AO Role-Based Training

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

Objectives

Gain Understanding and Working Knowledge of:

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

Who is the AO?

Authorizing Official (AO)

- Senior DOE Managers are AOs by DOE Order
  - Can delegate AO authority to other Federal Employee(s)
  - Delegation must be in writing – by name or position
  - Delegated AO cannot re-delegate the authority
  - AO authority covers all Operating Units under his/her jurisdiction

What does the AO do?

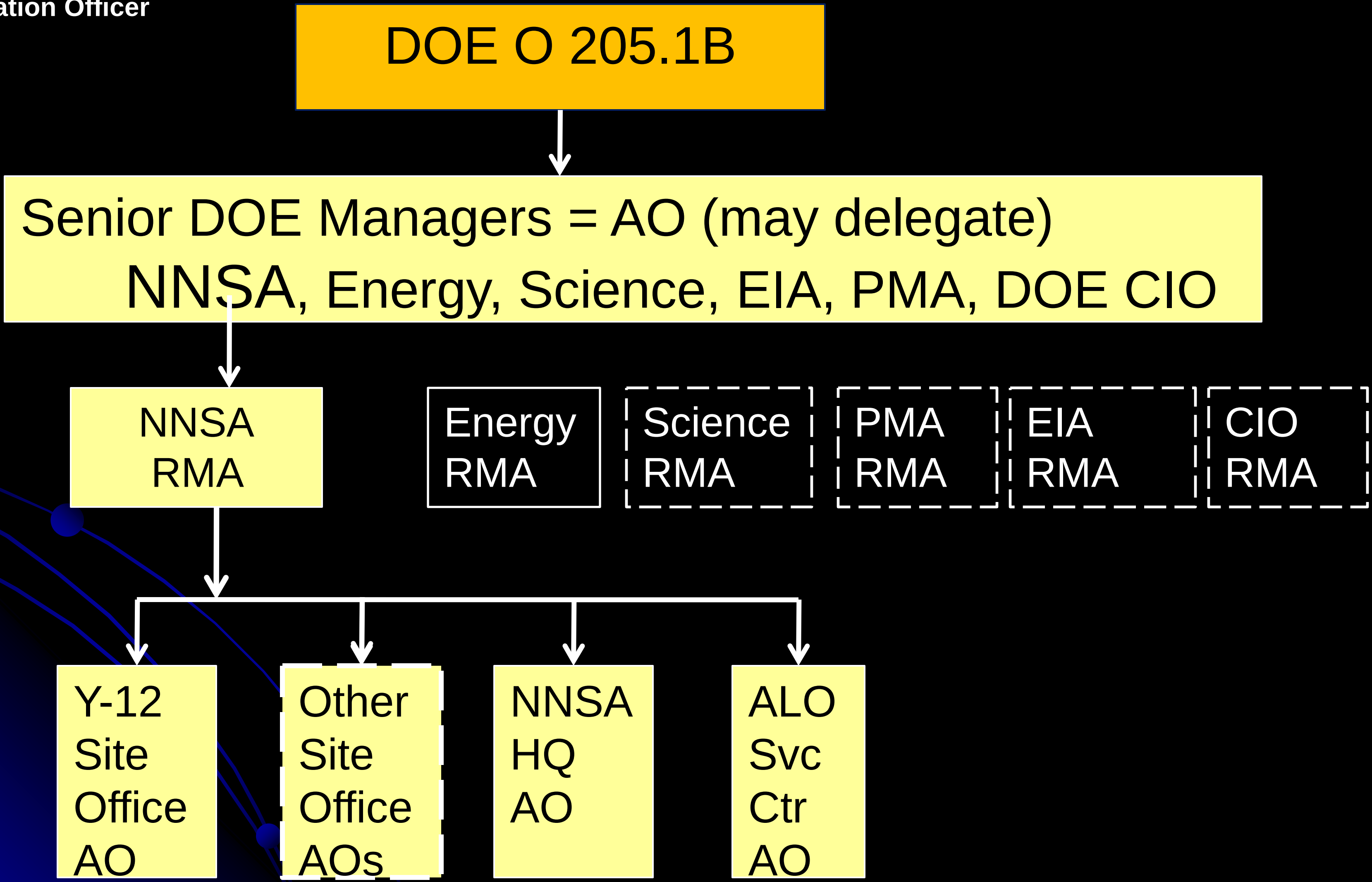
The AO is

- Responsible for Protection of Information and Information Technology for the DOE
- Responsible for Oversight of Operating Unit Cyber Security Program which includes
  - DOE Organizations
  - Contractors
  - Sub-contractors
- Fully accountable for information system operation at an acceptable level of risk

What does the AO do?

- Responsible for Incident Management Implementation
  - Assign or assist with assigning appropriate incident characterization
  - Ensure incidents are categorized and reported in accordance with incident reporting requirements
  - Provide incident coordination with law enforcement other DOE organizations

AO Structure



DOE O 205.1B

Senior DOE Managers = AO (may delegate)
NNSA, Energy, Science, EIA, PMA, DOE CIO

NNSA RMA

Energy RMA

Science RMA

PMA RMA

EIA RMA

CIO RMA

Y-12 Site Office AO

Other Site Office AOs

NNSA HQ AO

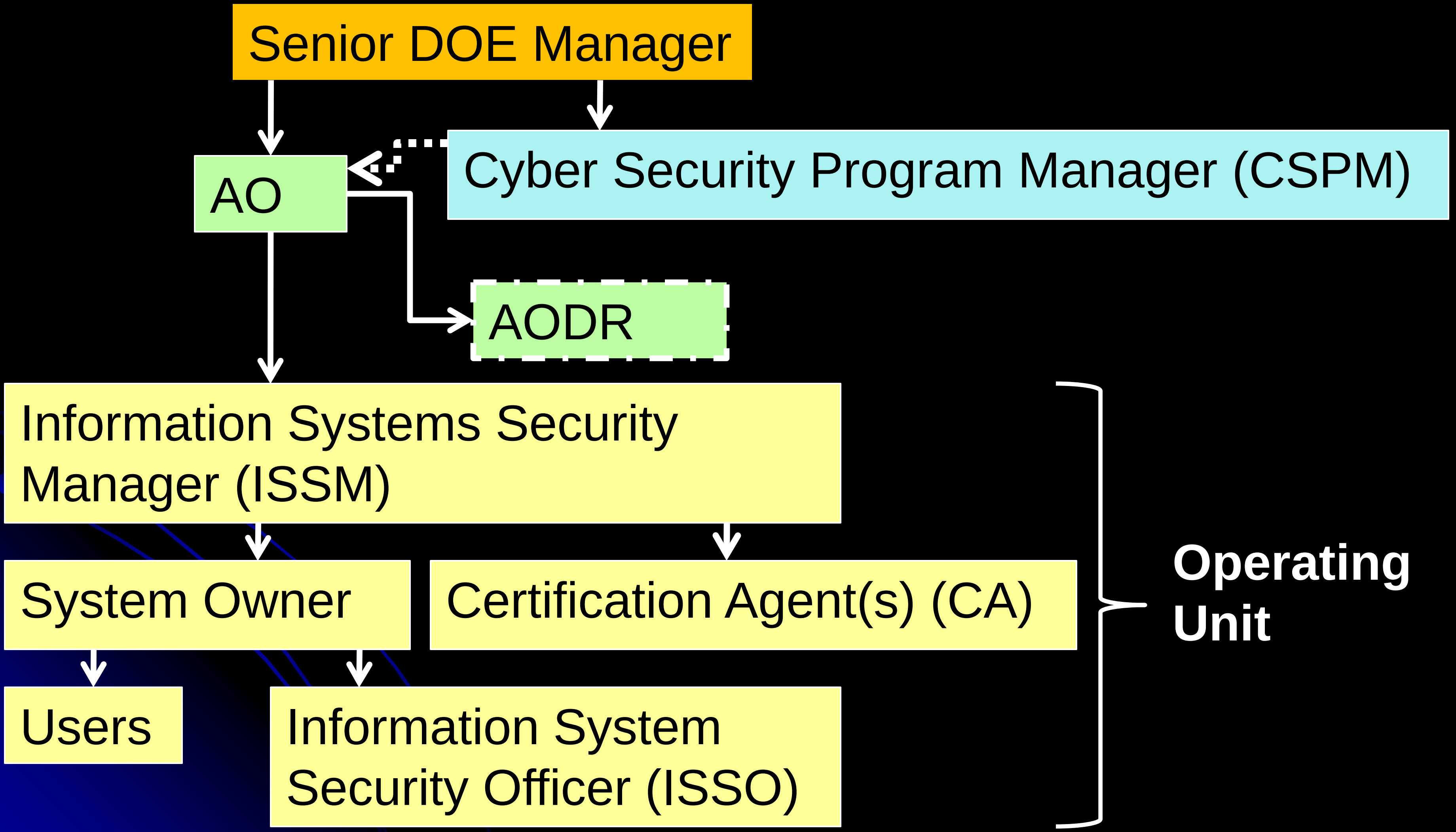
ALO Svc Ctr AO

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



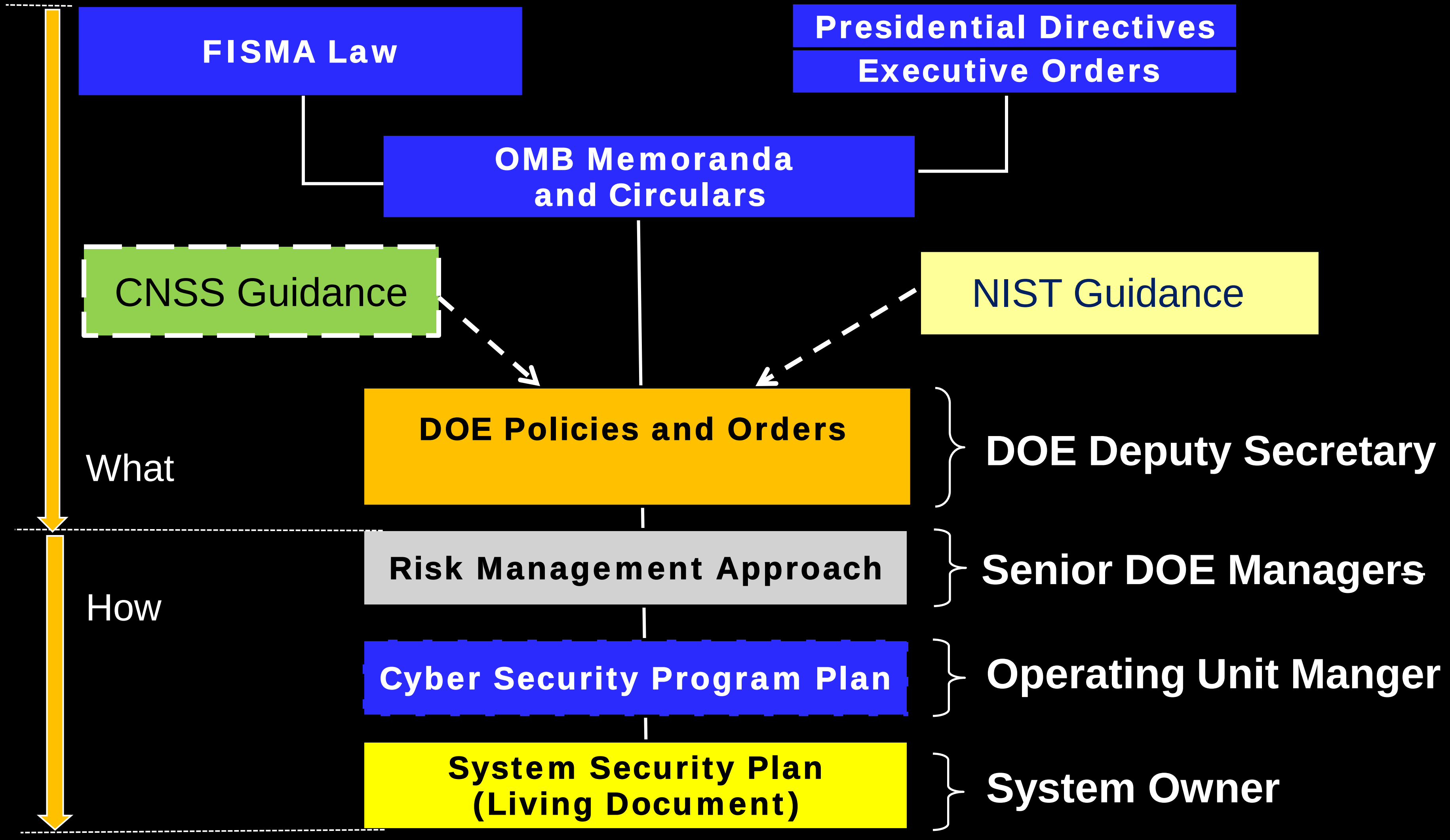
Senior DOE Manager
AO
Cyber Security Program Manager (CSPM)
AODR
Information Systems Security Manager (ISSM)
System Owner
Certification Agent(s) (CA)
Users
Information System Security Officer (ISSO)
Operating Unit

Cyber Security Management Structure

DOE Cyber Security Management Structure Key Roles

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

The Policy Hierarchy



FISMA Law

Presidential Directives

Executive Orders

OMB Memoranda
and Circulars

CNSS Guidance

NIST Guidance

What

DOE Policies and Orders

DOE Deputy Secretary

How

Risk Management Approach

Senior DOE Managers

Cyber Security Program Plan

Operating Unit Manger

System Security Plan
(Living Document)

System Owner

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

The Policy Hierarchy

Key Documents

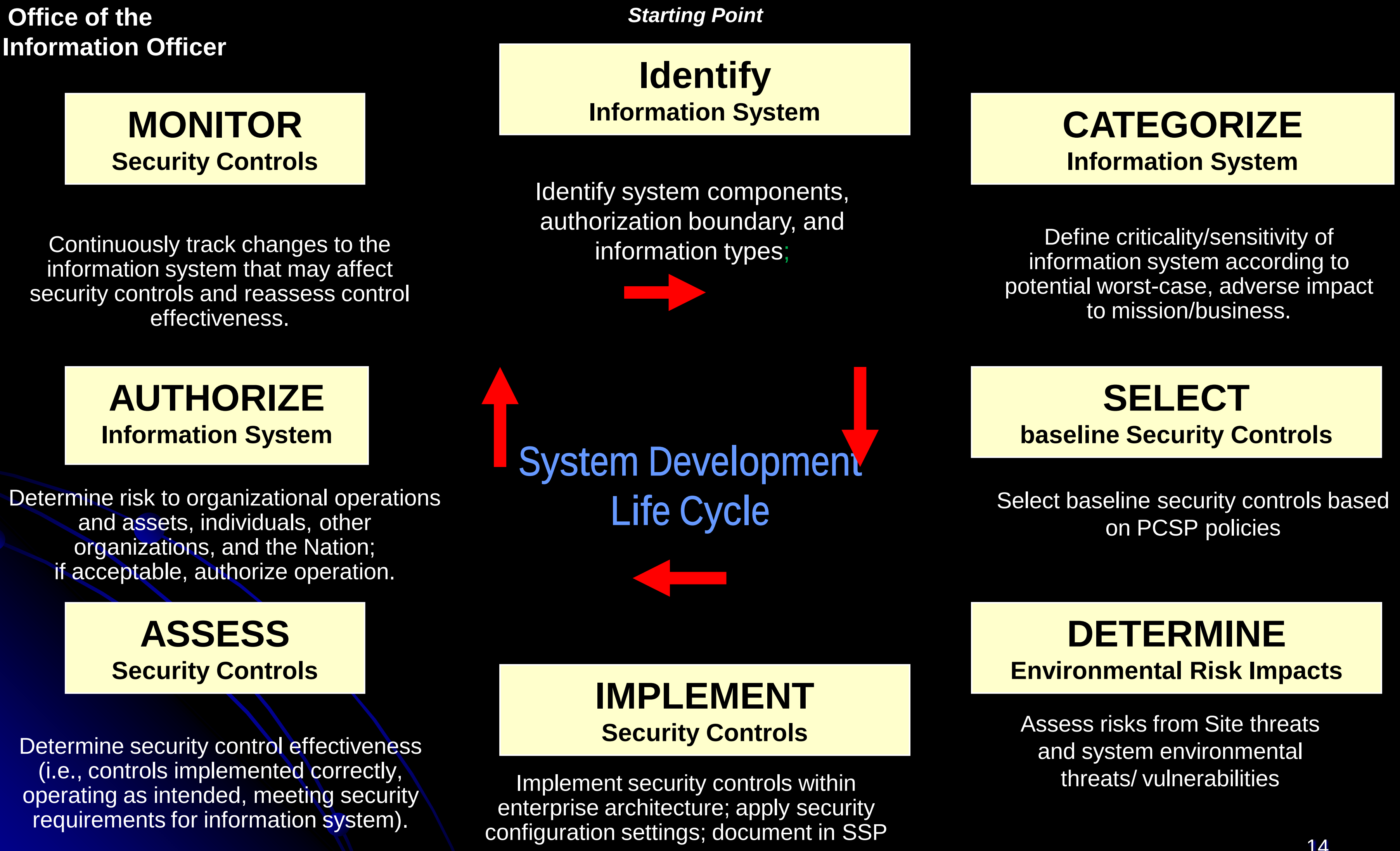
- Risk Management Approach (RMA)
- Cyber Security Program Plan (CSPP) - Optional
- System Security Plan (SSP)

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.

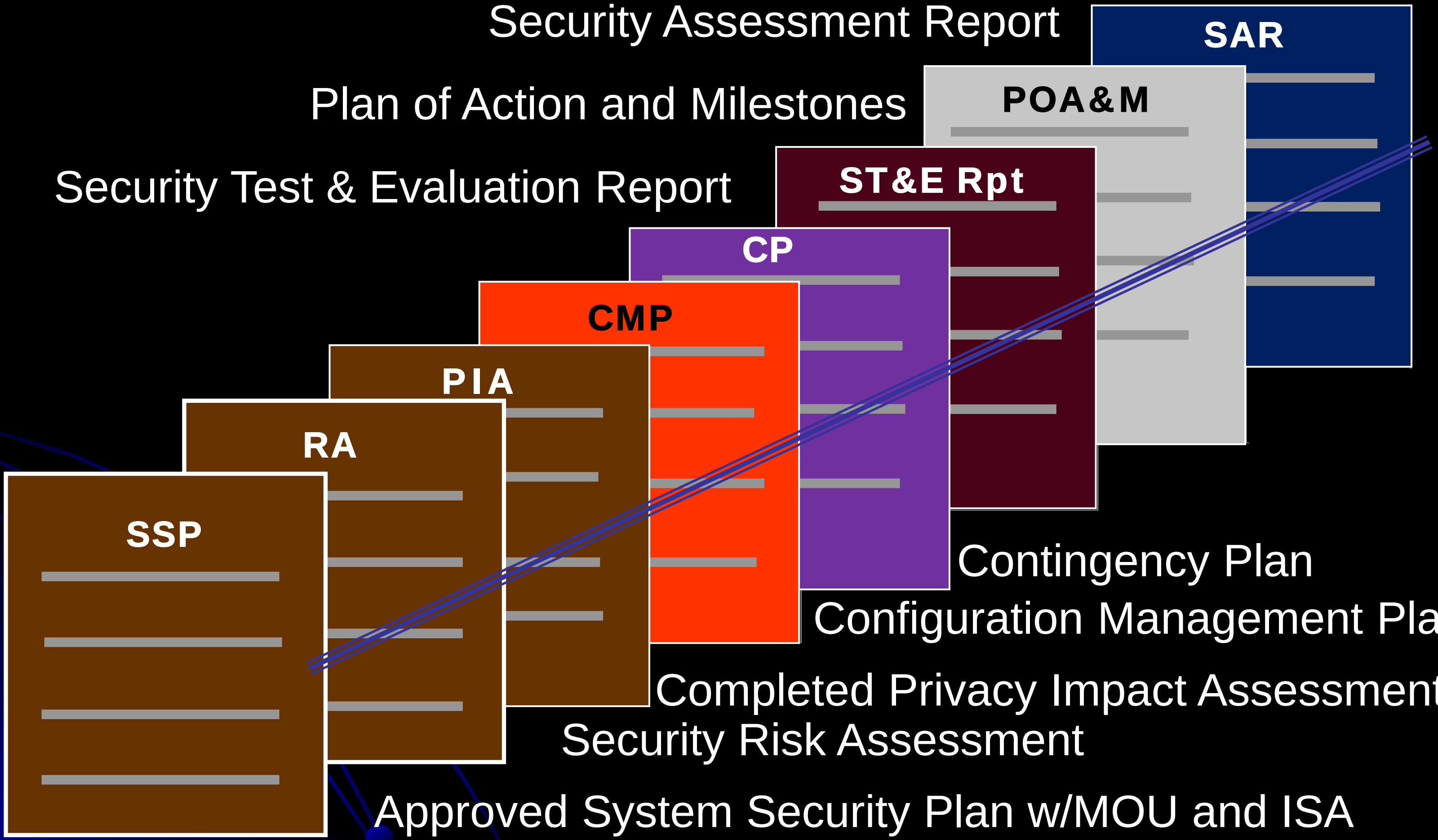
System Development Life Cycle

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

Assess - Assemble C & A Package



Security Assessment Report

Plan of Action and Milestones

Security Test & Evaluation Report

Contingency Plan

Configuration Management Plan

Completed Privacy Impact Assessments

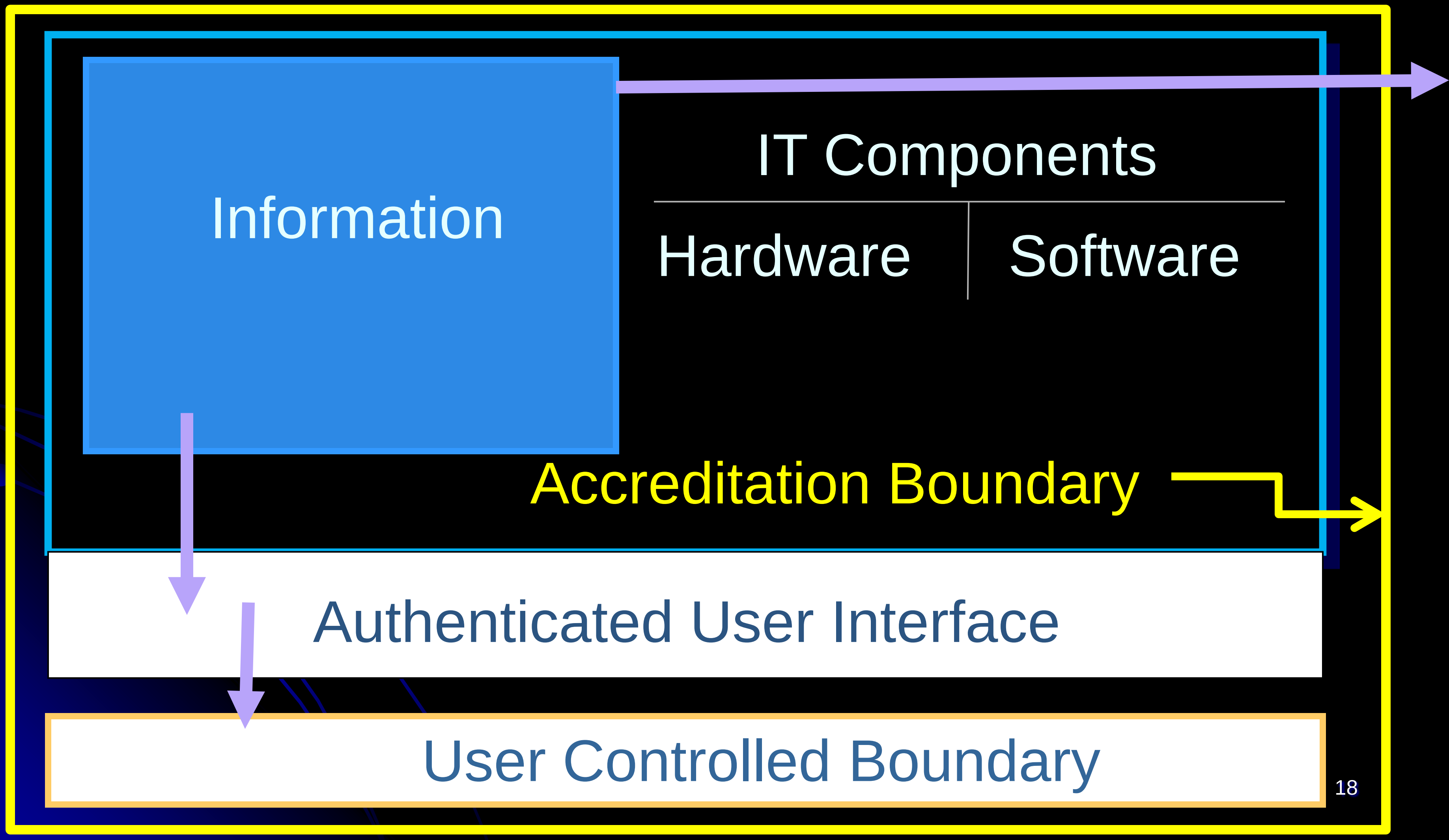
Security Risk Assessment

Approved System Security Plan w/MOU and ISA

OA C&A Package Review

- Determines that all package components are present
- Examines:
  - Authorization/Accreditation Boundaries
  - Common Controls
- Determines that Risk is acceptable to Mission, system and information assets, Nation
- Determines that POA&Ms are generated and acceptable for corrective actions

Information System Accreditation Boundaries



Information

IT Components

Hardware

Software

Accreditation Boundary

Authenticated User Interface

User Controlled Boundary

Common Controls and Inheritance

- Many security controls are common to all systems in an Operating Unit

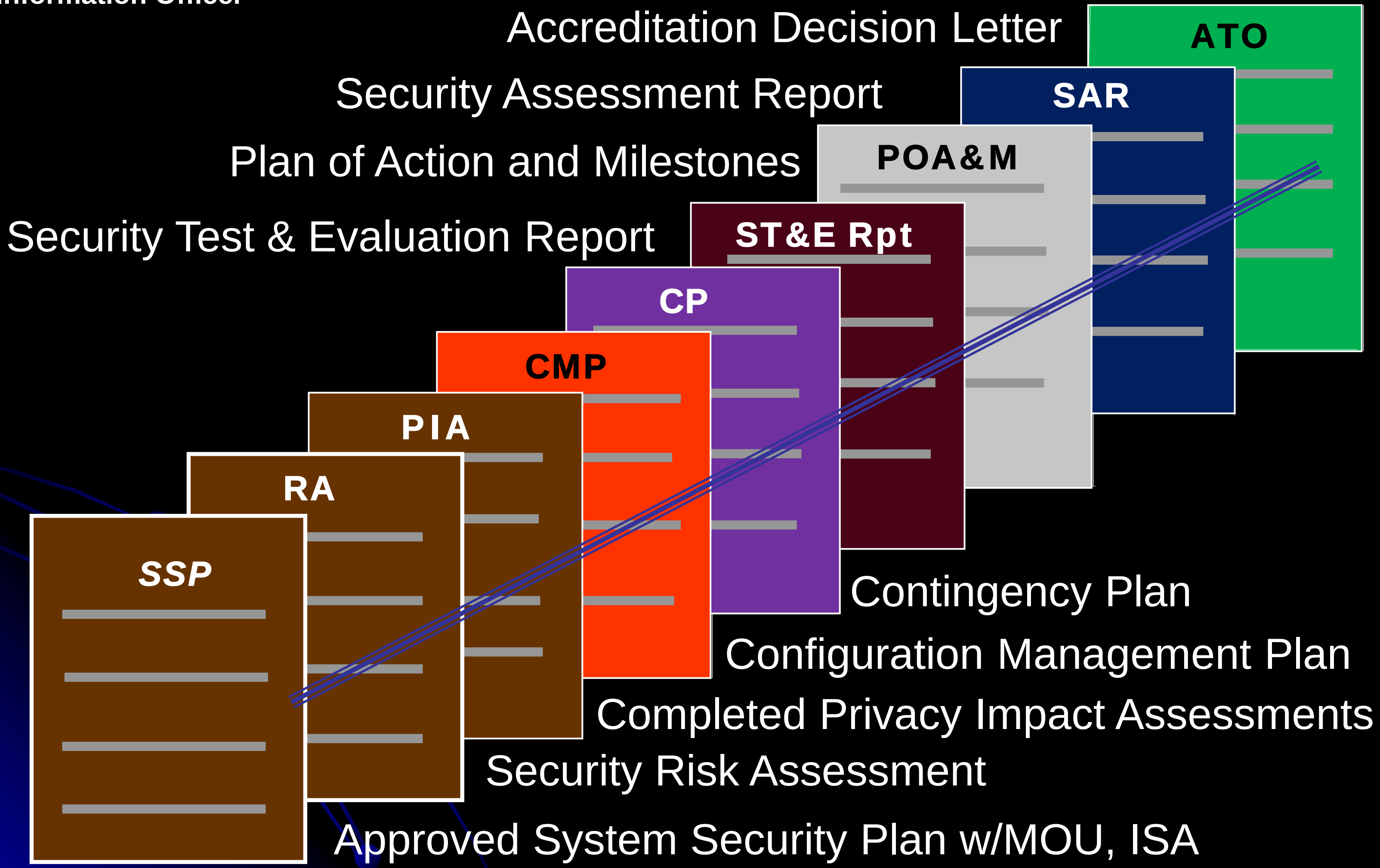
- Common Security Controls can be implemented on one system and other systems can inherit the control implementation

- Inherited security controls ATO must be validated

Authorize - Accrediation 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

Authorize - Accreditation Package Transmission Process



Accreditation Decision Letter

Security Assessment Report

Plan of Action and Milestones

Security Test & Evaluation Report

Contingency Plan

Configuration Management Plan

Completed Privacy Impact Assessments

Security Risk Assessment

Approved System Security Plan w/MOU, ISA

Continuous Monitoring

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

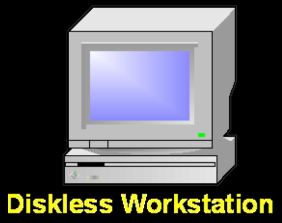
Summary

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

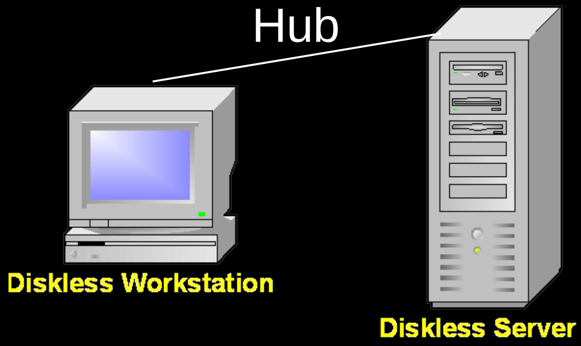
- Note: The following slides have been retained to use only if an illustration would be helpful in answering an attendee question

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.



System Component

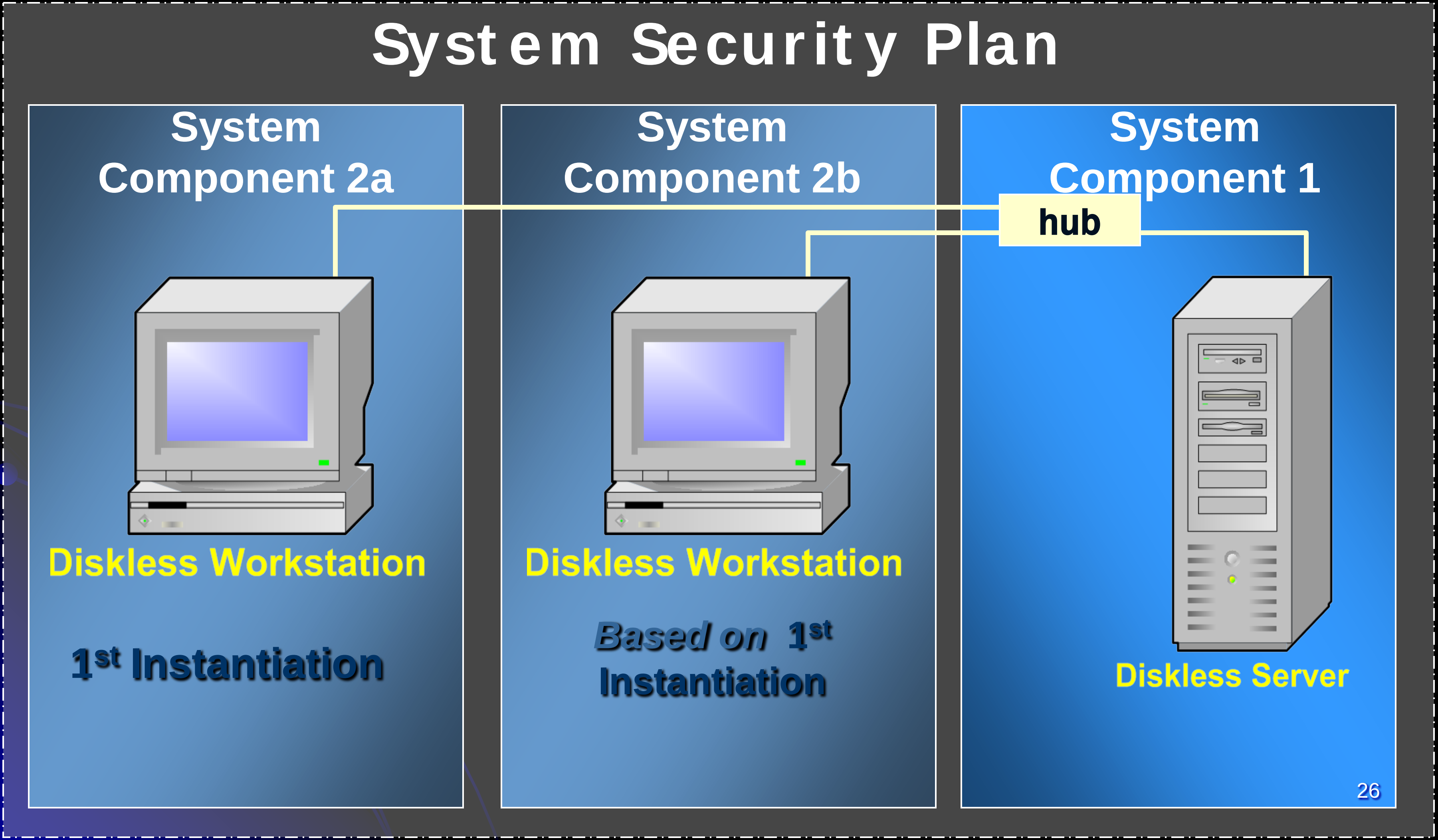


Hub

System Component 2

System Component 1

Instantiation Model



System Security Plan

System Component 2a

Diskless Workstation

1st Instantiation

System Component 2b

Diskless Workstation

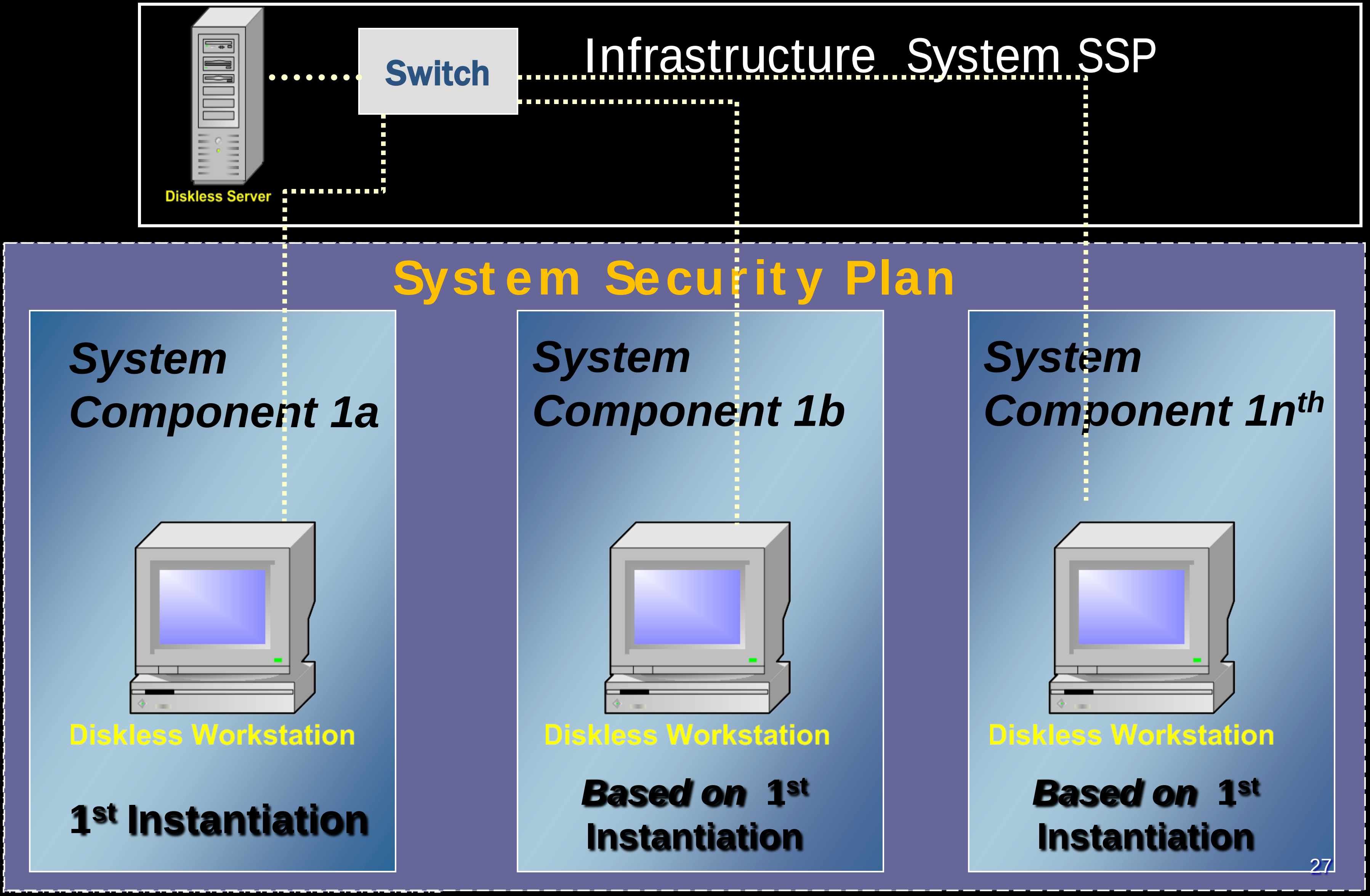
Based on 1st Instantiation

System Component 1

hub

Diskless Server

Instantiation Model



Diskless Server

Switch

Infrastructure System SSP

System Security Plan

System Component 1a

Diskless Workstation

1st Instantiation

System Component 1b

Diskless Workstation

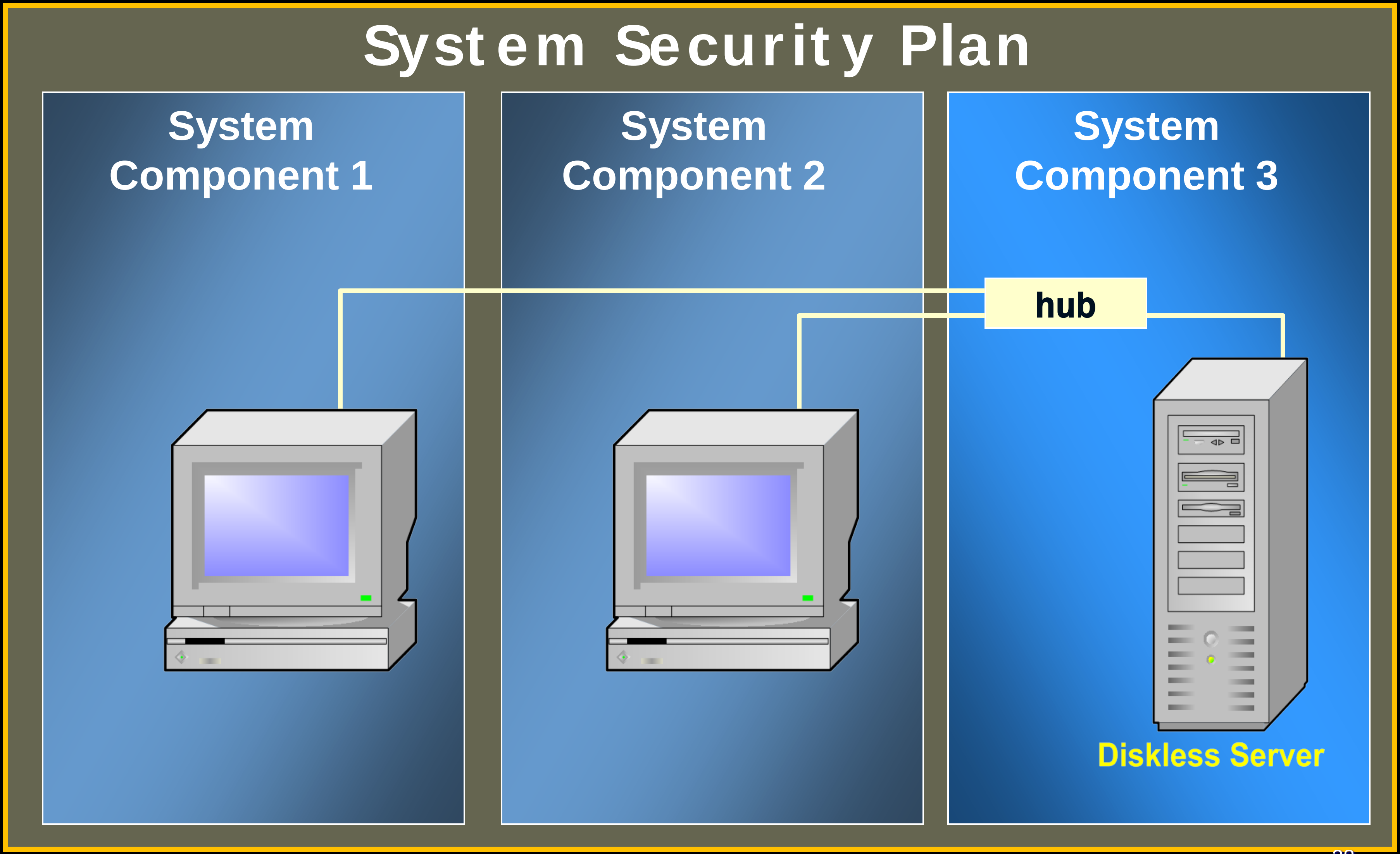
Based on 1st Instantiation

System Component 1nth

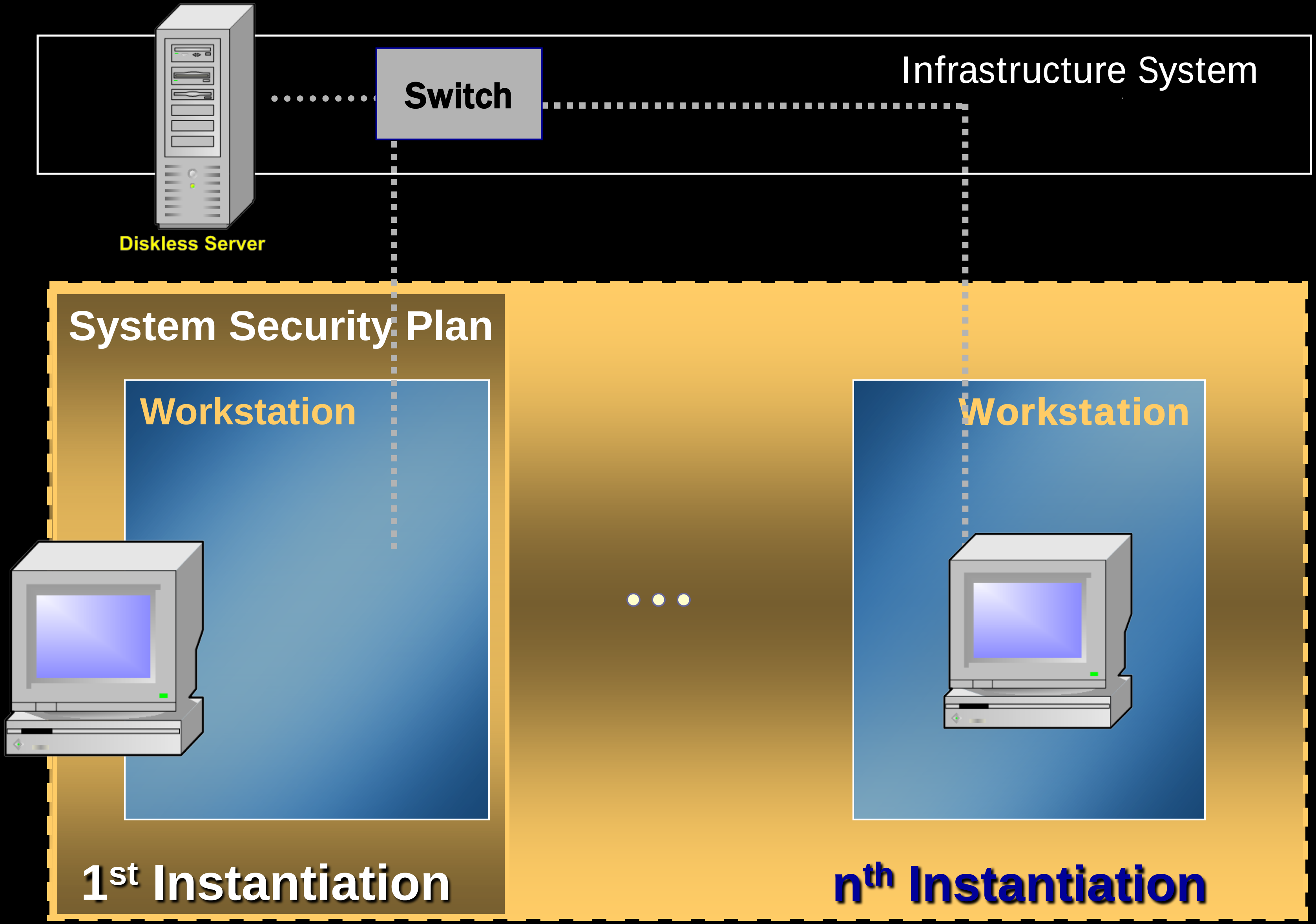
Diskless Workstation

Based on 1st Instantiation

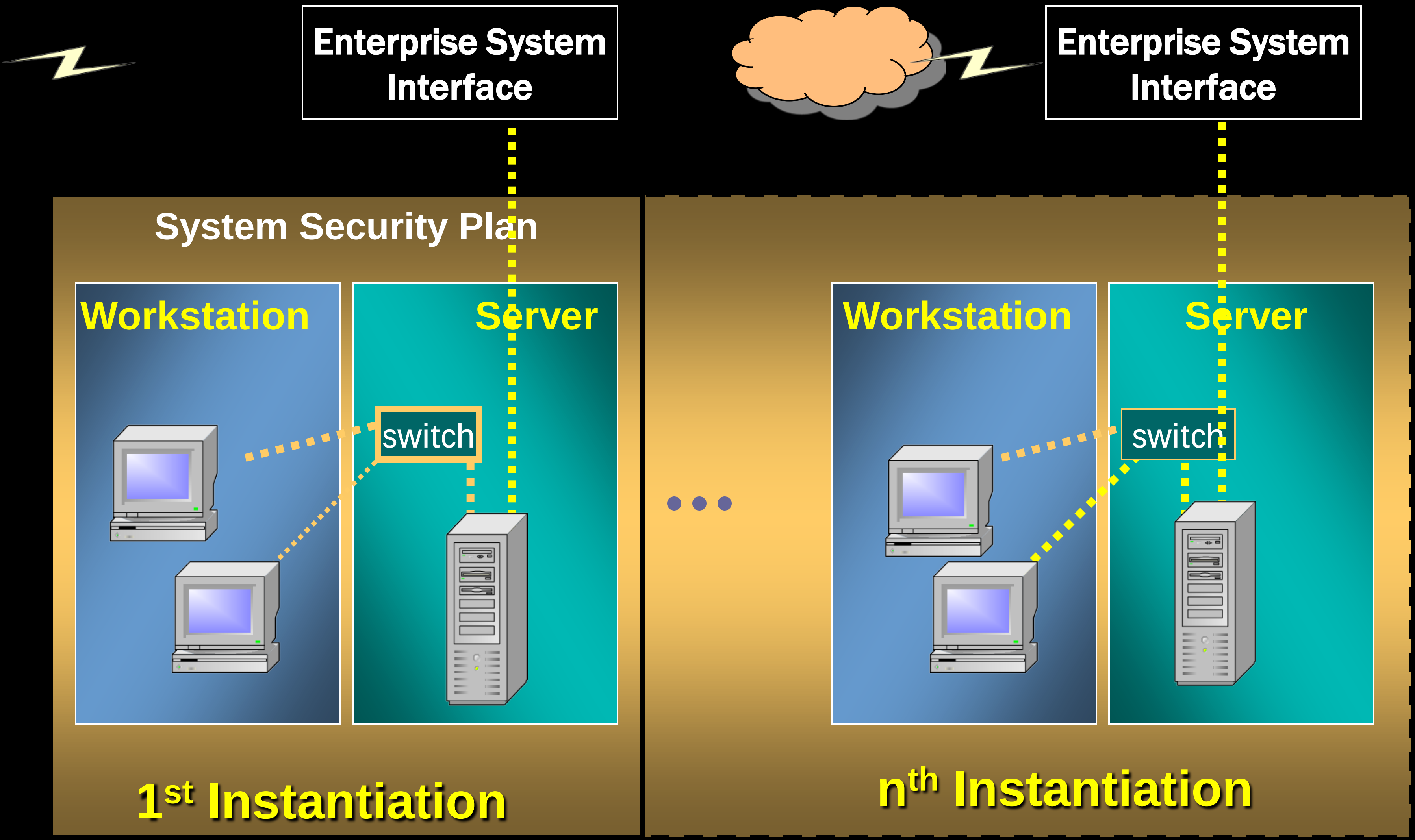
System Form of Accreditation



Site Form of Accreditation



Type Form of Accreditation



Enterprise System Interface

Enterprise System Interface

System Security Plan

Workstation

Server

switch

1st Instantiation

Workstation

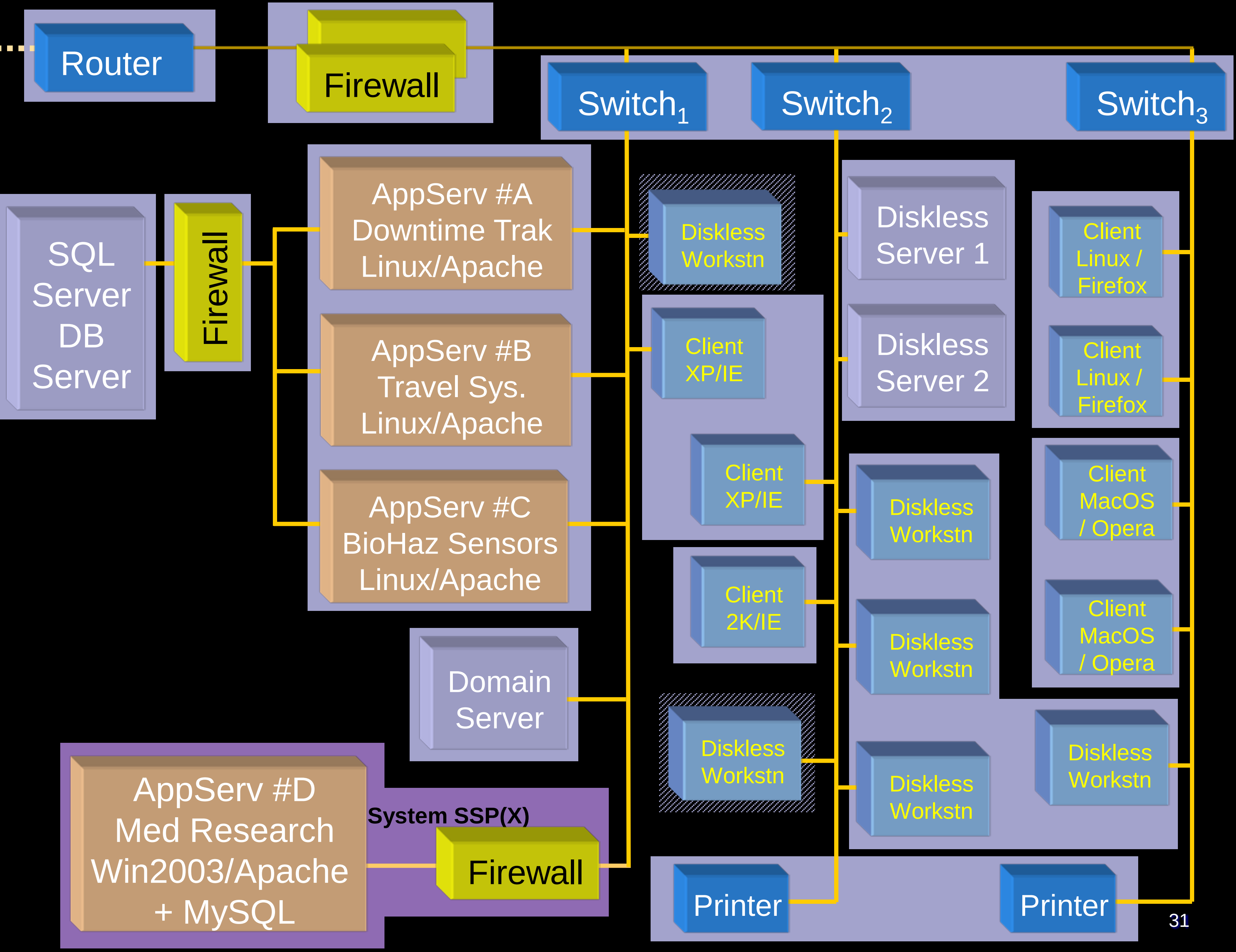
Server

switch

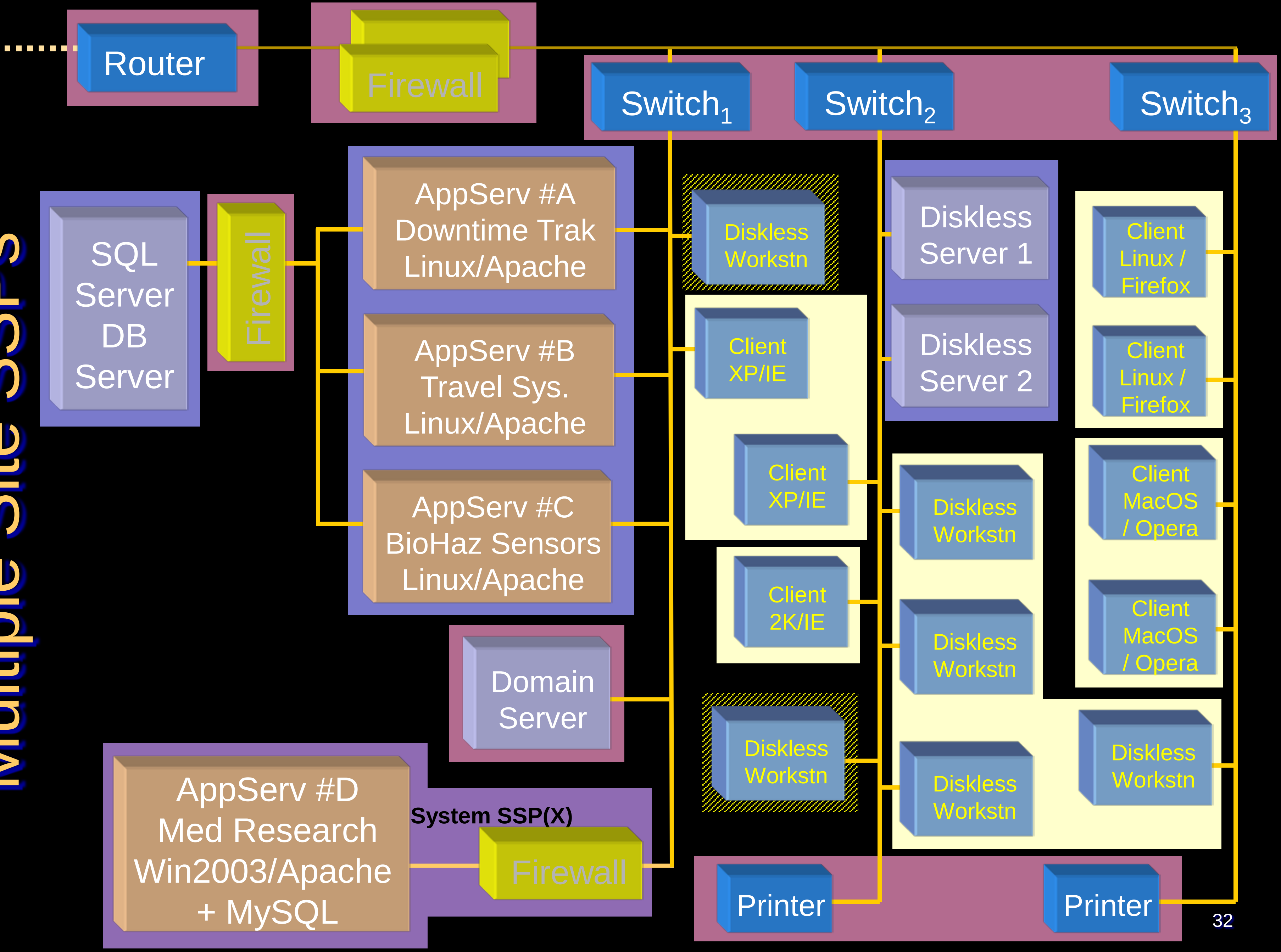
• • •

nth Instantiation

One system & one Site SSP



Multiple Site SSPs



Router

Firewall

Switch$_1$

Switch$_2$

Switch$_3$

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

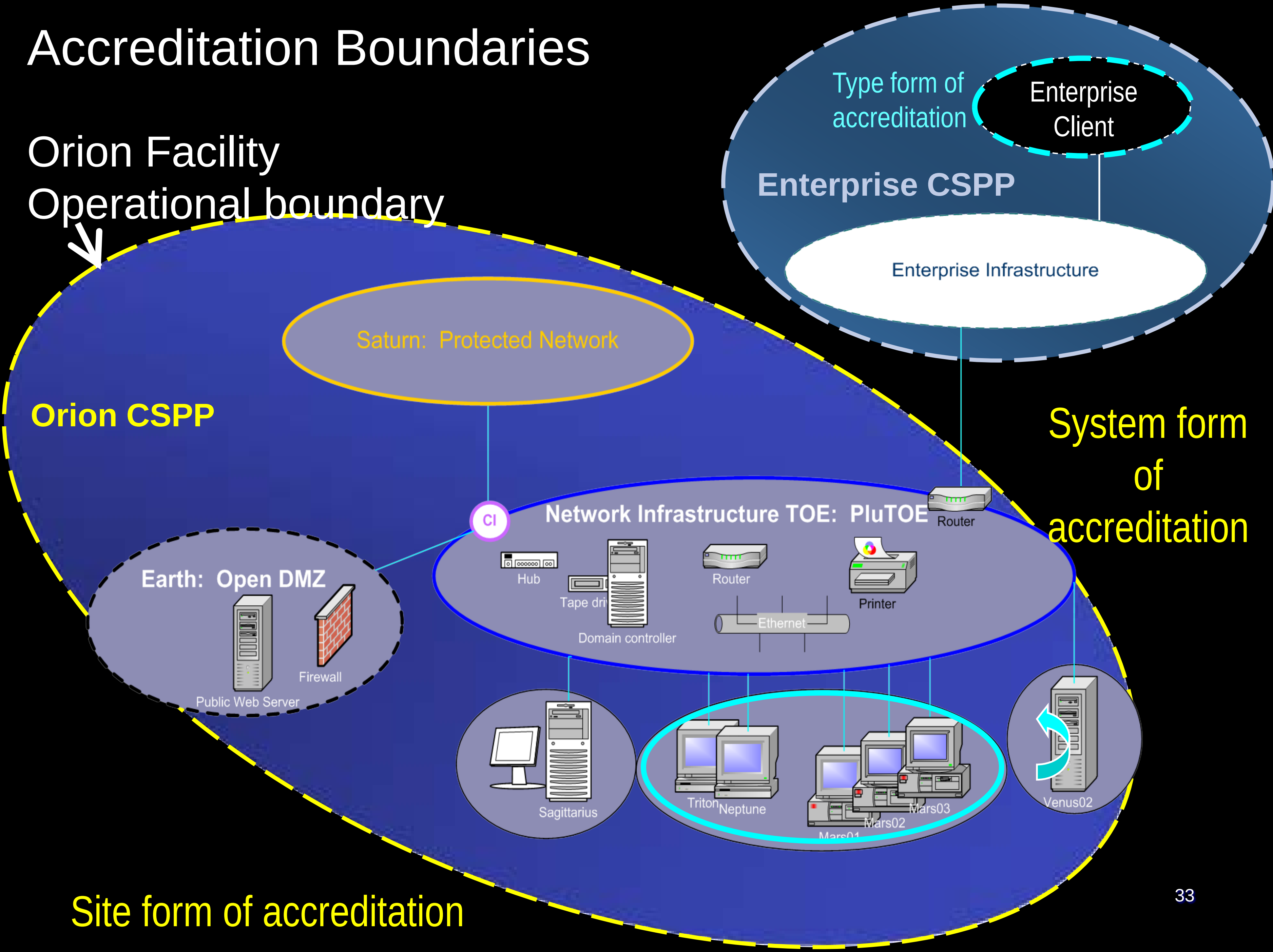
Client MacOS / Opera

Diskless Workstn

Printer

Printer

Accreditation Boundaries



Orion Facility
Operational boundary

Type form of accreditation

Enterprise Client

Enterprise CSPP

Enterprise Infrastructure

Saturn: Protected Network

Orion CSPP

System form of accreditation

Network Infrastructure TOE: PluTOE

Earth: Open DMZ

Site form of accreditation