AODR Role-Based Training

- *Name*
  Title
- *Division Name*
- *U.S. Department of Energy*
- *Office of the Associate CIO for Cyber Security*

Office of the
Chief Information Officer

Objectives

Gain Understanding and Working Knowledge of:

- AODR Authority, Role and Responsibilities
- Key Cyber Security Terms
- Cyber Security Program Management Structure
- Policy Hierarchy
- Risk Management Framework and Certification and Accreditation Process Relationship
- Pre-AO C&A Package Review
- Accreditation Forms, Boundaries and Common Controls and Inheritance
- Accreditation Decision and Package Transmission
- Continuous Monitoring

Office of the
Chief Information Officer

Who is the AODR?

- Authorizing Official Designated Representative (AODR)
- AODRs are appointed by the AO
  - AODR function can be performed by AO
  - AODR role is not a required role by DOE Order or National policy
  - If AODR position is appointed it can be filled by one or more technical experts
  - AODR authority covers Operating Units under AO jurisdiction as identified by appointment

Office of the
Chief Information Officer

What does the AODR do?

- Serves as a technical representative to the AO
- Is responsible to the AO for ensuring cyber security is
  - Integrated into the System Development Life Cycle (SDLC)
  - Implemented throughout the SDLC
- Ensures effectiveness of established standards, guidelines and requirements required by Senior DOE Management-developed policies such as the Risk Management Approach (RMA) or Program Cyber Security Plan (if applicable).
- Maintains a working knowledge of system
  - Functions
  - Security policy
  - Technical security safeguards

Office of the
Chief Information Officer

What does the AODR do?

Drilling down a little

- Data Security
- Information Technology (IT) System Operations and Management
- Network and Telecommunications Security and Remote Access
- Regulatory and Standards Compliance
- Security Risk Management
- System Application Security

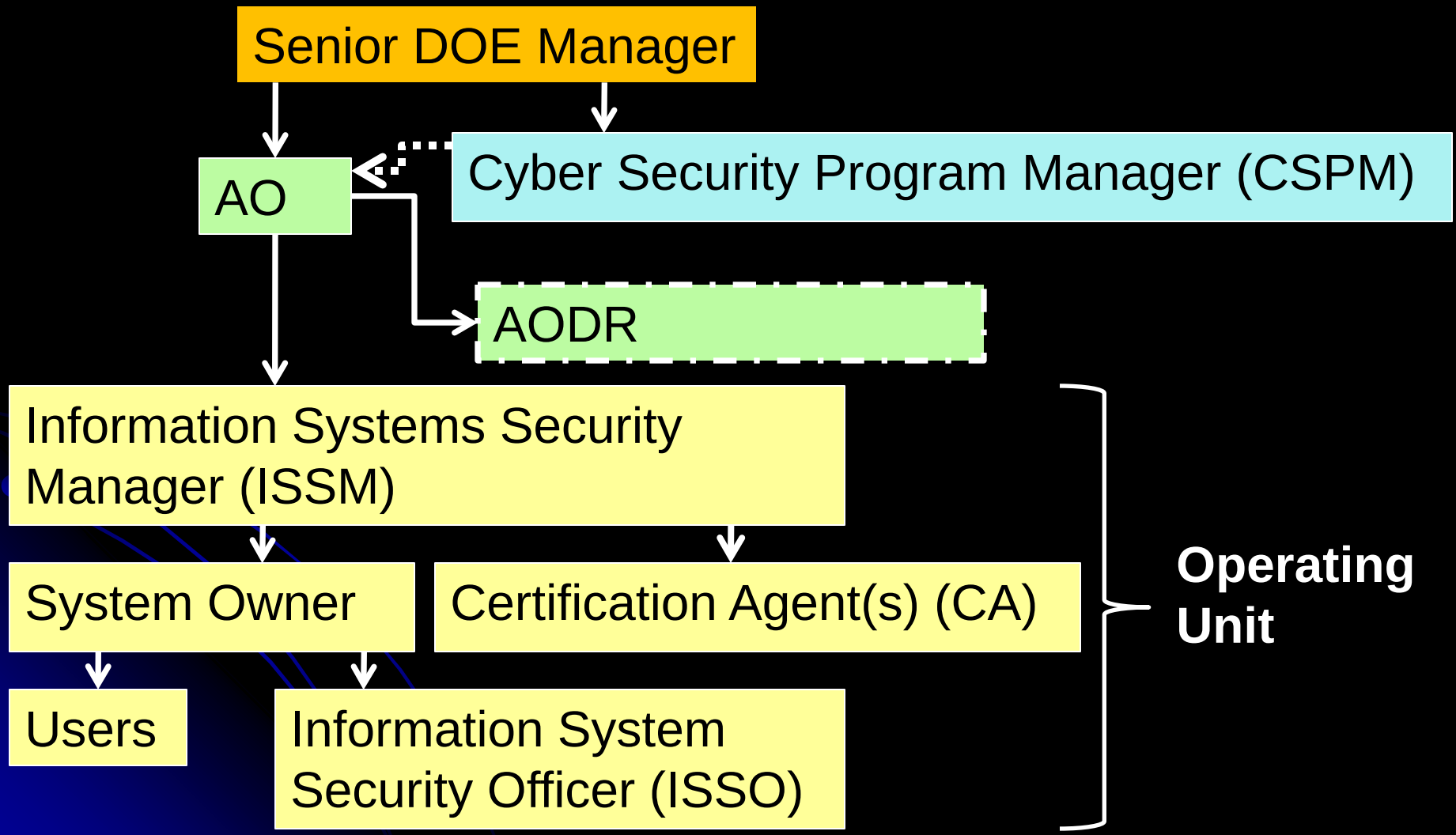
Office of the
Chief Information Officer

Key Cyber Security Terms

- Operating Unit
- Information Resources
  - Government Information and Information Technology
- Government information
  - Federal, Contractors/ subcontractors, licensees
- Government Information Types
- Information Technology (IT)
- Information System
- Information System Types

Office of the
Chief Information Officer

Cyber Security Management Structure



Office of the
Chief Information Officer

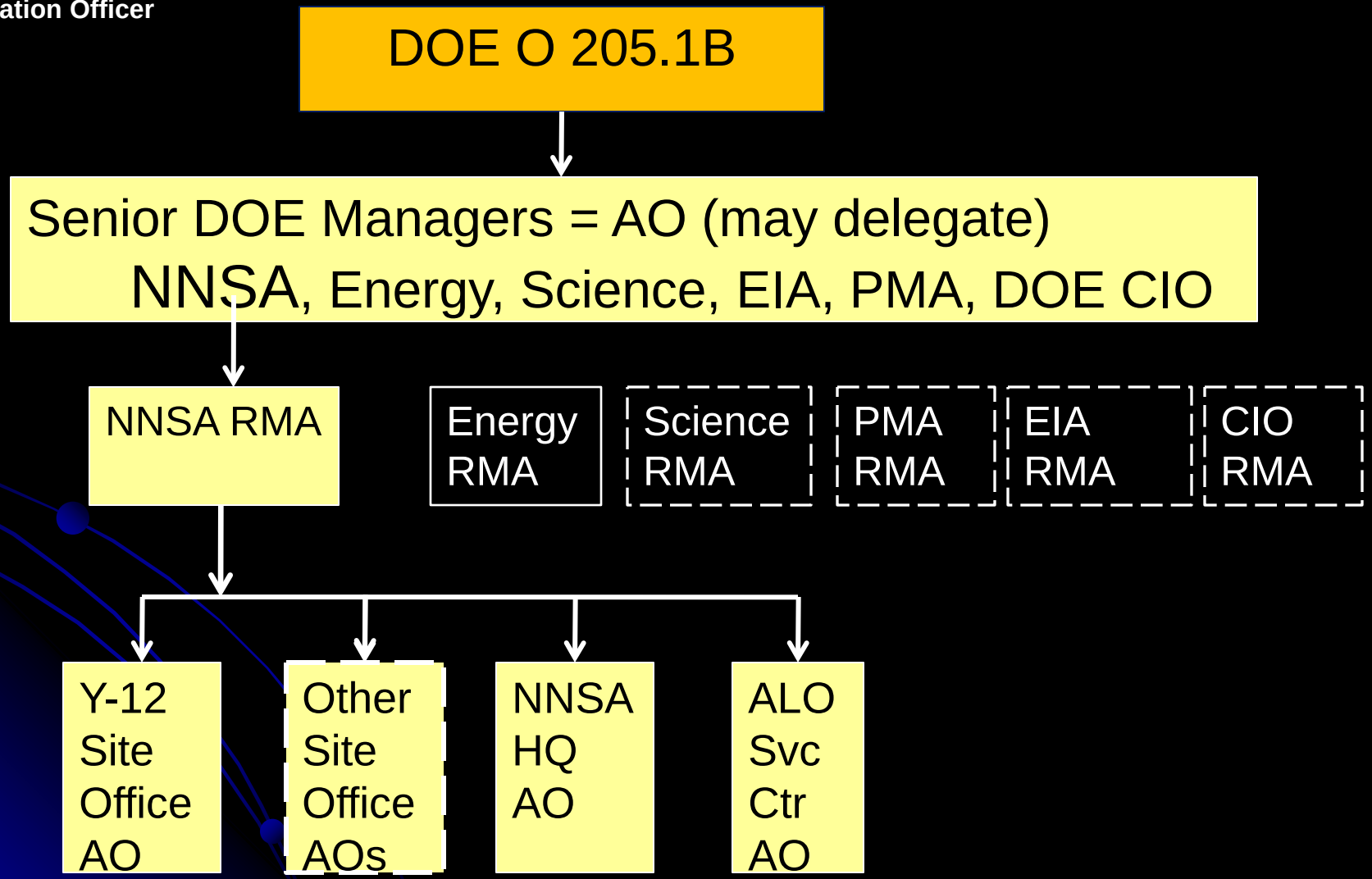
Cyber Security Management Structure

DOE Cyber Security Management Structure Key Roles

- **Senior DOE Manager**
- **Authorizing Official (AO)**
- **Cyber Security Program Manager** (CSPM)
- **Authorizing Official Designated Representative** (AODR)
- **Information Systems Security Manager** (ISSM)
- **Certification Agent** (CA) or Security Control Assessor
- **System Owner**
- **Information System Security Officer** (ISSO)

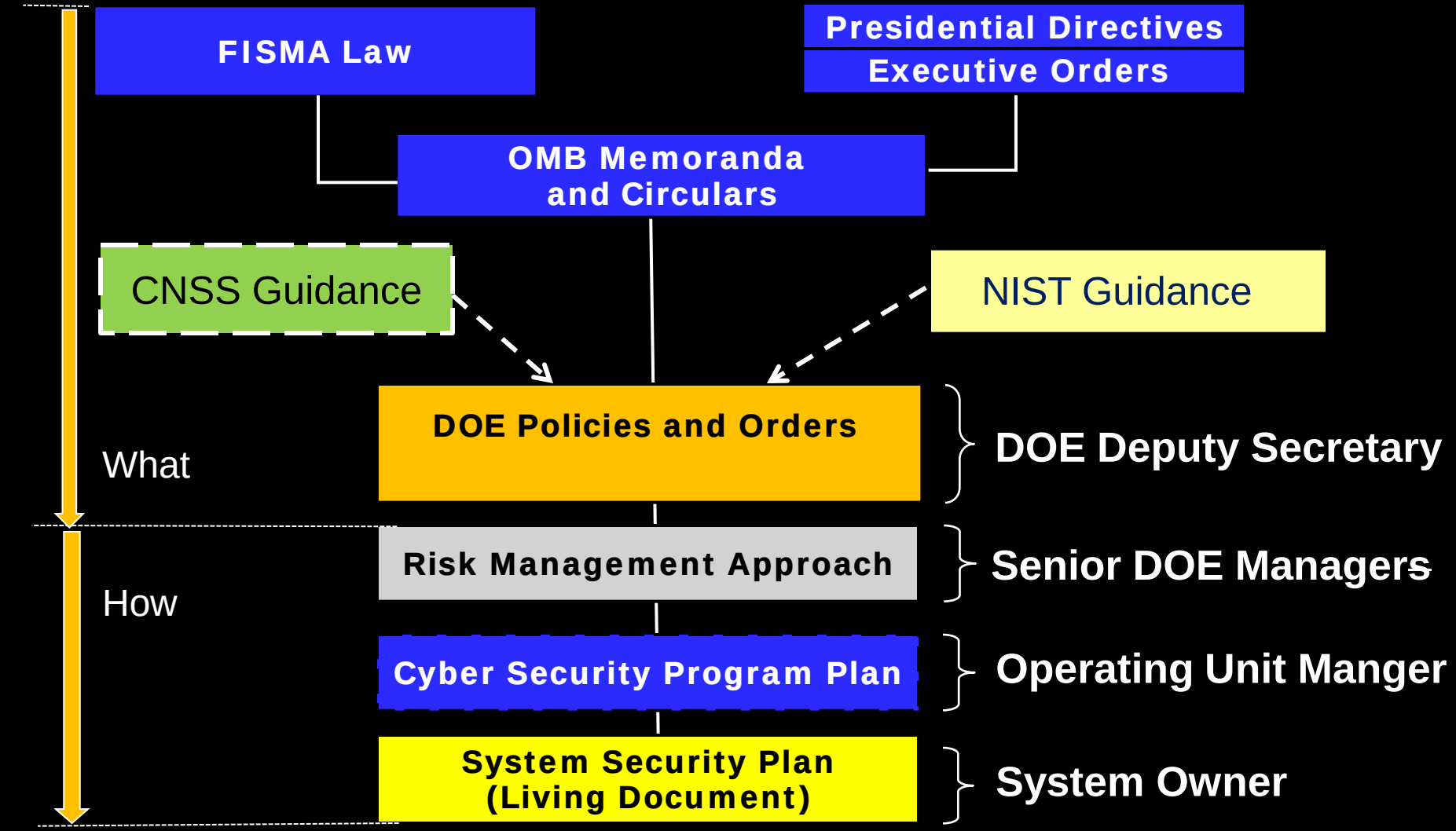
Office of the
Chief Information Officer

AO Structure



The Policy Hierarchy

Office of the
Chief Information Officer



Office of the
Chief Information Officer

The Policy Hierarchy

- **DOE O 205.1B–Establishes DOE Cyber Security Program**
  - Requires the Senior DOE Managers to
    - Implement a Cyber Security Program
    - Develop a Risk Management Approach (RMA)

- **DOE Cyber Security Policy and Orders are based on requirements and guidance from**
  - Office of Management and Budget
  - National Institute of Standards and Technology
  - Committee for National Security Systems instructions

Office of the
Chief Information Officer

The Policy Hierarchy

Key Documents

- Risk Management Approach (RMA)
- Cyber Security Program Plan (CSPP) - Optional
- System Security Plan (SSP)

Office of the
Chief Information Officer

The Policy Hierarchy

- **The System Security Plan describes:**
  - System/system accreditation boundary
  - Information types and the confidentiality, integrity, and availability requirements for each
  - System categorization
  - Baseline set of cyber security controls
  - How each control is implemented by the system
  - System environment [physical, logical (networking, etc.), and operational] and identifies
    - Environment unique threats/ vulnerabilities
    - Countermeasures (special security controls)
  - System interconnections and signed agreements

Risk Management Framework (RMF)

Office of the Chief Information Officer

Starting Point

Identify
Information System

Identify system components, authorization boundary, and information types;

CATEGORIZE
Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

SELECT
baseline Security Controls

Select baseline security controls based on PCSP policies

DETERMINE
Environmental Risk Impacts

Assess risks from Site threats and system environmental threats/ vulnerabilities

IMPLEMENT
Security Controls

Implement security controls within enterprise architecture; apply security configuration settings; document in SSP

ASSESS
Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

AUTHORIZE
Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

MONITOR
Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

System Development Life Cycle

Office of the
Chief Information Officer

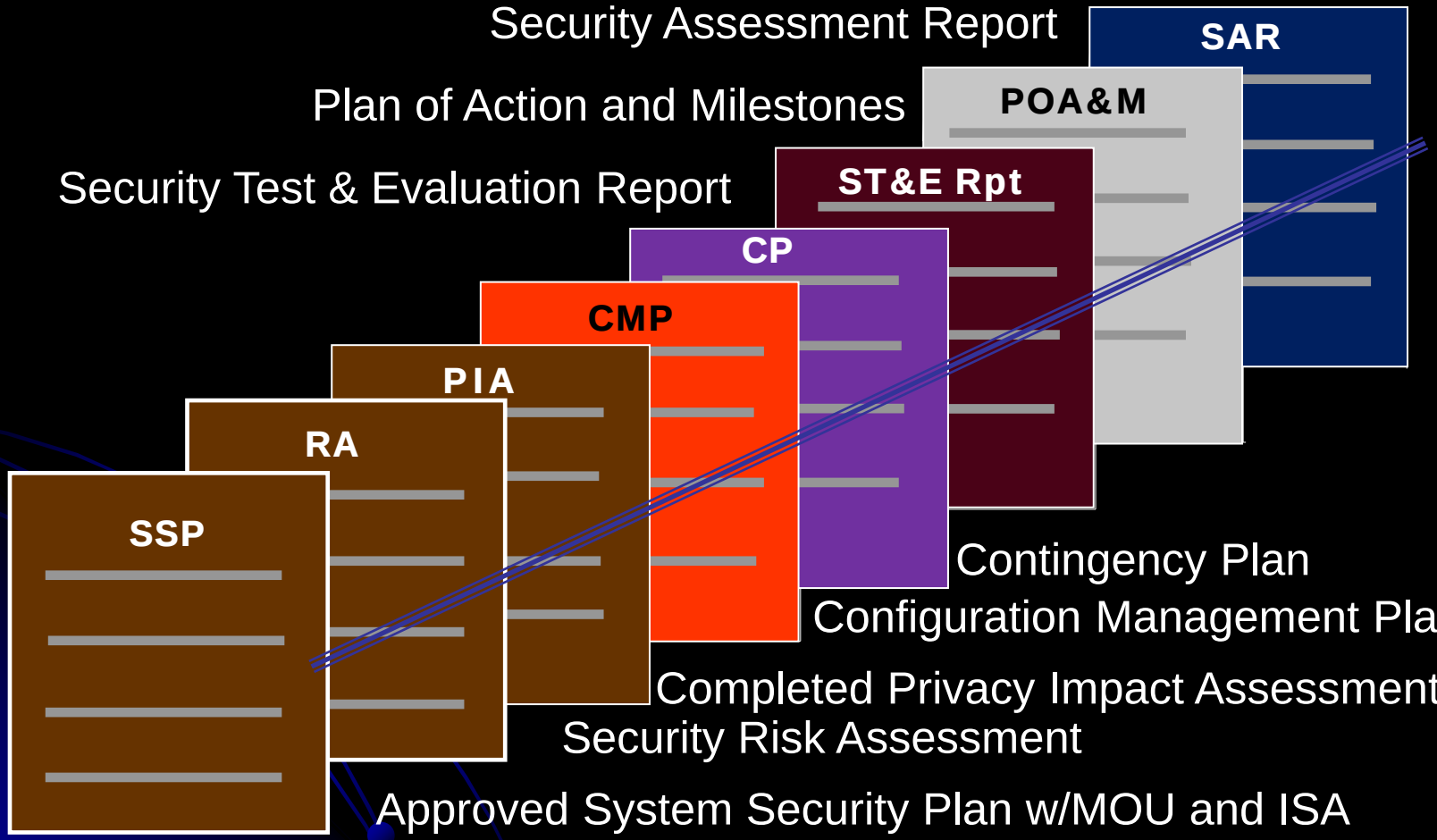
Certification and Accreditation Process

- Relationship between the Risk Management Framework and the Certification and Accreditation Process

Certification & Accreditation Process	Risk Management Framework
Initiation Phase	Identify, Categorize, Select, Determine, Implement
Certification Phase	Assess
Accreditation Phase	Authorize
Continuous Monitoring Phase	Monitor

Office of the
Chief Information Officer

Assess - Assemble C & A Package



Office of the
Chief Information Officer

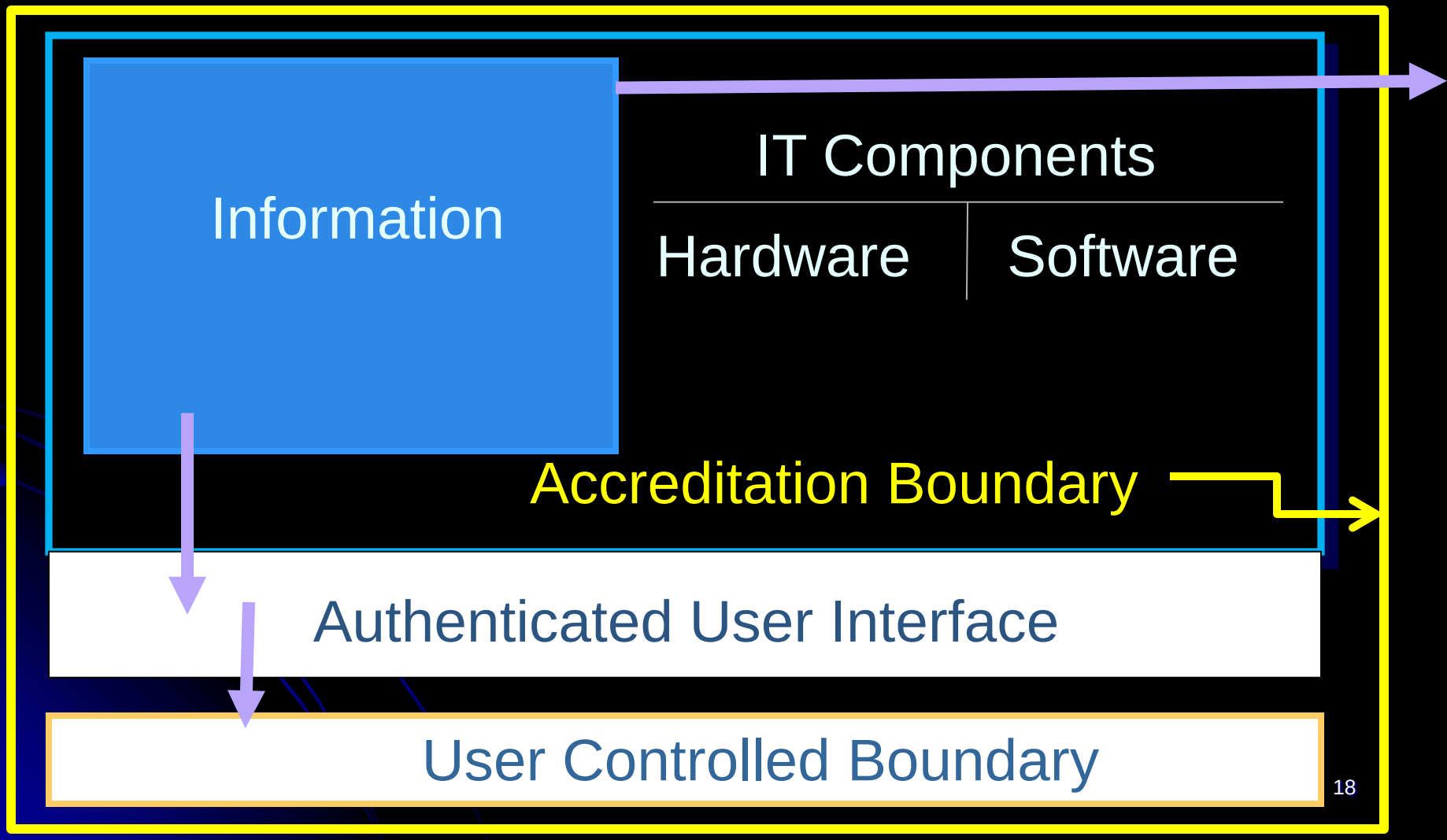
AODR & Pre-AO C&A Package Review

Determines that all package components are present

- Ensures accurate documentation of:
  - Authorization/Accreditation Boundaries
  - Common Controls
- Evaluates and ensures that Risk is acceptable to Mission, system and information assets, Nation
- Evaluates generated POA&Ms to ensure that they are acceptable for corrective actions

Office of the
Chief Information Officer

Information System Accreditation Boundaries



Office of the
Chief Information Officer

Common Controls and Inheritance

- Many security controls are common to all systems in an Operating Unit
- Common Security Controls can be implemented on one system and other systems can inherit the control implementation
- Inherited security controls ATO must be validated

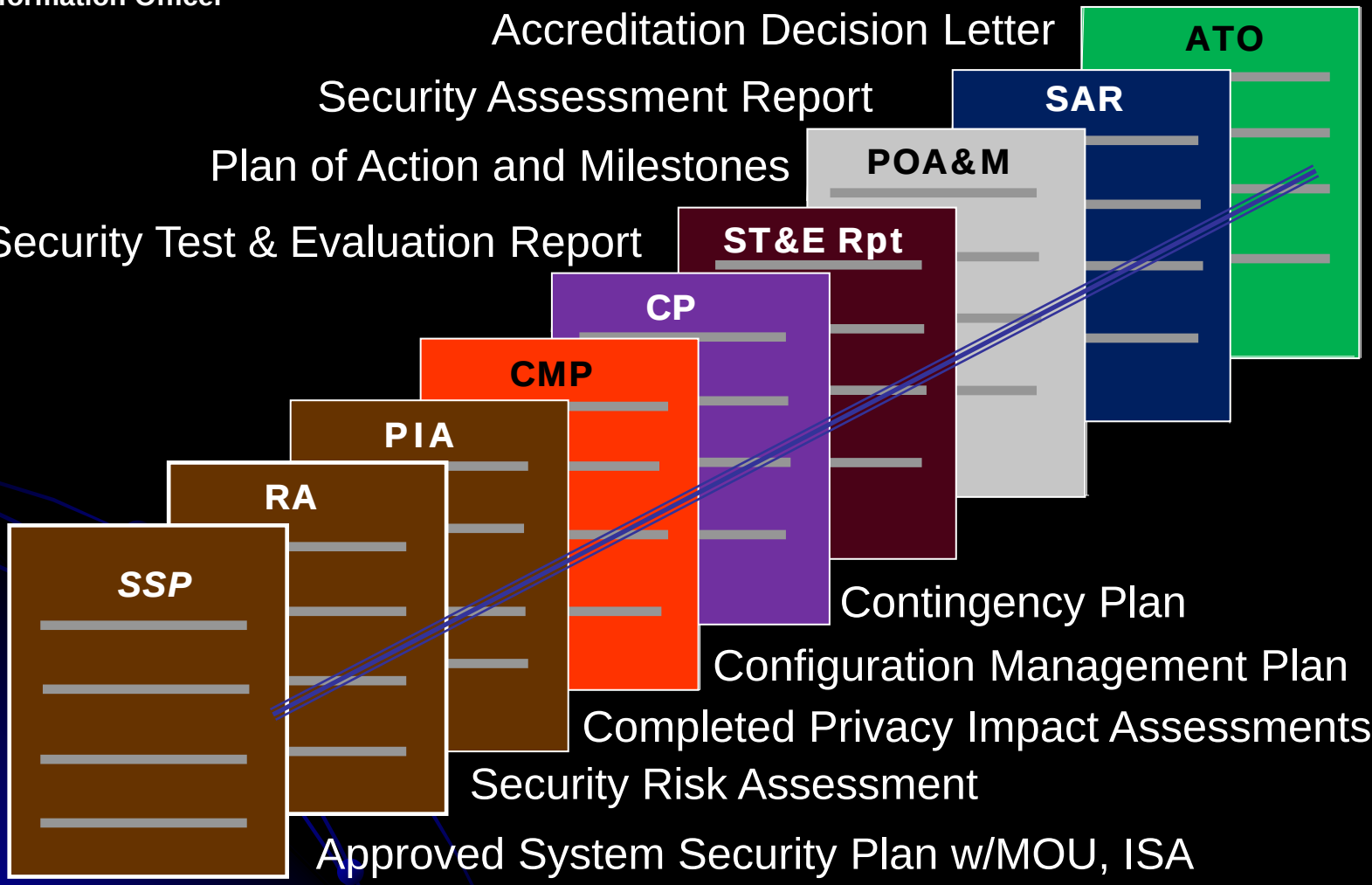
Office of the
Chief Information Officer

Authorize - Accreditation Decision

- AO Accreditation Decision Options
  - Grants Approval to Operate (ATO)
  - Grants Interim Approval to Operate (IATO)
  - Disapproves ATO/IATO based on evaluation of system and mission risk
  - Withdraws existing ATO/IATO on operational system if risk becomes unacceptable

Office of the
Chief Information Officer

Authorize - Accreditation Package Transmission Process



Office of the
Chief Information Officer

Continuous Monitoring

- **Maintain** system configuration per SSP documentation
  - Develop and document a continuous monitoring strategy
- **Assess** controls
- **Review** each system change for security impacts

Office of the
Chief Information Officer

Summary

- AODR Authority, Role and Responsibilities
- Key Cyber Security Terms
- Cyber Security Program Management Structure
- Policy Hierarchy
- Risk Management Framework and Certification and Accreditation Process Relationship
- Pre-AO C&A Package Review
- Accreditation Forms, Boundaries and Common Controls and Inheritance
- Accreditation Decision and Package Transmission
- Continuous Monitoring

- Note: The following slides have been retained to use only if an illustration would be helpful in answering an attendee question

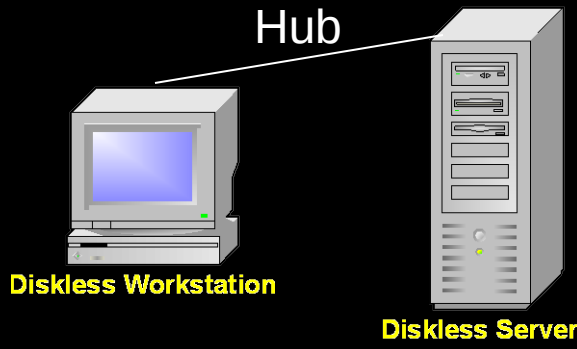
Office of the
Chief Information Officer

Information System

- A system consists of one or more system components
  - Simple: workstation or workstation & printer
  - Complex: workstations, servers, network cables and switches, router, etc.

Diskless Workstation

System Component

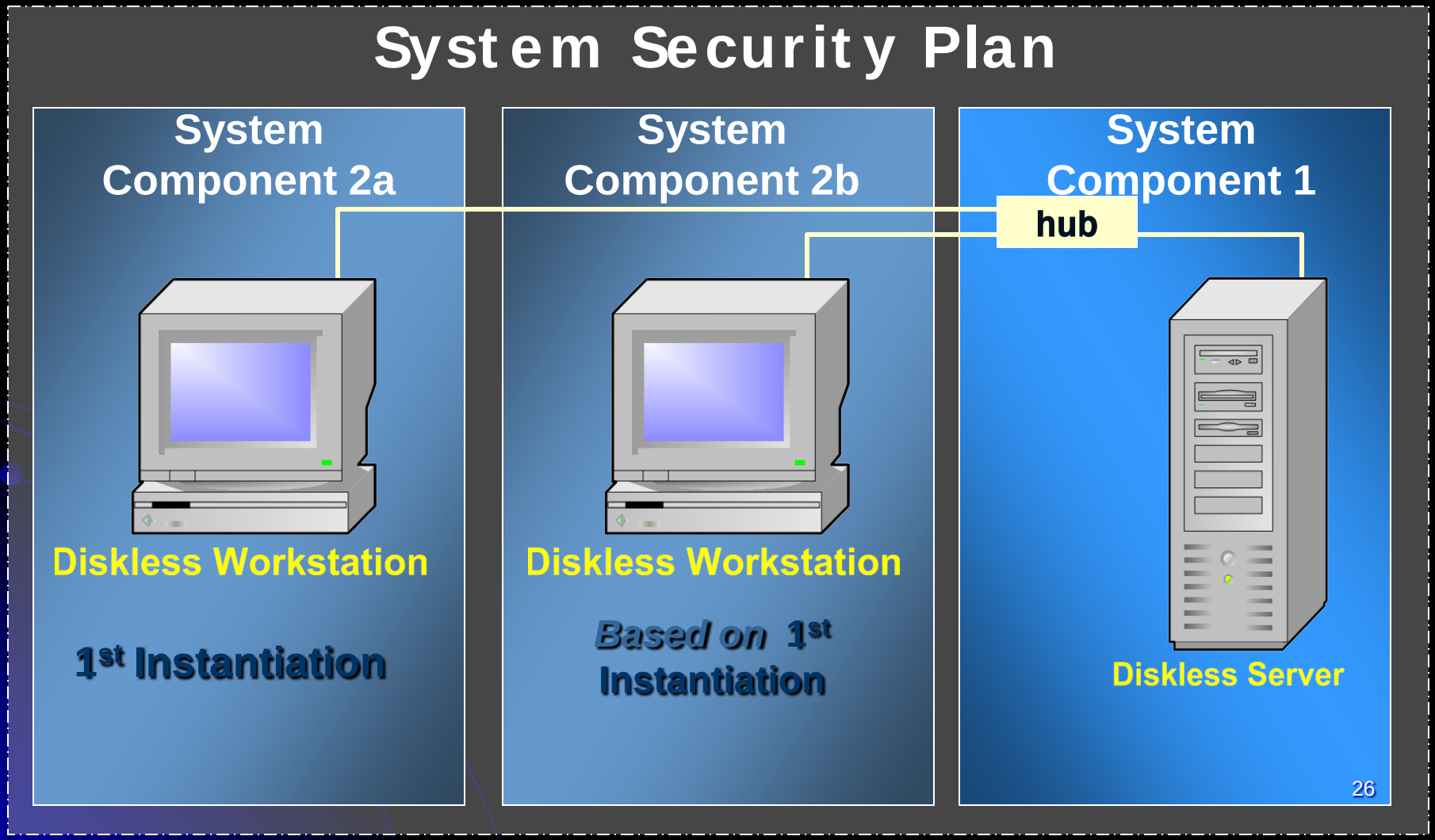


System Component 2

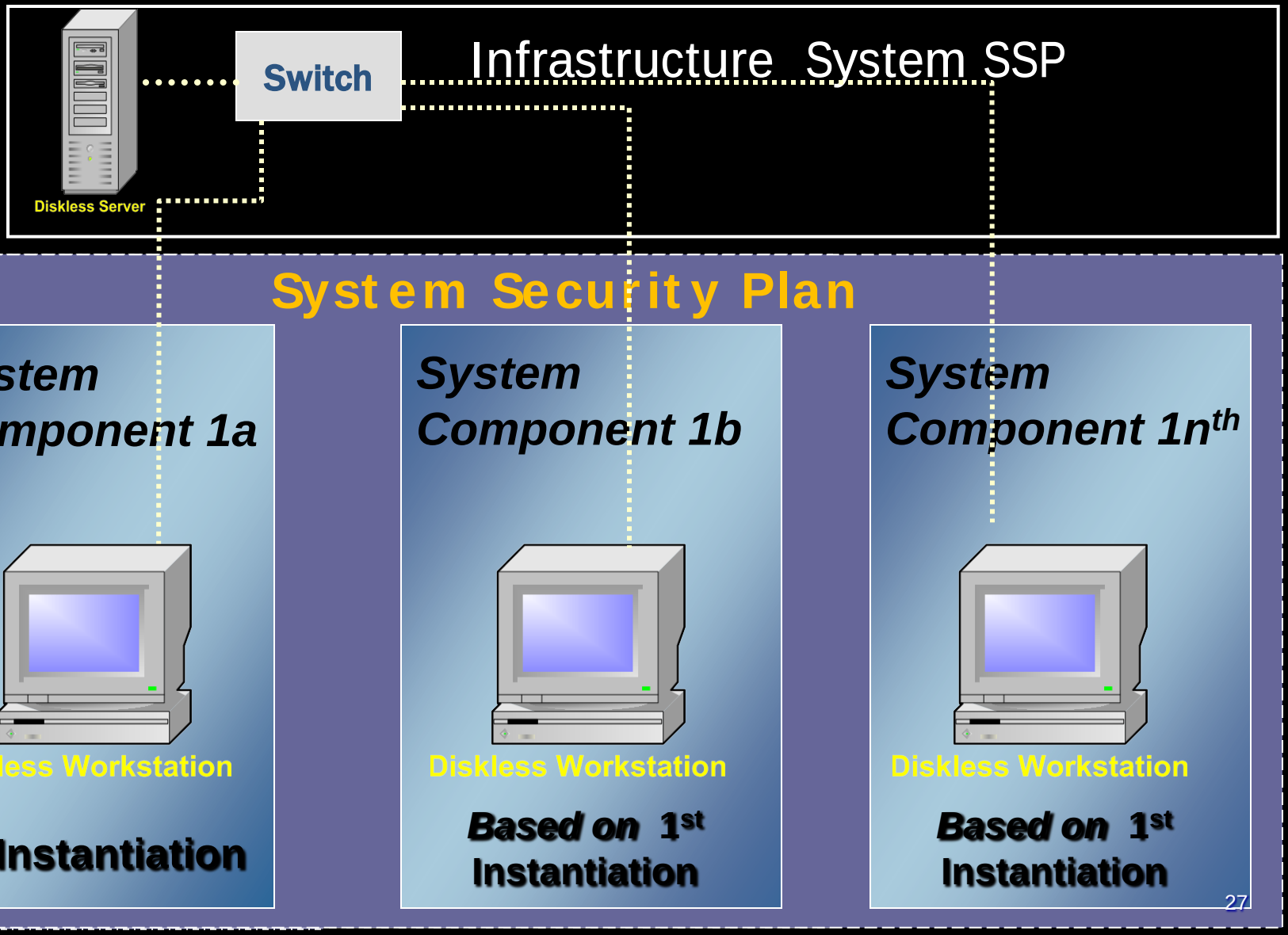
System Component 1

Office of the
Chief Information Officer

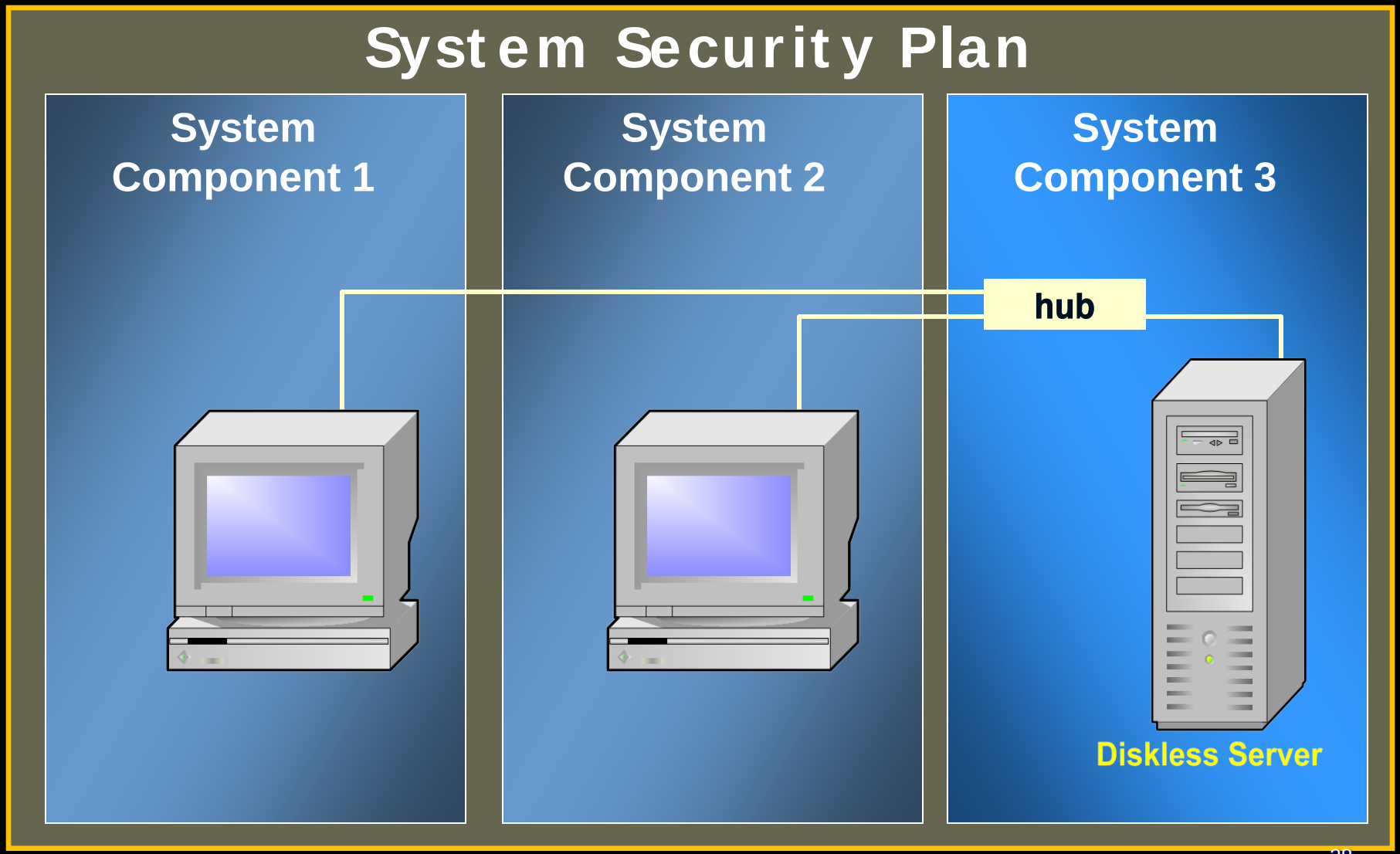
Instantiation Model



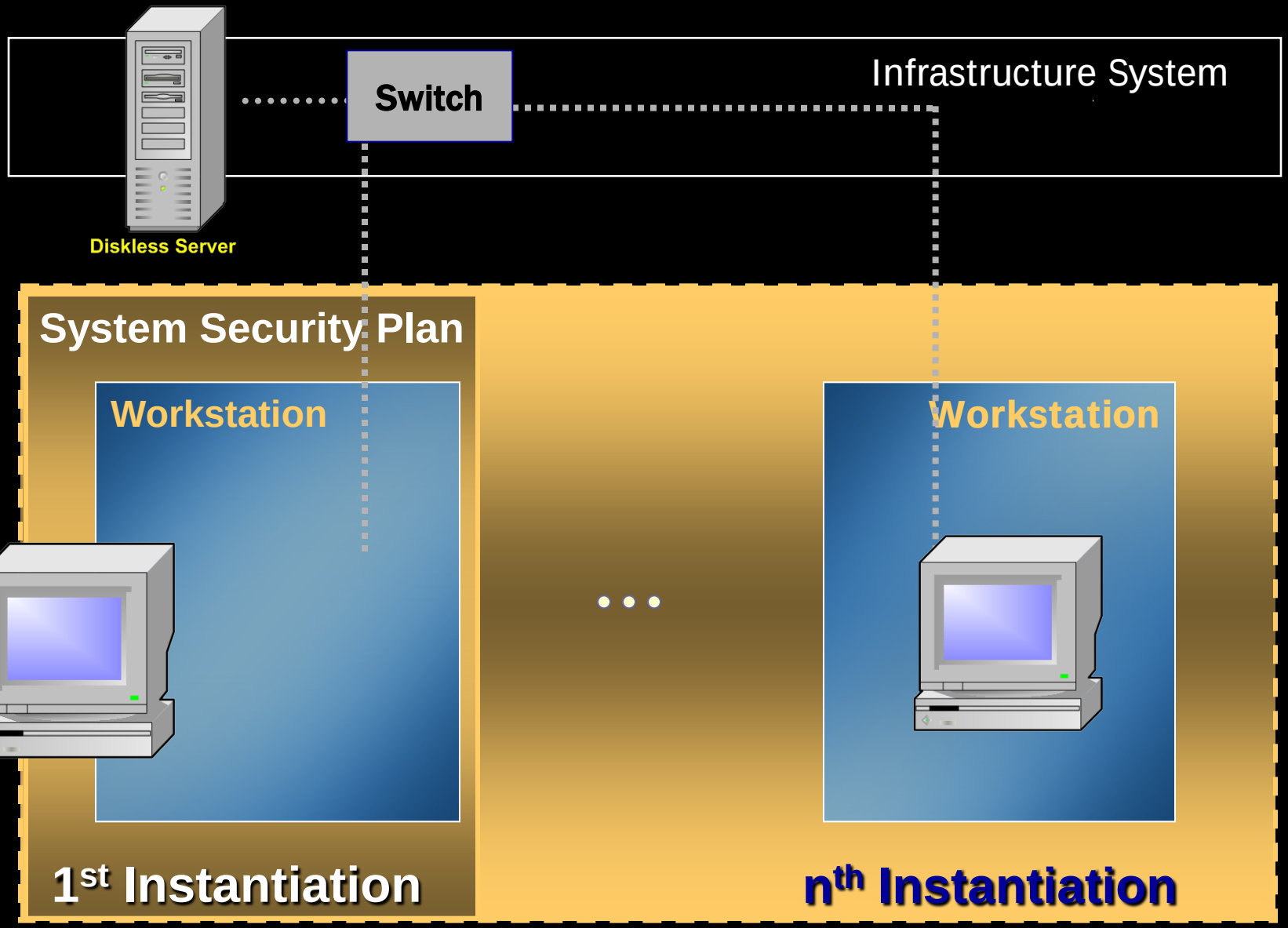
Instantiation Model



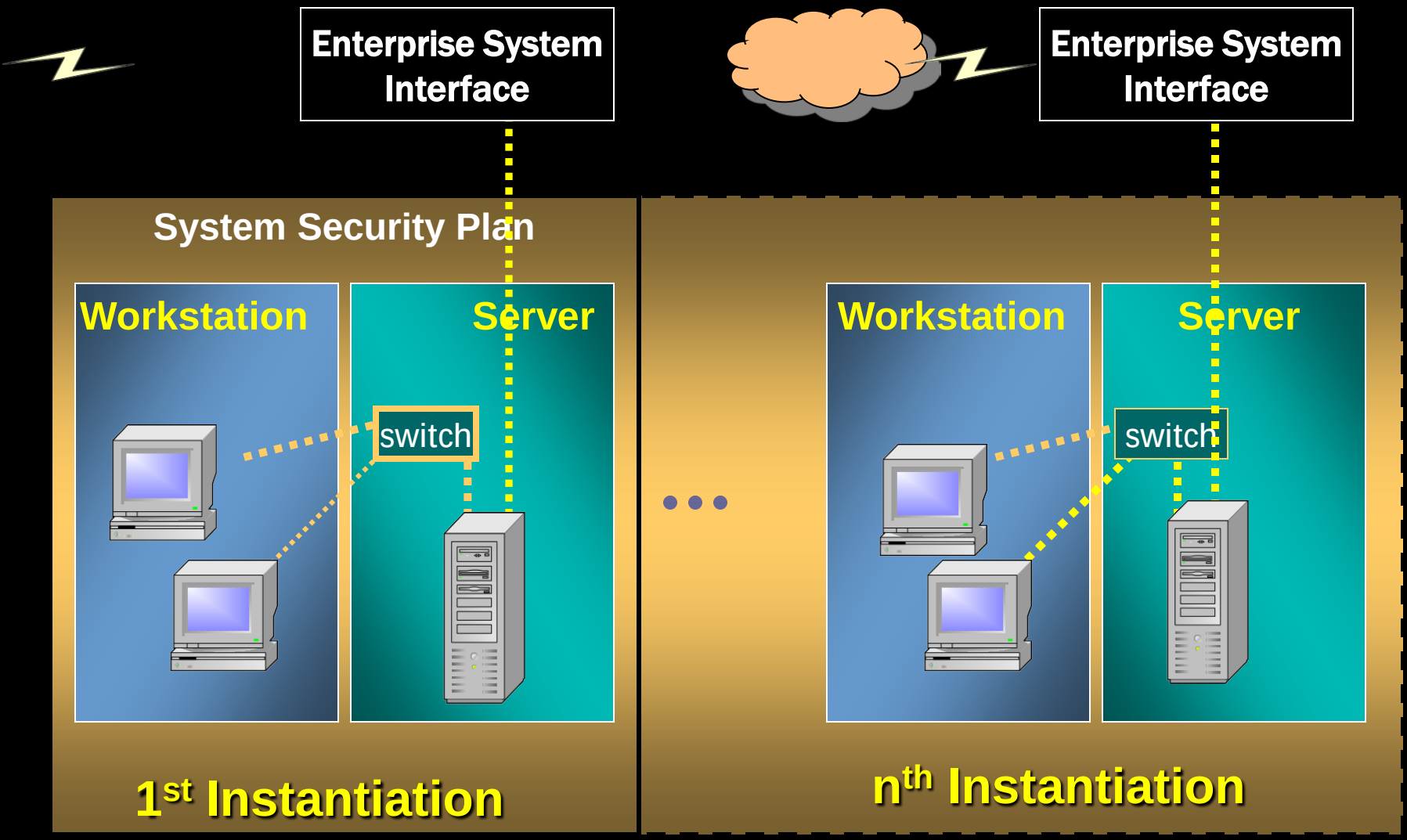
System Form of Accreditation

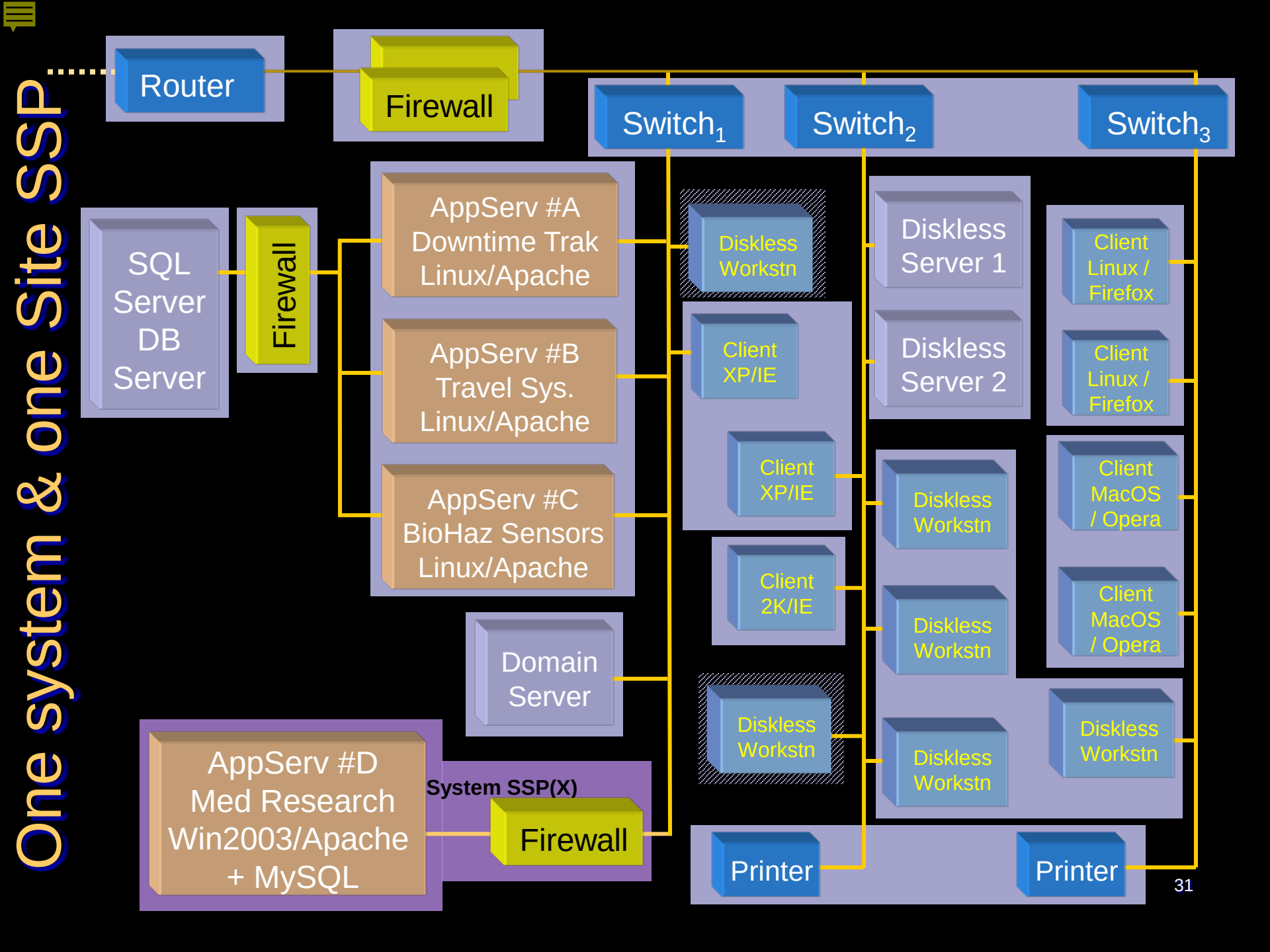


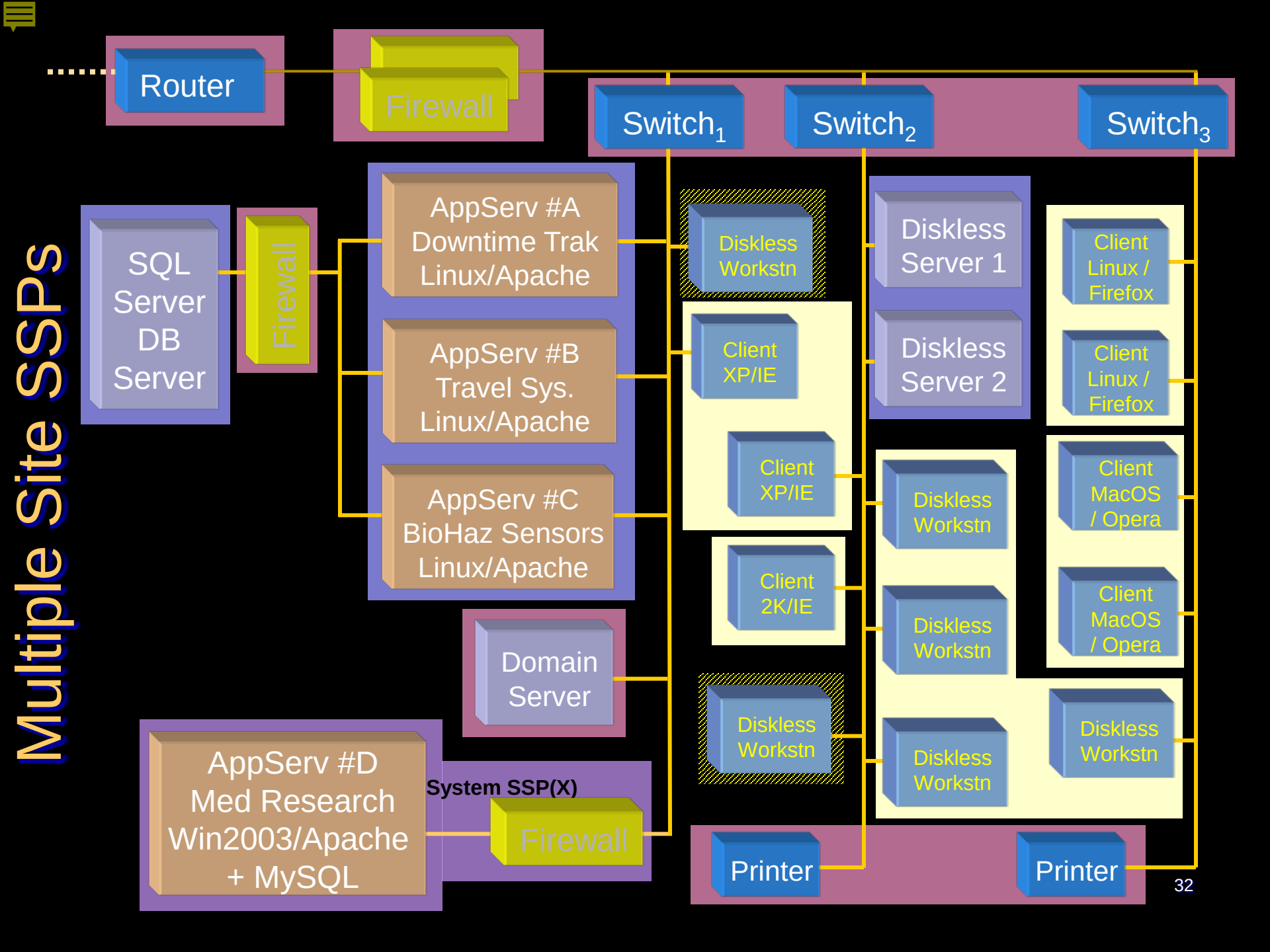
Site Form of Accreditation



Type Form of Accreditation

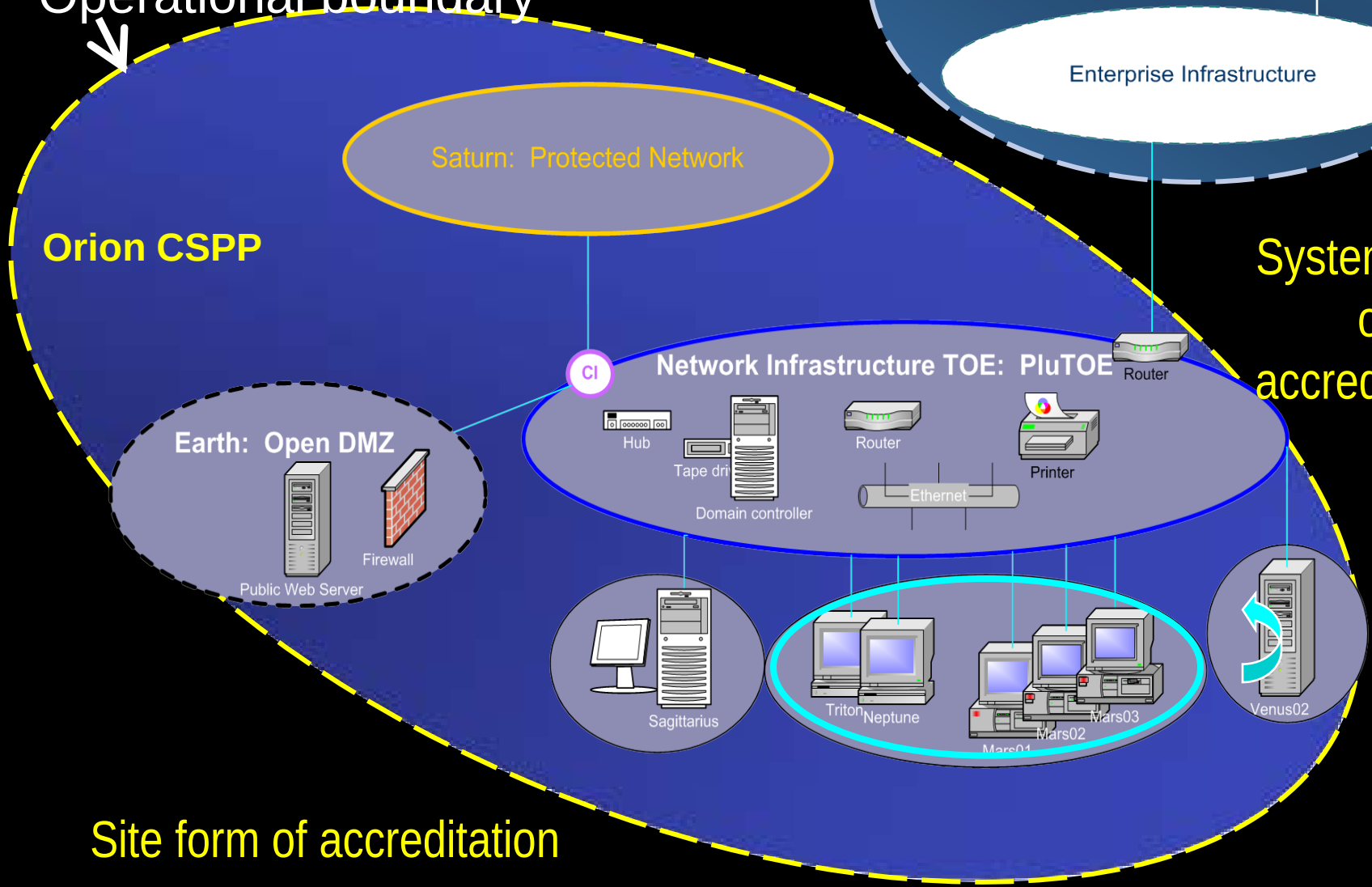



One system & one Site SSP
Router
Firewall
Switch1
Switch2
Switch3
SQL Server DB Server
Firewall
AppServ #A Downtime Trak Linux/Apache
AppServ #B Travel Sys. Linux/Apache
AppServ #C BioHaz Sensors Linux/Apache
Domain Server
AppServ #D Med Research Win2003/Apache + MySQL
System SSP(X)
Firewall
Diskless Workstn
Client XP/IE
Client XP/IE
Client 2K/IE
Diskless Workstn
Diskless Server 1
Diskless Server 2
Diskless Workstn
Diskless Workstn
Diskless Workstn
Client Linux / Firefox
Client Linux / Firefox
Client MacOS / Opera
Client MacOS / Opera
Diskless Workstn
Printer
Printer
31


Multiple Site SSPs
Router
Firewall
Switch1
Switch2
Switch3
SQL Server DB Server
Firewall
AppServ #A Downtime Trak Linux/Apache
AppServ #B Travel Sys. Linux/Apache
AppServ #C BioHaz Sensors Linux/Apache
Domain Server
AppServ #D Med Research Win2003/Apache + MySQL
System SSP(X)
Firewall
Diskless Workstn
Client XP/IE
Client XP/IE
Client 2K/IE
Diskless Workstn
Diskless Server 1
Diskless Server 2
Diskless Workstn
Diskless Workstn
Diskless Workstn
Client Linux / Firefox
Client Linux / Firefox
Client MacOS / Opera
Client MacOS / Opera
Diskless Workstn
Printer
Printer
32

Accreditation Boundaries

Orion Facility
Operational boundary



System form of accreditation

Site form of accreditation