



ERCOT Cyber Security Workshop

How to Get Started with a NERC CIP Gap Analysis

Presented by Ron Blume, P.E.
November 1, 2006



DYONYX – The Company

- IT Management & Consulting Firm
- Founded in 1996
- Offices in Houston, Chicago, Dallas, Washington, D.C.
- Energy Practice Focus
 - NERC Compliant Policies & Procedures Design and Implementation
 - Security Assessments (Cyber / Physical) for:
 - SCADA/DCS Networks
 - Business Networks
 - Business Continuity & Disaster Recovery Planning
 - IT Outsourcing
 - IT Systems Planning
 - Business Process Optimization / Redesign
 - Research & Development



NERC Compliant Security Program Team Competitive Edge

- **Exceptional Team**
 - Average 25 Years Experience
 - NERC CIP Cyber Security Standard Experts
 - Engineers and Security Specialists with Intimate Understanding of Industry
 - Security Specialists with Real-Time Systems Focus
- **Process Approach**
 - Process Models and Instruction Sets
 - Employ Automated Tools
 - **Analytica – Metric Analysis Tool**
 - **ProVision – Process Modeling Tool**



NERC CIP Cyber Security Standard

Key Questions:

- How complicated can it really be to **establish** an effective security program?
- What type of **organizational issues** need to be addressed:
 - Who needs to be involved?
 - Who should be in charge?
 - Who will maintain the security program?
- What are the major **technical** issues?
- What are the major **cultural** issues?
- How much of an **effort** will be required?
- What are the **benefits**?



Project Scope

- 8 NERC Cyber Security Standards
 - 41 Requirements
 - 113 Sub-requirements
- Over 100 Deliverables
 - 20 Policies
 - 40 Procedures/Plans
 - 40 Documents (lists, logs, forms, templates, work instructions, drawings, criteria, etc)



How complicated are the Standards?



NERC CIP CYBER SECURITY STANDARDS Eight Standards / 41 Requirements

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009
CRITICAL CYBER ASSETS	SECURITY MANAGEMENT CONTROLS	PERSONNEL AND TRAINING	ELECTRONIC SECURITY	PHYSICAL SECURITY	SYSTEMS SECURITY MANAGEMENT	INCIDENT REPORTING & RESPONSE PLANNING	RECOVERY PLANS FOR CCA
<ol style="list-style-type: none"> 1. CRITICAL ASSETS 2. CRITICAL CYBER ASSETS 3. ANNUAL REVIEW 4. ANNUAL APPROVAL 	<ol style="list-style-type: none"> 1. CYBER SECURITY POLICY 2. LEADERSHIP 3. EXCEPTIONS 4. INFORMATION PROTECTION 5. ACCESS CONTROL 6. CHANGE CONTROL 	<ol style="list-style-type: none"> 1. AWARENESS 2. TRAINING 3. PERSONNEL RISK ASSESSMENT 4. ACCESS 	<ol style="list-style-type: none"> 1. ELECTRONIC SECURITY PERIMETER 2. ELECTRONIC ACCESS CONTROLS 3. MONITORING ELECTRONIC ACCESS 4. CYBER VULNERABILITY ASSESSMENT 5. DOCUMENTATION 	<ol style="list-style-type: none"> 1. PLAN 2. PHYSICAL ACCESS CONTROLS 3. MONITORING PHYSICAL ACCESS 4. LOGGING PHYSICAL ACCESS 5. ACCESS LOG RETENTION 6. MAINTENANCE & TESTING 	<ol style="list-style-type: none"> 1. TEST PROCEDURES 2. PORTS & SERVICES 3. SECURITY PATCH MANAGEMENT 4. MALICIOUS SOFTWARE PREVENTION 5. ACCOUNT MANAGEMENT 6. SECURITY STATUS MONITORING 7. DISPOSAL OR REDEPLOYMENT 8. CYBER VULNERABILITY ASSESSMENT 9. DOCUMENTATION 	<ol style="list-style-type: none"> 1. CYBER SECURITY INCIDENT RESPONSE PLAN 2. DOCUMENTATION 	<ol style="list-style-type: none"> 1. RECOVERY PLANS 2. EXERCISES 3. CHANGE CONTROL 4. BACKUP & RESTORE 5. TESTING BACKUP MEDIA

Security Program Functional Framework

Functions

Access
Control

Change
Control

Document
Control

Information
Classification
& Handling

Testing & QA

Asset
Inventory

Incident
Response

Systems
Management

Recovery
Operations

Network
Management

Vulnerability
Assessment

Training

Physical
Security

Governance

Personnel
Risk
Management

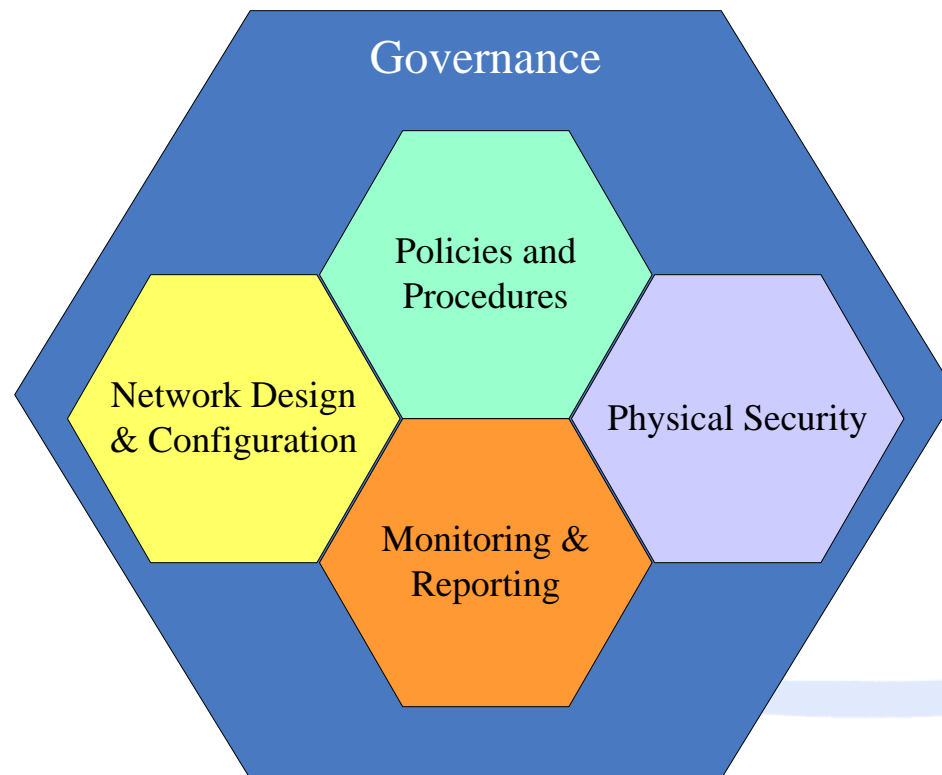
Benefits of Functional Framework

- Simplifies security program processes for:
 - Development
 - Implementation
 - Organizational Analysis
 - On going operations and maintenance
- Provides a framework for training and security awareness

Typical Organizational Impact Matrix

	<div>ORGANIZATION</div> <div>FUNCTION</div>	IT Management Services	Facilities Security	Grid Operations	Substation Engineering	Energy Supply	Human Resources	Audit Services	General Counsel	Corporate Communications	Vendors
1	Access Control	X	X	X	X	X	X				X
2	Change Management	X		X	X	X	X				X
3	Document Control	X	X	X	X	X			X		X
4	Information Classification & Handling	X	X	X	X	X	X	X	X	X	X
5	Testing & Q/A			X	X	X					X
6	Asset Inventory Management		X	X	X	X					
7	Vulnerability Assessment	X	X	X	X	X		X			
8	Incident Response	X	X	X	X	X			X	X	X
9	Systems Management	X		X	X	X					X
10	Training	X	X	X	X	X	X			X	X
11	Physical Security		X	X	X	X					X
12	Recovery Operations	X	X	X	X	X				X	X
13	Governance	X	X	X	X	X	X	X	X	X	
14	Personnel Risk Management		X	X	X	X	X		X		
15	Network Management	X		X	X	X					X

Key Security Program Ingredients



Key Security Program Ingredients

- Corporate **governance** framework;
 - Complex organizations will require broad corporate visibility (not just operations);
 - Sr. management accountability and responsibility for:
 - Design
 - Implementation
 - Operations and Maintenance
 - Physical and cyber security organizational;
 - Integration with existing security programs for business networks and other infrastructures;
 - Security Program Architecture (Entity)

Key Security Program Ingredients

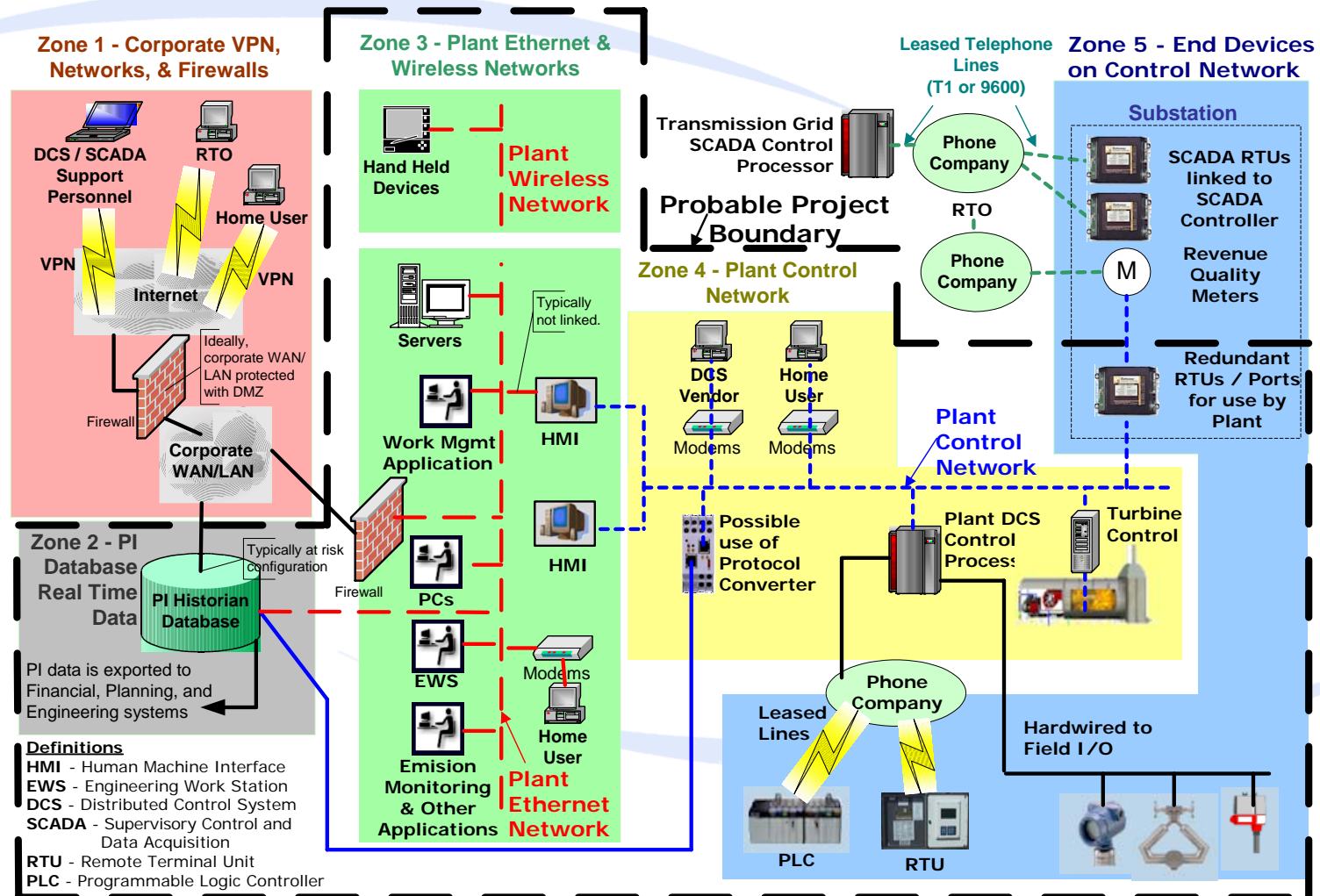
- **Network design and configuration;**
 - Without a security-centric network design and configuration, all the policies and procedures in the world will not make the facilities secure;
 - Establish design and configuration standards (ISO / NERC / NIST);
 - Electronic security perimeter design for critical cyber assets;
 - Impacts implementation costs of program
 - Impacts operational costs of program.

Why is Securing SCADA Different?

- Vulnerabilities at each layer of architecture (end devices, communications, Master Station, View Stations, etc..)
- SCADA Systems can not be shut down easily for patches
- SCADA Systems normally do not have any Antivirus Protection
 - Difficult to Automate Signature Updates
 - AV Software Has Had Impact on SCADA Performance
- Real-Time Requirements Currently Negate Use of Encryption
- SCADA Master and End Devices do not use Authentication
- Need for System Integration Counters Security Measures:
 - EMS, Maintenance, ERP, Dispatch, Accounting/Billing, Trading...
 - SCADA Systems were not designed to be securely connected
 - Backdoors and open routes to Corporate LAN often created after installation
- Critical availability and data integrity requirements
- Can not Simply Use Traditional IT Security Solutions to Secure SCADA Systems

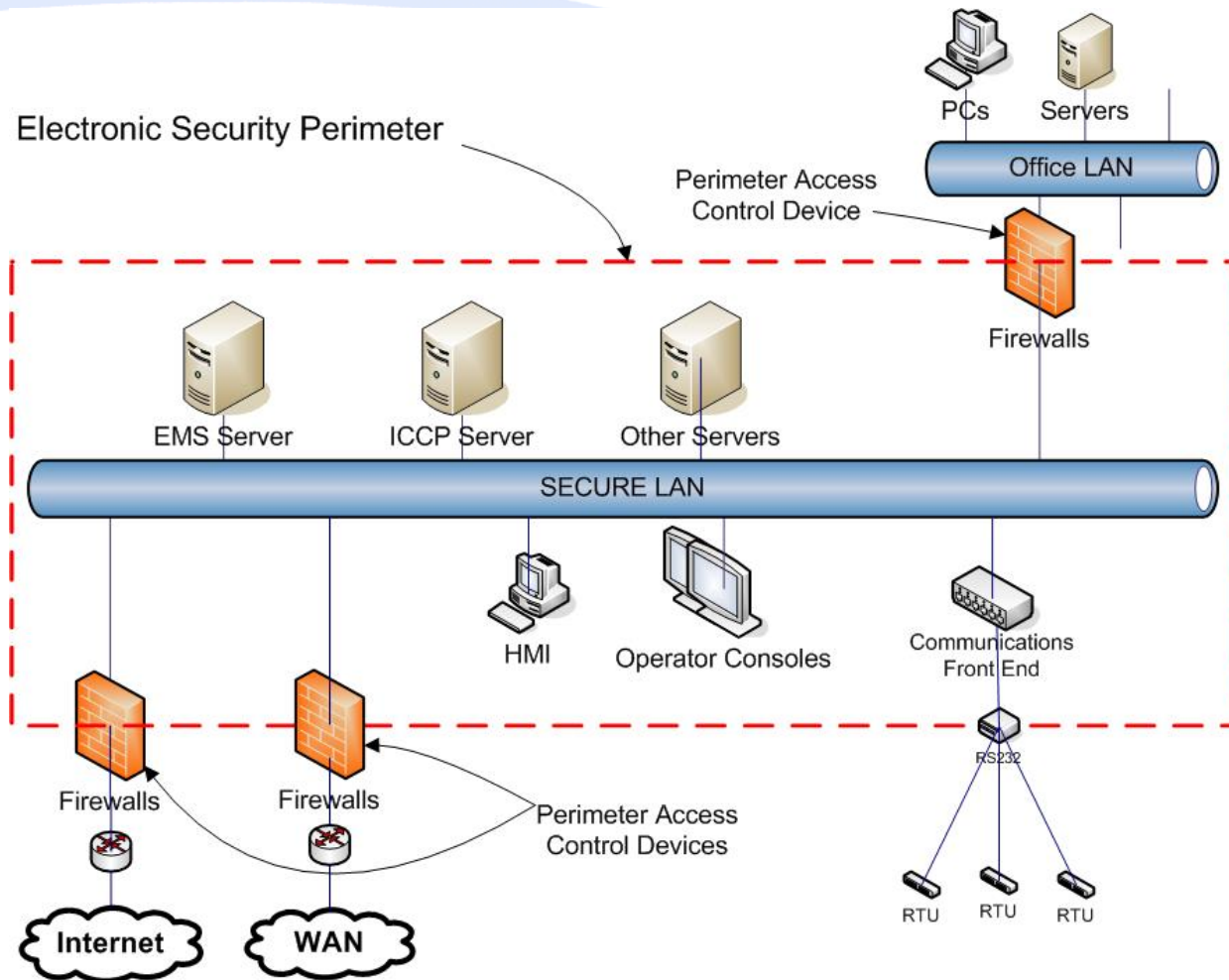
Network Design Review

Typical DCS / SCADA Network Infrastructure with Zones of Vulnerability



Network Design & Configuration

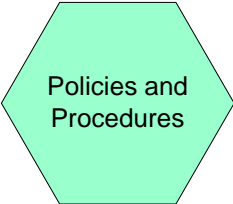
NERC Perspective Network Architecture Considerations



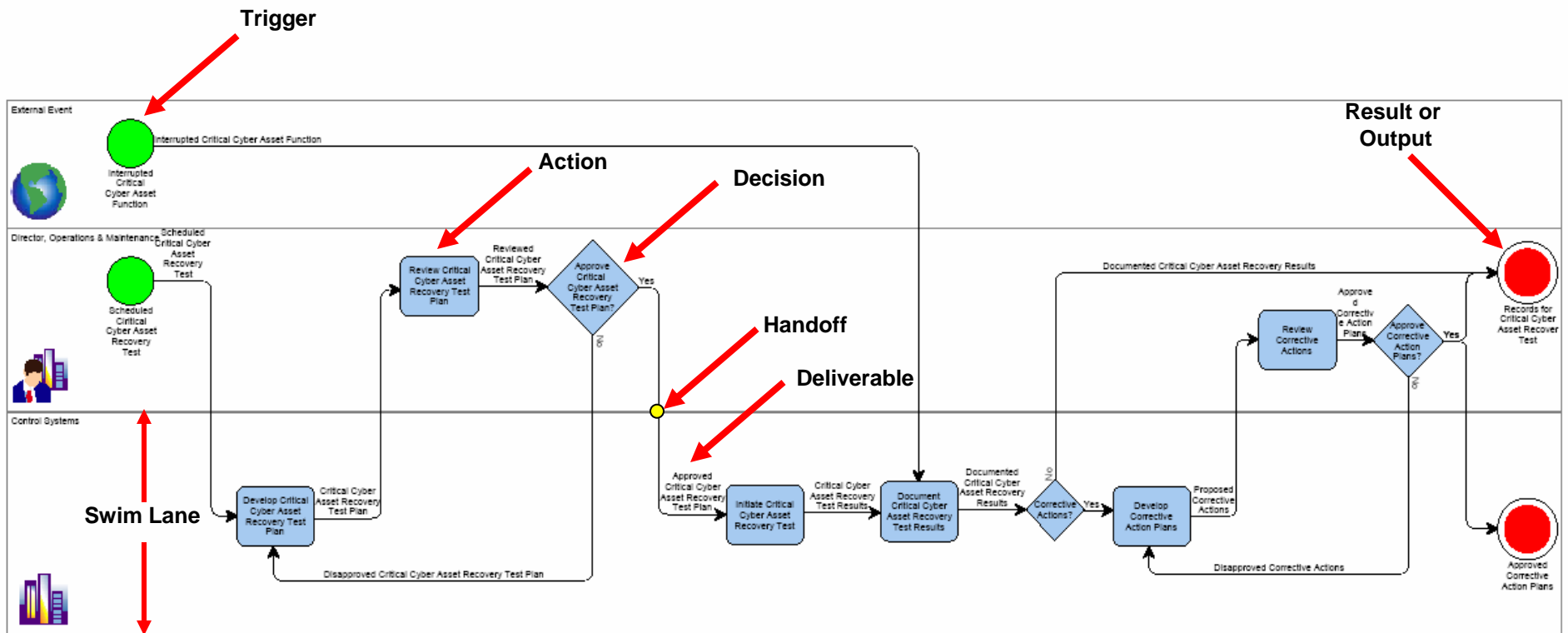
Network Design
& Configuration

Key Security Program Ingredients

- **Policies and procedures** that are complimentary and commensurate with:
 - Appropriate Standards;
 - Governance provisions;
 - Responsible entity critical success factors (CSF's).



Policies and
Procedures



Answers the questions:

What
Who
How
When
Where
Why

Key Security Program Ingredients

- **Physical security** that protects critical cyber assets and critical assets commensurate with:
 - Appropriate Standards
 - Electronic security perimeter;
 - Responsible entity critical success factors (CSF's)
- **Issues**
 - Can be very expensive
 - Typically the Achilles Heal of many facilities



Physical
Security

Key Security Program Ingredients

- Effective compliance **monitoring and reporting** / Audit Proof
 - Review of policies and procedures to ensure compliance with applicable standards;
 - Review of actual practices to ensure they are consistent with the established policies and procedures;
 - Reporting (Incidents / Recovery Planning)
 - Effective controls are in place.

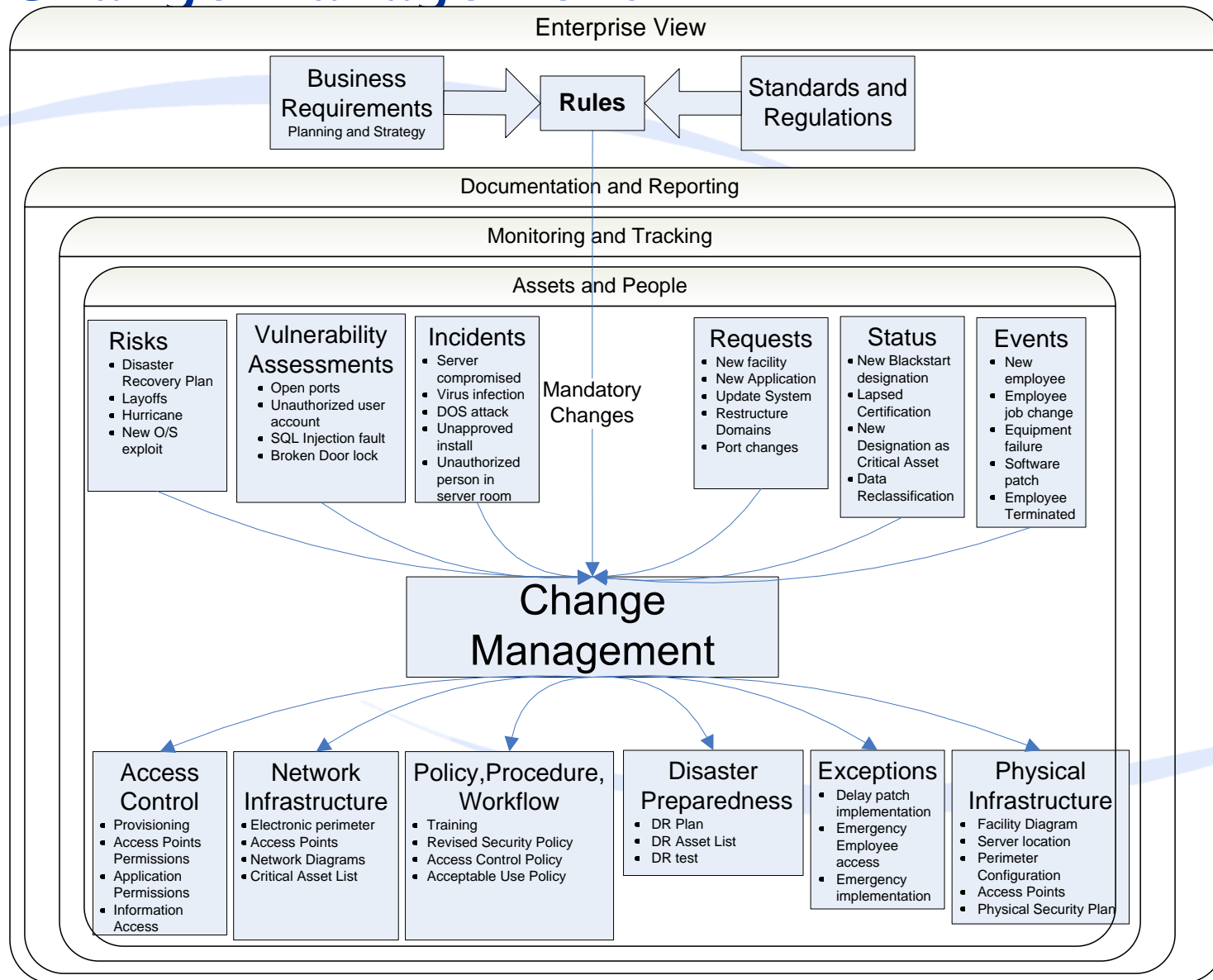
Technical Issues:

- Configuration Management
 - Configuration management is paramount in the ongoing **asset management, access control, and change control** functions for an effective security program.
 - Configuration control needs to address the identity of:
 - Critical assets;
 - Critical cyber assets, ports, services, etc.
 - Access points;
 - Inter-relationships of critical cyber assets;
 - People who have access to critical cyber assets.
 - Configuration management structures will require adjustments for various asset types and operating characteristics.

Technical Issues:

- Access Control
 - Who has access to what?
 - Access control involves **people, assets, and authentication processes** here-to-for not typically addressed in identity management or similar programs;
 - How is access provisioned and de-provisioned?
 - Assurance that synchronization is maintained between **authorized** and **actual** access provisioning / de-provisioning will be required and audited.

Why Change Management?



Technical Issues:

- **Document Control;**
 - Infrastructure configurations;
 - Network design;
 - Floor plans of critical facilities;
 - Incident response and recovery plans;
 - Testing results;
 - Asset information.
- **Operational Efficiency**
 - Leverage technology through process automation and effective controls;
 - Keep it simple
 - Manage level of detail

Cultural Issues:

- Implementation of “New” Processes;
 - Access control granulation
 - Password management
 - Change management
 - Configuration management
 - Document management
 - Event monitoring and documentation
 - Software design
 - Testing
- Organizational Responsibilities
 - Turf battles
 - Collaborative processes

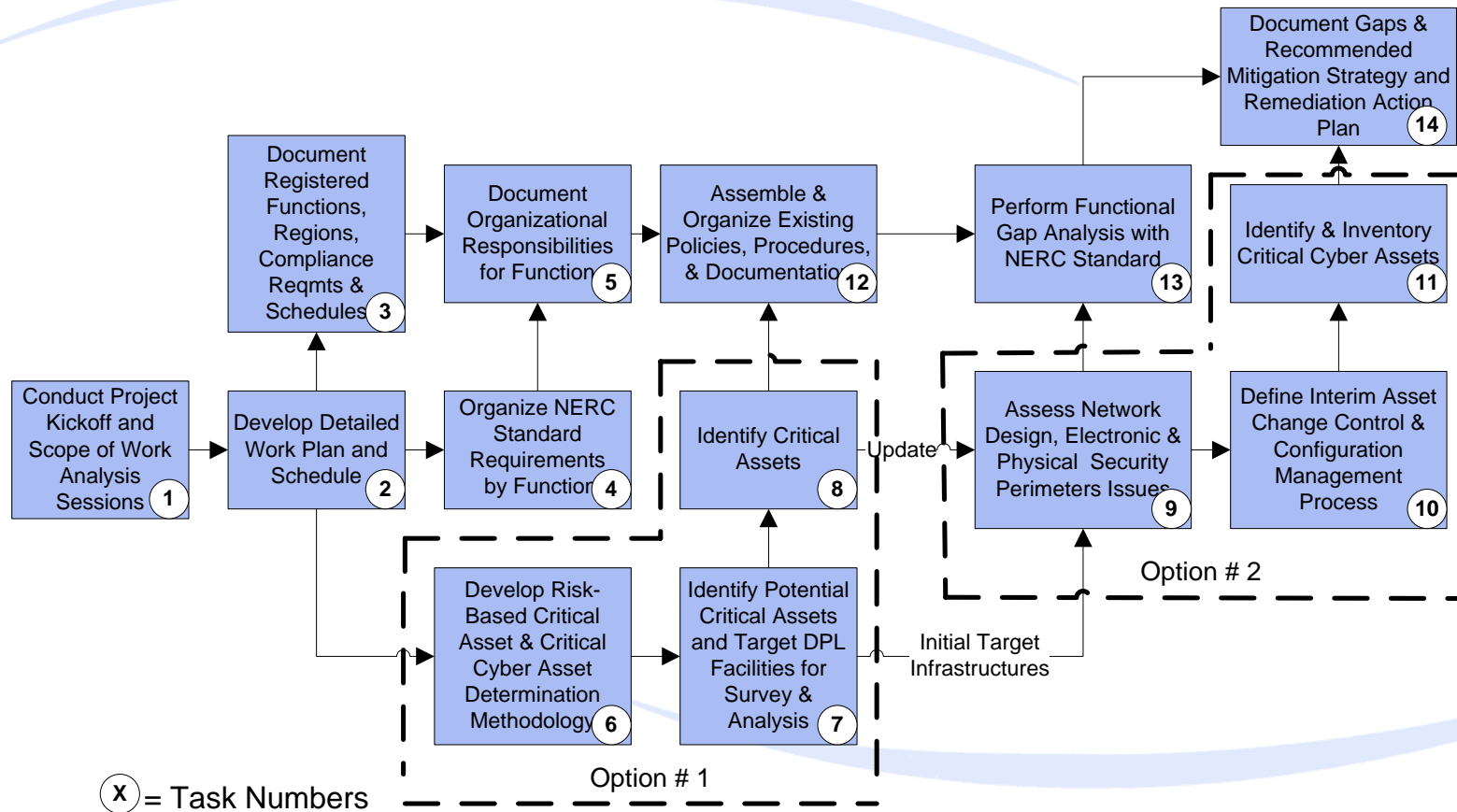
Key Deliverables:

- Policy & procedures (estimates);
 - 20 Policies
 - 40 Procedures
 - 40 Documents (Reports, Logs, Drawings)
- Network design & configuration evaluation;
- Physical security initiatives;
- Organization restructuring;
- Training program.

First Steps: How to Get Started?

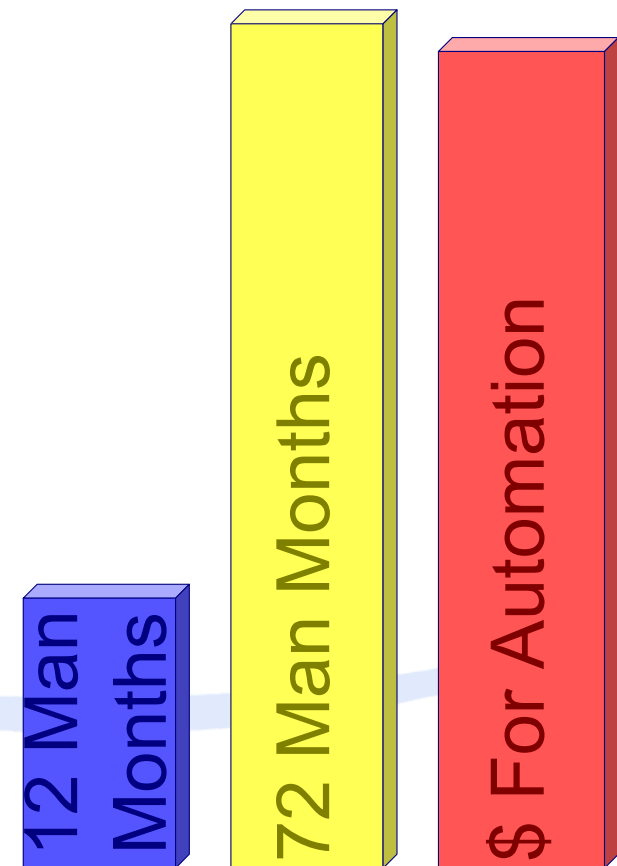
- Conduct a NERC CIP Cyber Security Standard **Gap Analysis** of the Existing Policies and Procedures
- **Identify Critical Assets**, Critical Cyber Assets, Electronic Security Perimeters, and Physical Security Perimeters
- Conduct a Design Level **Review** of the Relevant **Network Infrastructures**

Typical NERC Gap Analysis Work Plan



Level of Effort Attributes

- Size, complexity, and nature of organization;
- Number and location of **critical cyber assets**;
- Established provisions for **physical security** of critical cyber assets;
- Current **cyber security provisions** of networked infrastructures and access control points within electronic security boundaries;
- **Compliance** of existing policies and procedures with standard;
- Availability of required technical **support systems**.



Benefits

- Enhanced **reliability** and availability of the bulk electric system;
- Improved incident **response**;
- Improved **audit** reporting;
- **Optimized utilization** of resources through the implementation of **risk** management concepts and **alignment** with CSFs;
- **Investment** in operational **resiliency**.

