimeter)	X
CIP–006–1	Physical Security	X
CIP–007–1	Systems Security Management	X
CIP–008–1	Incident Reporting and Response Planning	X
CIP–009–1	Recovery Plans for Critical Cyber Assets	X

Reference source: Enterprise Security Architecture: A Business-Driven Approach, John Sherwood, Andrew Clark, David Lynas, 2005

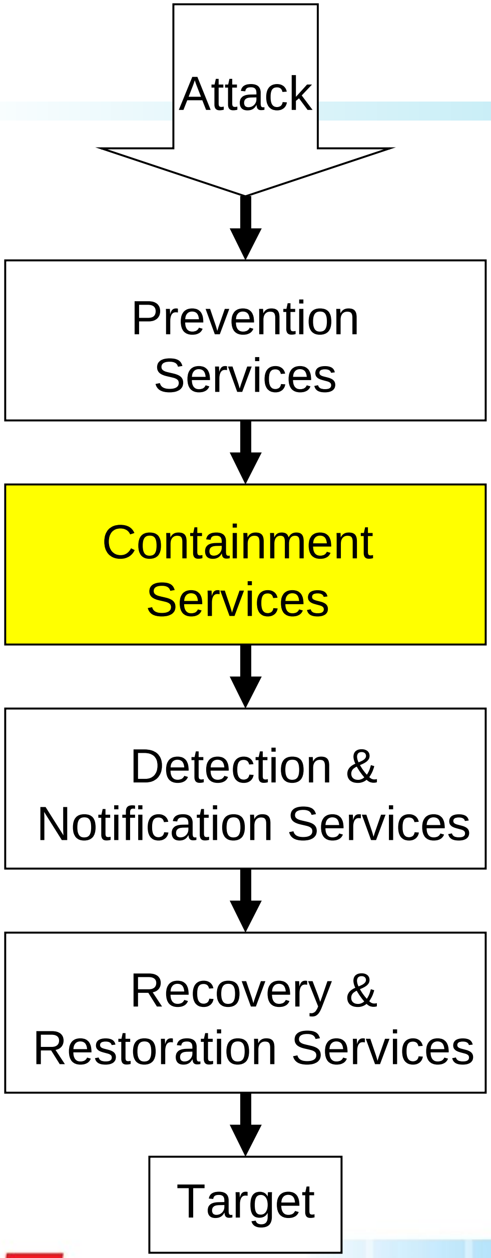
Prevention Services


Attack
Prevention Services
Containment Services
Detection & Notification Services
Recovery & Restoration Services
Target

Security Architecture Tier	Security Services	Detail
Prevention	Entity Security Services	Unique Naming
		Registration
		Public Key Certification
		Credentials Certification
		Directory Service
		Authorization
		Authentication
	Communications Security	Session Authentication
		Message Origin Authentication
		Message Integrity Protection
		Message Content Confidentiality
		Measurement & Metrics
		Security Administration
		User Support
		Physical Security
		Environment Security
		Non-repudiation
		Message Replay Protection
		Traffic Flow Confidentiality
	Application & System Security	Authorization
		Logical Access Controls
		Audit Trails
		Stored Data Integrity Protection
		Store Data Confidentiality
		Software Integrity Protection
		Software Licensing Management
		System Configuration Protection
		Data Replication & Backup
		Software Replication & Backup
		Trusted Time
		User Interface for Security
	Security Management	Policy Management
		Training & Awareness
		Operations Management
		Provisioning
		Monitoring
		Measurement & Metrics
		Security Administration
		User Support
		Physical Security Devices
		Environmental Security

Applicable NERC Standards for Cyber Security		
CIP–002–1	Critical Cyber Asset Identification	X
CIP–003–1	Security Management Controls	X
CIP–004–1	Personnel and Training	X
CIP–005–1	Electronic Security Perimeter)	X
CIP–006–1	Physical Security	X
CIP–007–1	Systems Security Management	X
CIP–008–1	Incident Reporting and Response Planning	

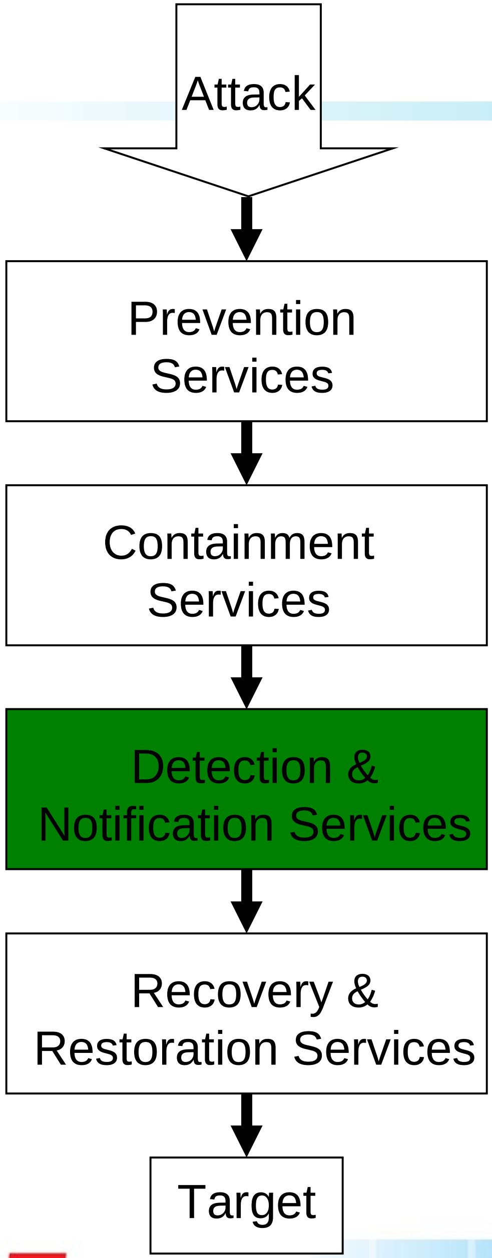
Containment Services


Attack
Prevention Services
Containment Services
Detection & Notification Services
Recovery & Restoration Services
Target

Security Architecture Tier	Security Services
Containment	Entity Authorization
	Store Data Confidentiality
	Software Integrity Protection
	Physical Security
	Environmental Security
	Training & Awareness

Applicable NERC Standards for Cyber Security		
CIP–002–1	Critical Cyber Asset Identification	X
CIP–003–1	Security Management Controls	X
CIP–004–1	Personnel and Training	X
CIP–005–1	Electronic Security Perimeter)	X
CIP–006–1	Physical Security	X
CIP–007–1	Systems Security Management	X
CIP–008–1	Incident Reporting and Response Planning	
CIP–009–1	Recovery Plans for Critical Cyber Assets	

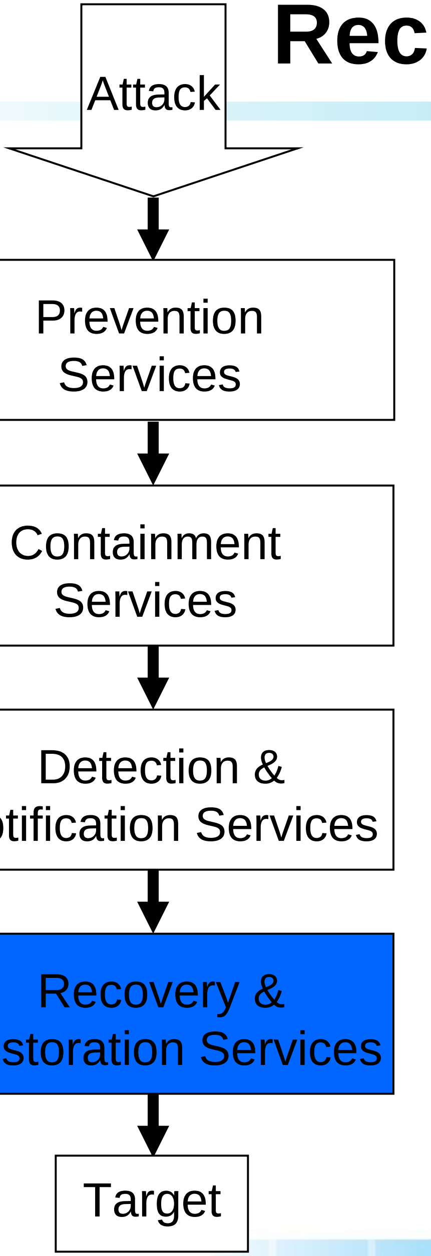
Detection & Notification Services


Attack
Prevention Services
Containment Services
Detection & Notification Services
Recovery & Restoration Services
Target

Security Architecture Tier	Security Services
Detection & Notification	Message Integrity Protection
	Store Data Confidentiality
	Security Monitoring
	Intrusion Detection
	Security Alarm Management
	Training & Awareness
	Measurement & Metrics

Applicable NERC Standards for Cyber Security		
CIP–002–1	Critical Cyber Asset Identification	X
CIP–003–1	Security Management Controls	X
CIP–004–1	Personnel and Training	X
CIP–005–1	Electronic Security Perimeter)	
CIP–006–1	Physical Security	
CIP–007–1	Systems Security Management	X
CIP–008–1	Incident Reporting and Response Planning	X
CIP–009–1	Recovery Plans for Critical Cyber Assets	

Recovery & Restoration Services


Attack
Prevention Services
Containment Services
Detection & Notification Services
Recovery & Restoration Services
Target

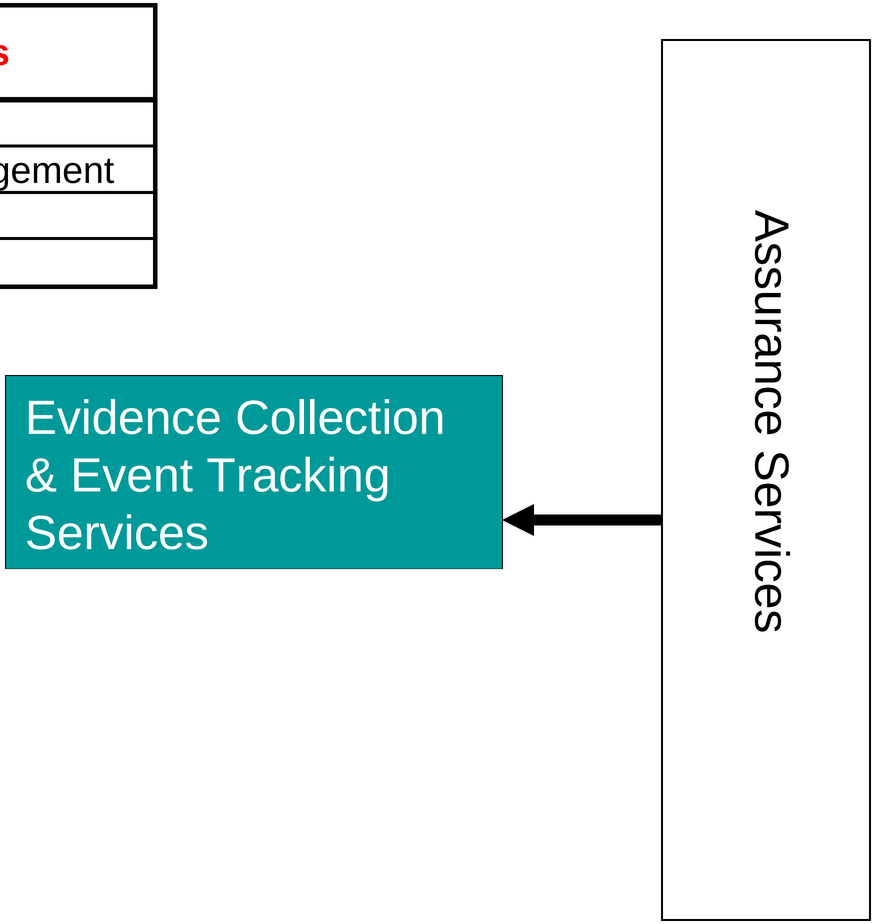
Security Architecture Tier	Security Services
Recovery & Restoration	Incident Response Data Replication & Backup Software Replication & Backup Disaster Recovery Crisis Management

Applicable NERC Standards for Cyber Security		
CIP–002–1	Critical Cyber Asset Identification	X
CIP–003–1	Security Management Controls	X
CIP–004–1	Personnel and Training	
CIP–005–1	Electronic Security Perimeter)	
CIP–006–1	Physical Security	
CIP–007–1	Systems Security Management	X
CIP–008–1	Incident Reporting and Response Planning	X
CIP–009–1	Recovery Plans for Critical Cyber Assets	X

Event Collection & Tracking Services

Security Architecture Tier	Security Services
Event Collection & Event Tracking	Audit Trails
	Security Operations Management
	Security Monitoring
	Measurement & Metrics

Applicable NERC Standards for Cyber Security		
CIP–002–1	Critical Cyber Asset Identification	X
CIP–003–1	Security Management Controls	X
CIP–004–1	Personnel and Training	
CIP–005–1	Electronic Security Perimeter)	
CIP–006–1	Physical Security	
CIP–007–1	Systems Security Management	X
CIP–008–1	Incident Reporting and Response Planning	X
CIP–009–1	Recovery Plans for Critical Cyber Assets	X

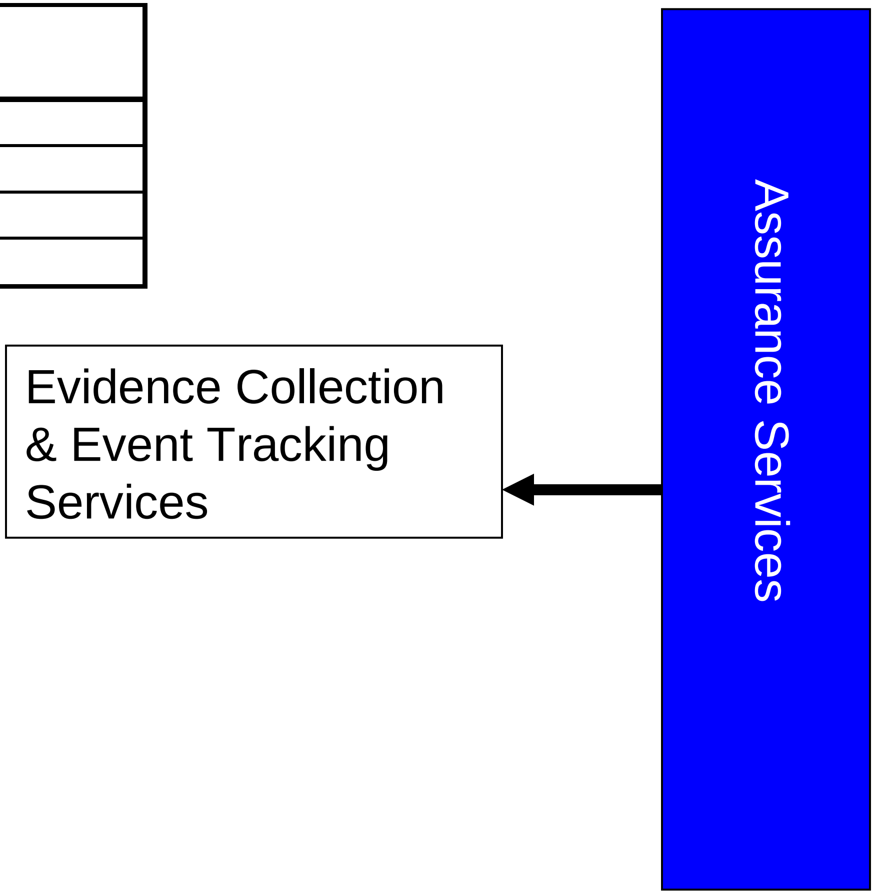


Evidence Collection & Event Tracking Services

Assurance Services

Assurance Services

Security Architecture Tier	Security Services
Assurance	Audit Trails
	Security Audit
	Security Monitoring
	Measurement & Metrics



Evidence Collection & Event Tracking Services

Applicable NERC Standards for Cyber Security		
CIP–002–1	Critical Cyber Asset Identification	X
CIP–003–1	Security Management Controls	X
CIP–004–1	Personnel and Training	
CIP–005–1	Electronic Security Perimeter)	
CIP–006–1	Physical Security	
CIP–007–1	Systems Security Management	X
CIP–008–1	Incident Reporting and Response Planning	
CIP–009–1	Recovery Plans for Critical Cyber Assets	

Security, Quality and the SDLC

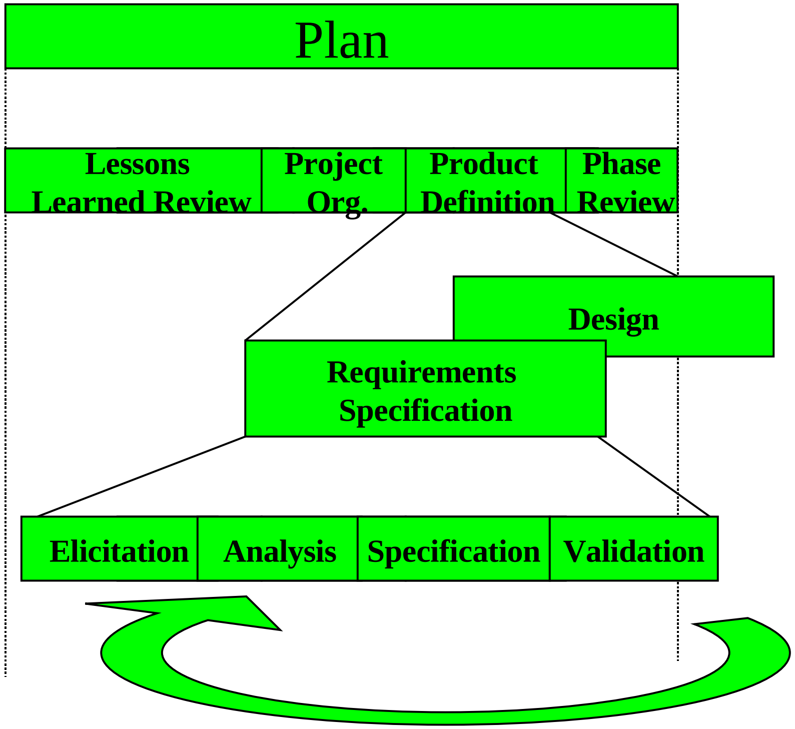
System Development Life Cycle

Proposal	Plan	Construct	Test	Deliver	Close

Security is an aspect of quality which should be addressed throughout the System Development Life Cycle (SDLC)

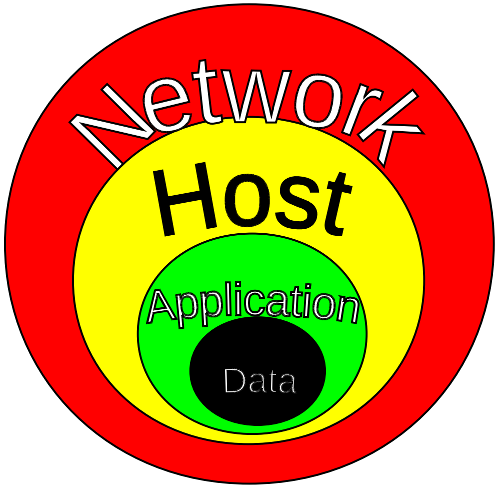
Incorporating Security Into the SDLC

- Begin with requirements
- Secure design
- Secure coding
- Security testing
- Secure deployment
- Security maintenance



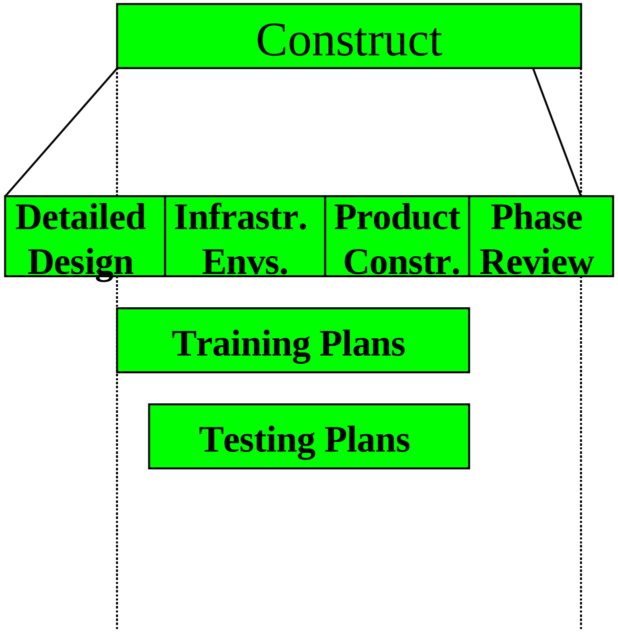
Secure System/Software Requirements

- Begin with requirements
  - What assets of value are accessible from the software?
  - What are the threats to those assets?
  - What protections must be provided for those assets?



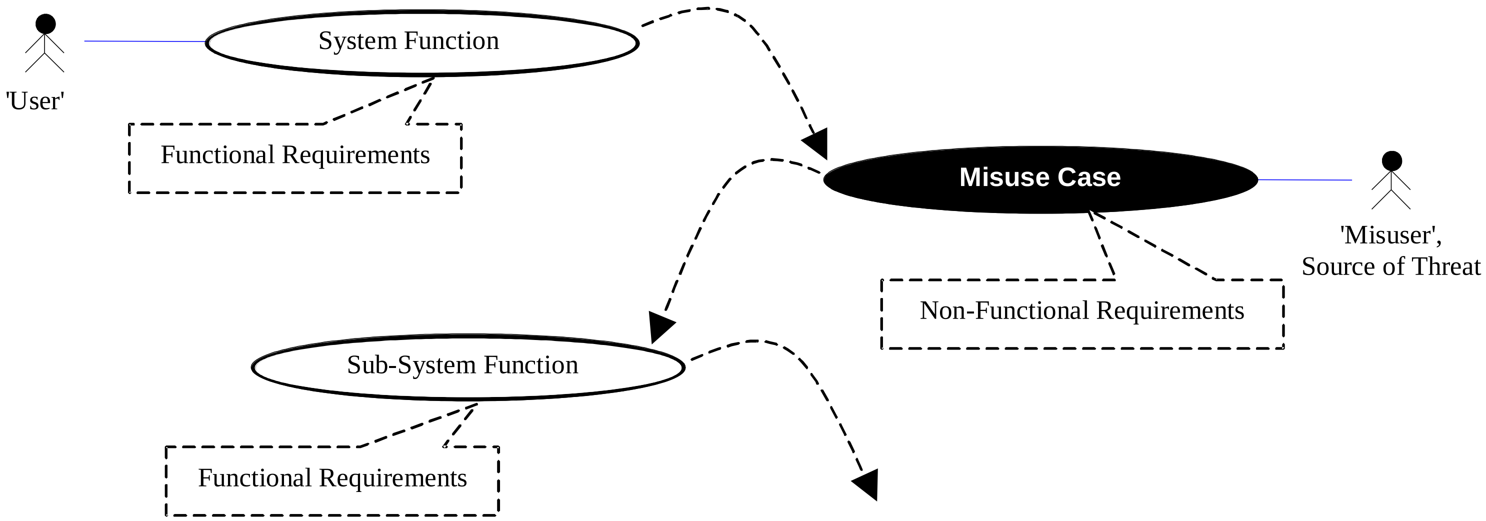
Secure System/Software Design Elements

- Authentication
- Authorization
- Auditing, logging, accountability
- Confidentiality and privacy
- Integrity
- Non-repudiation
- Availability



Secure Design Methodologies

- Design review and risk analysis
- Threat modeling
- Use cases
  - Misuse or abuse cases



Interplay of Use & Misuse Cases with Functional & Non-Functional Requirements

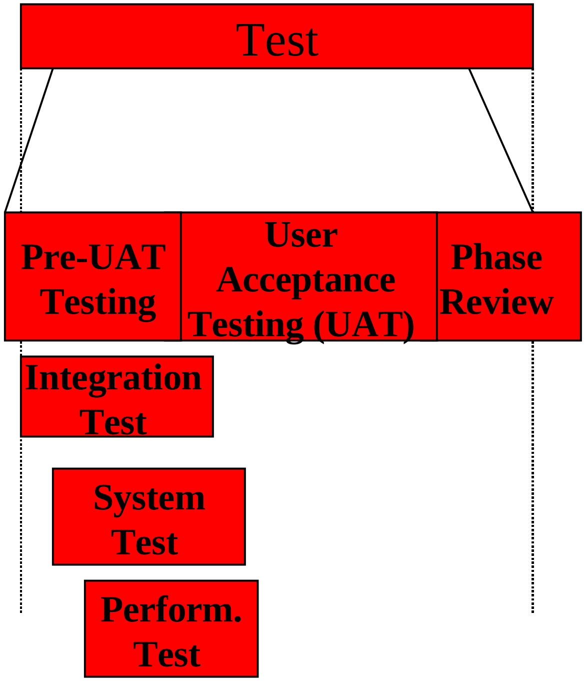
Source: Ian Alexander, Independent Consultant, http://www.scenarioplus.org.uk

Secure development

- Language-specific secure coding checklists
- Develop company coding standards, and include security standards
- Create libraries of security functions that are used by all project teams
- Code reviews and walkthroughs
- Development tools
- Debuggers
- Source code analysis tools

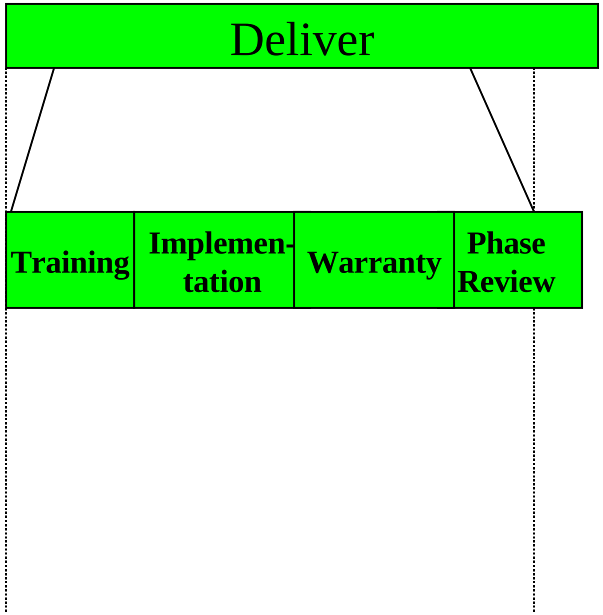
Security testing

- Fault injection
- Fuzzers
- Proxy-based tools
- Automated penetration testing
- Security assessments and penetration tests



Deployment Issues

- Offer a secure mode of installation
- Disable all default accounts at the end of installation
- Force the user to set an administrative password
- Offer configurable auditing and logging levels



Maintenance Issues

Monitor, Track and Control

- Enforce all secure system and software development processes for maintenance releases of code
- Make sure that engineers / developers / administrators fully understand the design and architecture of the entire product
- If the product is not fully understood, there is the probability that security vulnerabilities may be introduced

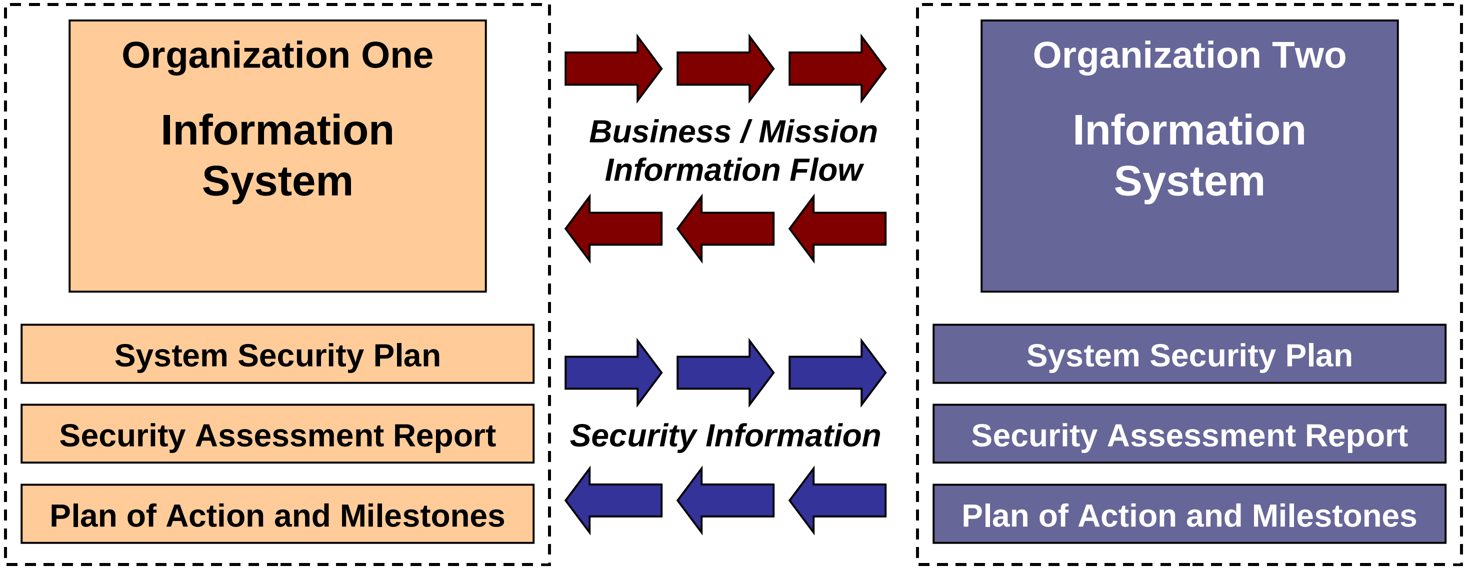
Recommendations

- Make security part of your SDLC
- Ensure someone (preferably more than one person) is responsible for security in each SDLC phase
- Create a virtual security team comprised of those individuals

The Desired Security End State

Why Standardization?

Security Visibility Among Business/Mission Partners



Organization One

Information System

System Security Plan

Security Assessment Report

Plan of Action and Milestones

Business / Mission Information Flow

Security Information

Organization Two

Information System

System Security Plan

Security Assessment Report

Plan of Action and Milestones

Determining the risk to the first organization's operations and assets and the acceptability of such risk

Determining the risk to the second organization's operations and assets and the acceptability of such risk

The objective is to achieve *visibility* into prospective business/mission partners information security programs BEFORE critical/sensitive communications begin…establishing levels of security due diligence.

gridSMART^{SM} Cyber Security Charter

AEP's gridSMART^{SM} initiative and the development and implementation of the modern electrical grid of the future is one of the key drivers behind employment and integration of Cyber Security controls and protection safeguards for networked communications, computerized intelligent electronic equipment and the data/information vital to the management of the gridSMART^{SM} environment.

gridSMART^{SM} Cyber Security Framework

Based upon standards and best practices:

- IntelliGrid / EPRI
- UCA International Usersgroup
  - AMI Working Groups
    - UtilityAMI, OpenAMI, AMI-SEC
  - HAN Working Groups
    - OpenHAN, UtilityHAN
- Department of Energy
  - National Energy Technology Laboratory
- Department of Homeland Security
- NIST – Computer Security Division
- ISO/IEC
- ITU
- Others

gridSMART^{SM} Cyber Security Features

Feature	***Function***	***Benefit***	***Method Example***
Confidentiality	Systems / data is kept secret / private from unauthorized individuals / entities	▪Business / technical security ▪Customer privacy	▪Encryption ▪Key Mgmt/PKI ▪Data Separation
Integrity	Prevents the unauthorized modification of data, provides detection and notification,	▪Ensures data is not modified by unauthorized users	▪Digital Signatures ▪Message Integrity Safeguards ▪Time Stamping
Availability	Systems / data are available and accessible when required	▪Timely, reliable access to data services to authorized users.	▪Protection from attack ▪Protection from unauthorized users ▪Resistance to routine failures
Identification	Identifies individuals / entities.	▪Ensures entities are who they say they are	▪User ID and passwords
Authentication	Substantiates the claimed identity of individuals / entities.	▪Ensures only truly authorized entities are who they say they are	▪Secure Tokens ▪Smart Cards ▪Single Sign-on
Authorization	Identified / authenticated entities have been authorized	▪Protects systems and data from unauthorized entities	▪Certificates ▪Attribute use
Access Control	Role-based access to systems and services	▪Protects systems and data via roles	▪Role-based Access Control ▪Passwords
Non-repudiation	Provides the ability to prove that an system did participate in an exchange of data	▪Proof of origin ▪Proof of delivery ▪Auditing for accountability	▪Digital Signatures ▪Time Stamping ▪Certificate Authority

Questions???