



---

# Information Security

Rob McKinney



# Topics

---

- **HIPAA Security**
- **Certification and Accreditation**
- **Websense**
- **Incident Response**
- **Certificates**
- **Blaster/Welchia Infection**
- **Security Training Requirements**
- **COOP**



# HIPAA Security – Final Rule

---

## ■ Covered entities

- Health Plans
- Health Care Clearinghouses
- Health Care Providers

## ■ Scope

- More limited than the Privacy Rule
- Applies only to Protected Health Information (PHI) in electronic form (E PHI)



# Basic Requirements

---

- **Ensure the CIA of all EPHI**
- **Protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI**
- **Protect against any reasonably anticipated unauthorized uses or disclosures of EPHI not allowed or required by Privacy Rule**
- **Ensure compliance by workforce**
- **Document, implement, and maintain policies, procedures, and “measures”**
- **Documentation must be kept for six years**



# Standards and Implementation Specifications

---

- **Entities must comply with Standards**
- **Implementation Specifications - a specific requirement or instruction for implementing a “standard.”** – HHS HIPAA Compliance Guide, October 29, 2003
  - **Required – must be implemented**
  - **Addressable – each covered entity must determine whether each measure (or some equivalent alternative measure) is “reasonable and appropriate” for that entity.** – HHS HIPAA Compliance Guide, October 29, 2003



# Summary of Security Safeguards

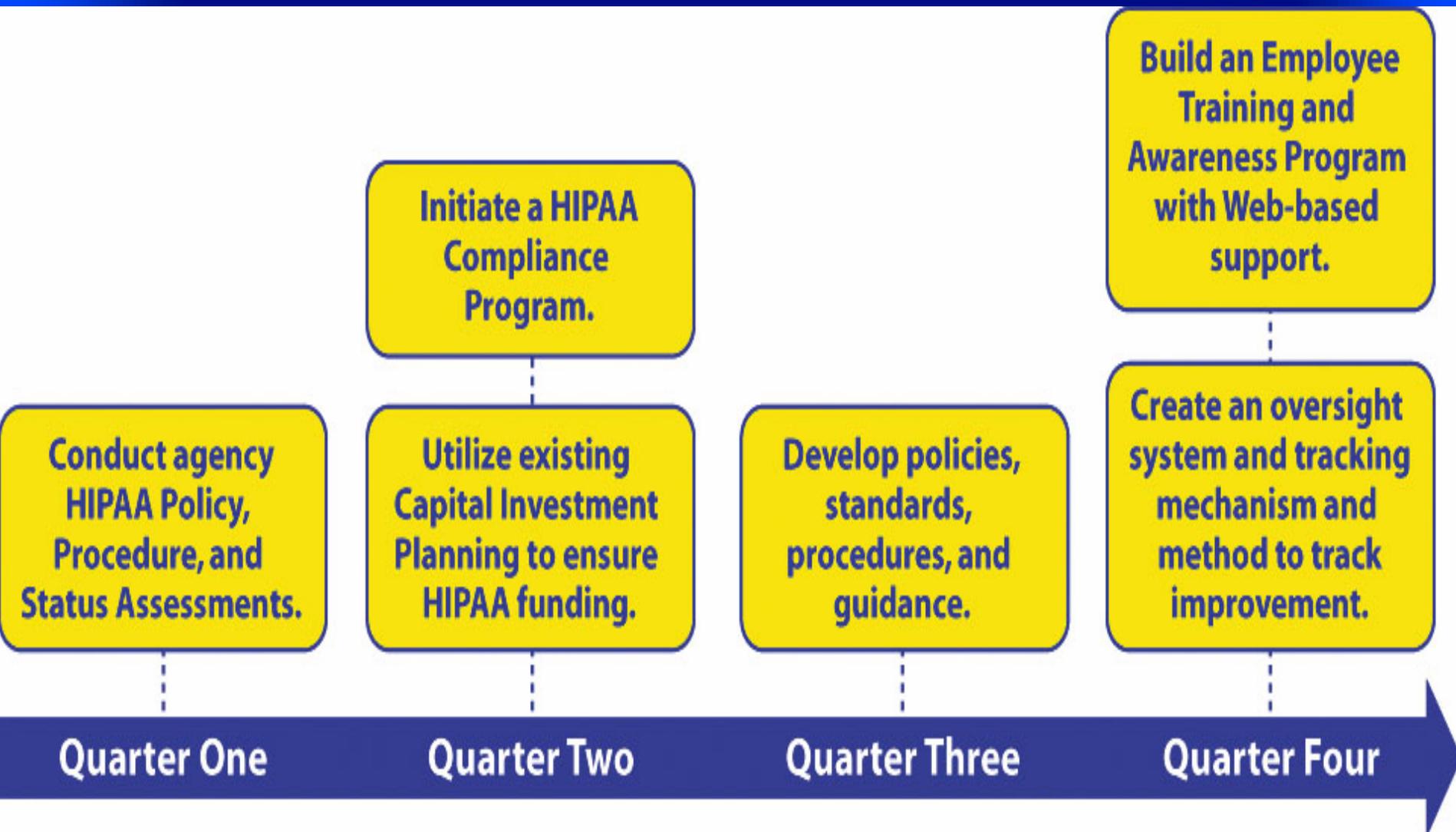
– HHS HIPAA Compliance Guide, October 29, 2003

STANDARD	Implementation Specifications		
	Required	Addressable	Total
Security Management Process	4	0	4
Assigned Security Responsibility	+ 0	+ 0	+ 0
Work Force Security	+ 0	+ 3	+ 3
Information Access Management	+ 1	+ 2	+ 3
Security Awareness and Training	+ 0	+ 4	+ 4
Security Incident Procedures	+ 1	+ 0	+ 1
Contingency Plan	+ 3	+ 2	+ 5
Evaluation	+ 0	+ 0	+ 0
Business Associate Contracts and Other Arrangements	+ 1	+ 0	+ 1
<b><i>SUBTOTALS—ADMINISTRATIVE SAFEGUARDS</i></b>	<b>= 10</b>	<b>= 11</b>	<b>= 21</b>
Facility Access Controls	0	4	4
Workstation Use	+ 0	+ 0	+ 0
Workstation Security	+ 0	+ 0	+ 0
Device and Media Controls	+ 2	+ 2	+ 4
<b><i>SUBTOTALS—PHYSICAL SAFEGUARDS</i></b>	<b>= 2</b>	<b>= 6</b>	<b>= 8</b>
Access Controls	2	2	4
Audit Controls	+ 0	+ 0	+ 0
Integrity	+ 0	+ 1	+ 1
Person or Entity Authentication	+ 0	+ 0	+ 0
Transmission Security	+ 0	+ 2	+ 2
<b><i>SUBTOTALS—TECHNICAL SAFEGUARDS</i></b>	<b>= 2</b>	<b>= 5</b>	<b>= 7</b>
<b>GRAND TOTALS</b>	<b>14</b>	<b>22</b>	<b>36</b>



# HHS Implementation Timeline – HHS

HIPAA Compliance Guide, October 29, 2003





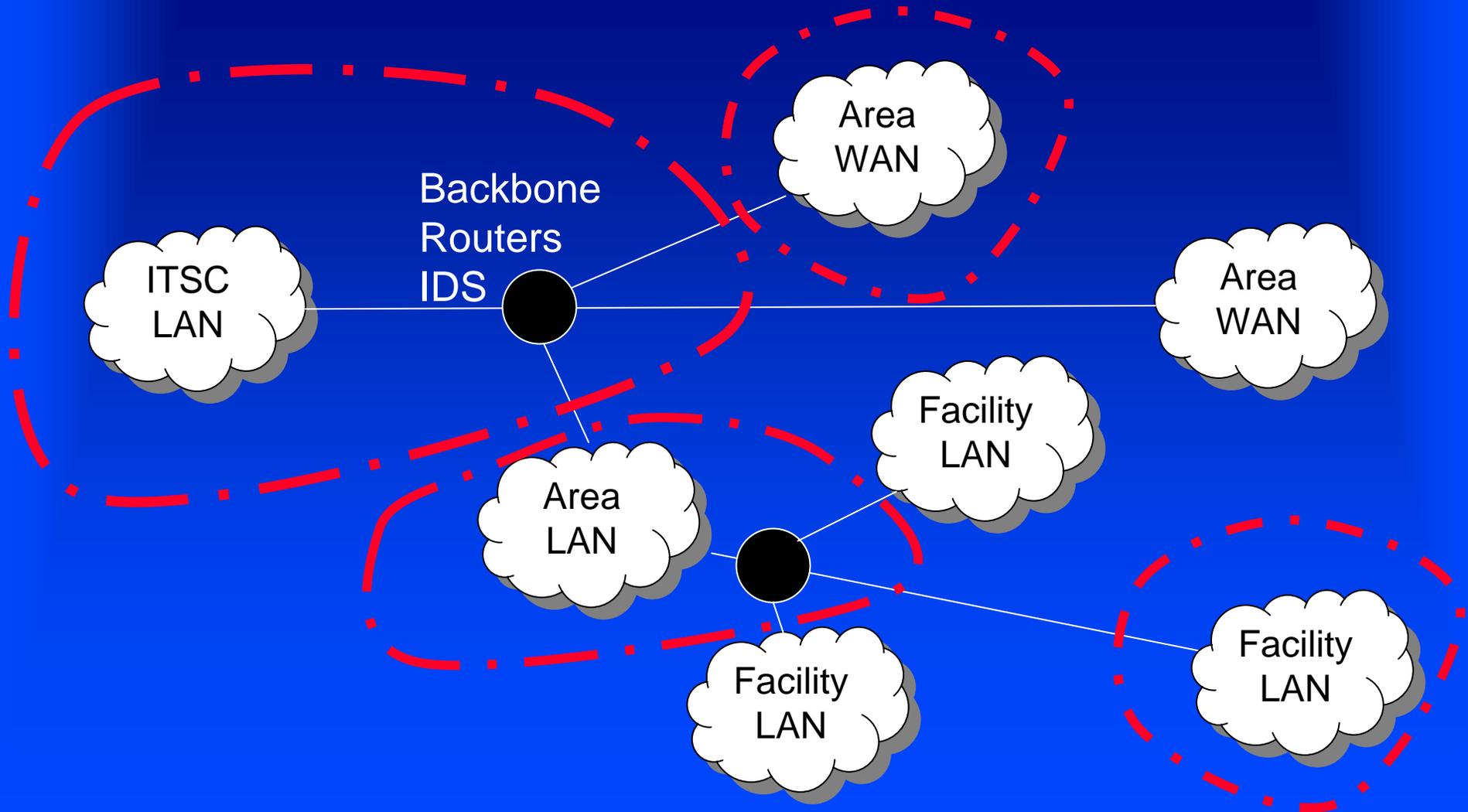
# HIPAA Administrative Simplification Compliance – HHS HIPAA

Compliance Guide, October 29, 2003

- 1) Determine if Covered Entity
  - Define “IHS entities” / risk assessment boundaries
- 2) Identify Applicable Information
  - Conduct risk analyses / management
- 3) Conduct Gap Analysis
  - Policies and procedures – HQE / ITSC
    - Cross reference to other requirements
      - PIA, C&A, FISMA
  - Review policies and procedures at “IHS entities” / Areas level
- 4) Document Policies[,] [and] Procedures [and] Practices, Guidelines, Checklists
- 5) Define Compliance Methodology
  - Implement policies and procedures via. practices, guidelines, checklists – “IHS entities” / Areas



# Defining Entities / Boundaries





# Reasoning

---

- **Standard: Security management process - required**
- **Implementation specifications**
  - Risk analysis – required
  - Risk management – required
- **Determining “reasonable and appropriate” is based on the covered entity’s**
  - Size, complexity, and capability
  - Technical infrastructure, hardware, and software security capabilities
  - Cost of security measures
  - Probability and criticality of potential risks to EPHI - Risk analysis



# Compliance Dates

---

- April 20, 2005 – all covered entities except small health plans
- April 20, 2006 – small health plans



# HIPAA Civil and Criminal Penalties

---

- **Apply to individuals as well as entities**
- **Civil**
  - Up to \$100 per violation and \$25,000 per year for each requirement or prohibition violated
- **Criminal – Federal Offense**
  - Up to \$50,000 and 1 year in prison
  - Up to \$100,000 and 5 years in prison if offenses committed under “false pretenses”
  - Up to \$250,000 and 10 years in prison if offenses committed with intent to sell, transfer or use PHI for commercial advantage, personal gain or malicious harm.



# Other Potential Consequences – HHS

HIPAA Compliance Guide, October 29, 2003

---

- **Enforcement and oversight by HHS**
- **Loss of public trust**
- **Budget effects**
- **Private lawsuits**



# Topics

---

- HIPAA Security
- **Certification and Accreditation**
- Websense
- Incident Response
- Certificates
- Blaster/Welchia Infection
- Security Training Requirements
- COOP



# Certification and Accreditation

---

- **Certification - the detailed review of security controls**
- **Accreditation - the official management decision to authorize system operations**
- **Process should be initiated during a system's planning phase**
- **Continuous process through the end of a system's life cycle**



# Certification and Accreditation

---

## ■ Requirements

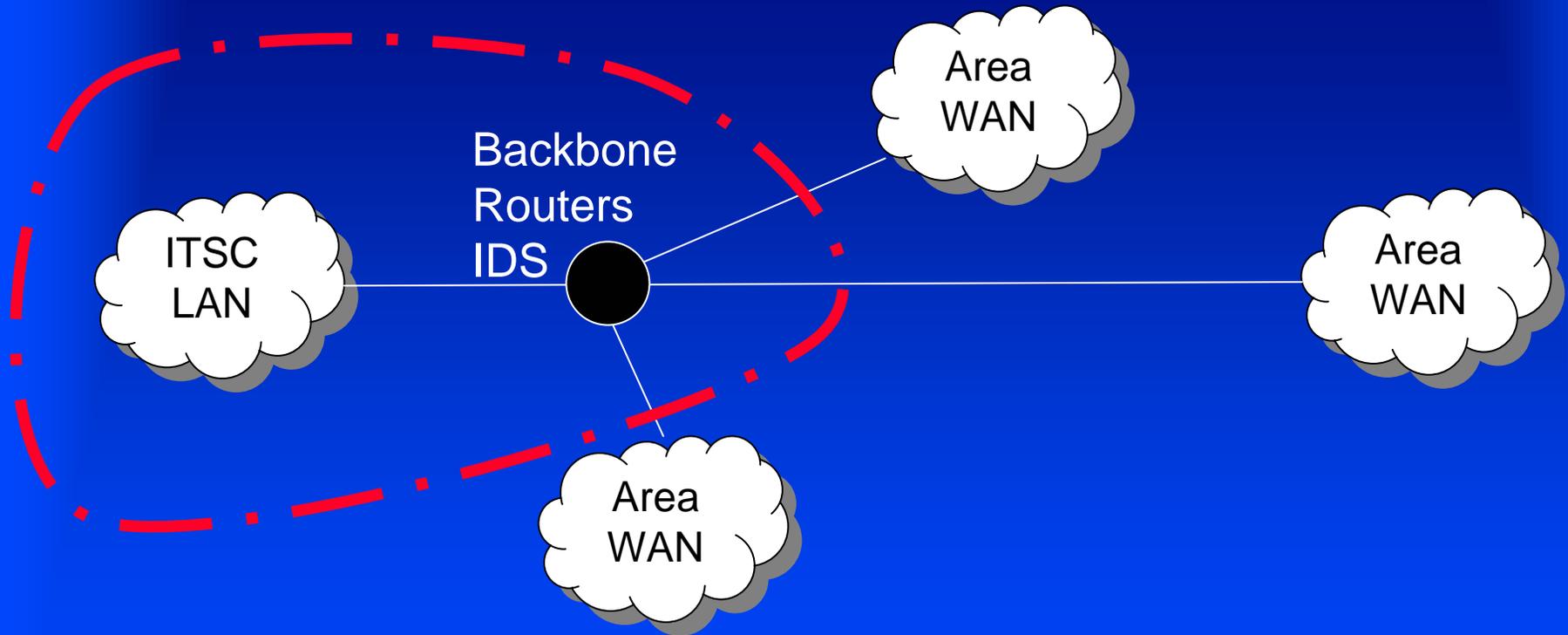
- Major System / Application
- General Support System
- Every three years, with a significant change, or compromise

## ■ IHS Plan

- ITSC – IHSNET, NPIRS, RPMS
- AAO – IFAS
- Areas – evaluate requirements

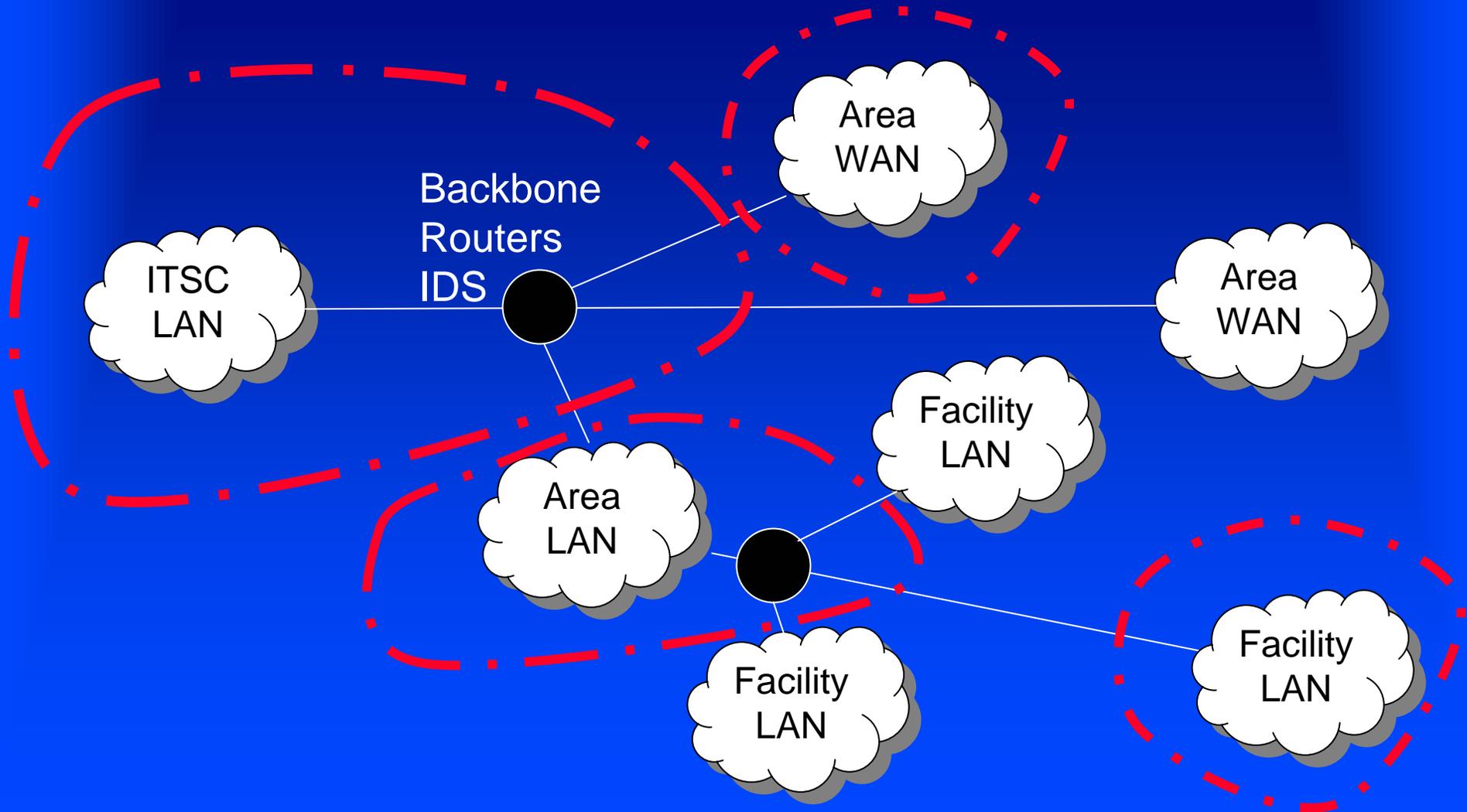


# IHSNET - GSS





# Boundaries





# Primary Roles

---

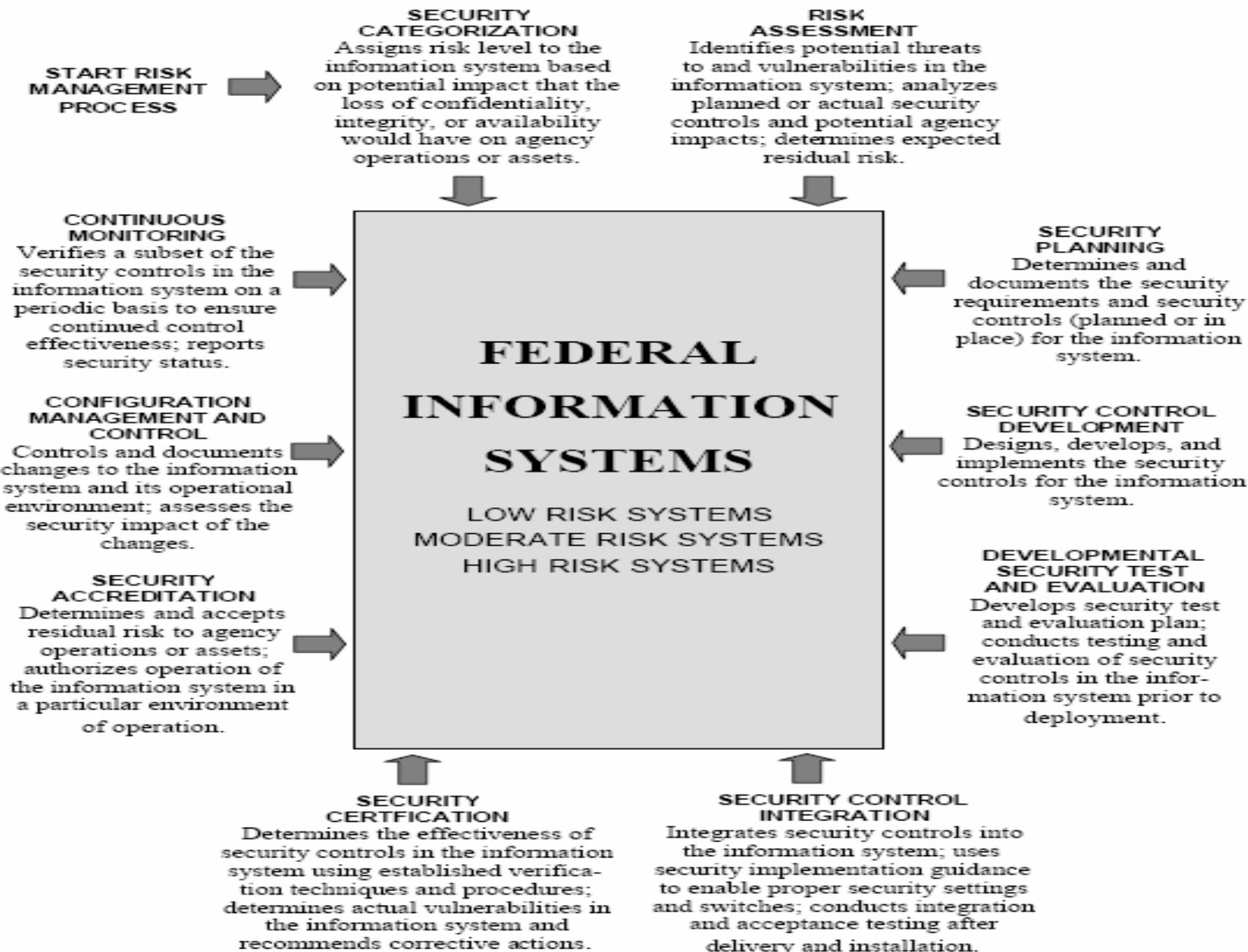
- **User Representative**
- **Program Manager**
- **Certification Authority**
- **Designated Approving Authority (DAA)**
- **ISSO may be added to increase the integrity and objectivity of C&A decisions in support of the system business case or mission**



# Minimum Requirements for Certification Package - NICAP

---

- **SSAA Sections 1-5**
- **ST&E Report**
- **Final Risk Assessment**
- **CA recommendation statement**
- **System Rules of Behavior**
- **Personnel Controls and Technical Security Controls**
- **Memorandums of Agreement – System Interconnection Agreements**





# Topics

---

- HIPAA Security
- Certification and Accreditation
- **Websense**
- Incident Response
- Certificates
- Blaster/Welchia Infection
- Security Training Requirements
- COOP



# Websense

---

## ■ Policy development

- Clinicians develop requirements
- Areas develop requirements
- Security develop requirements
- Management develop requirements
- Committee integrate requirements, stakeholder review, and develop policy

## ■ Central management

- Implement policy
- Incorporate reviewed changes



# Topics

---

- HIPAA Security
- Certification and Accreditation
- Websense
- **Incident Response**
- Certificates
- Blaster/Welchia Infection
- Security Training Requirements
- COOP



# Incident Response

---

## ■ Requirements

- Teams for IR, investigation, resolve, lessons learned, educate users

## ■ Resources

- ITSC / Areas

## ■ Training

- Software Engineering Institute
- SANS



# Topics

---

- HIPAA Security
- Certification and Accreditation
- Websense
- Incident Response
- **Certificates**
- Blaster/Welchia Infection
- Security Training Requirements
- COOP



# Certificates

---

- VeriSign
- Class III
  - Requires display of ID



# Topics

---

- HIPAA Security
- Certification and Accreditation
- Websense
- Incident Response
- Certificates
- **Blaster/Welchia Infection**
- Security Training Requirements
- COOP



# Blaster / Welchia Infection

---

- **Root cause**
  - Patching
- **Automated patching**
  - Link capacity
  - HFnetCheck
- **Out-of-band communications**
  - Telephone
  - Other email – outside IHS network
  - Alternatives



# Topics

---

- HIPAA Security
- Certification and Accreditation
- Websense
- Incident Response
- Certificates
- Blaster/Welchia Infection
- **Security Training Requirements**
- COOP



# Security Training Requirements

---

- Incident Response
- IHS Policy and Procedures
- Log analysis
- IT practices
- Firewall, router, switch, OS, and application etc. configuration
- IT security auditing



# Topics

---

- **HIPAA Security**
- **Certification and Accreditation**
- **Websense**
- **Incident Response**
- **Certificates**
- **Blaster/Welchia Infection**
- **Security Training Requirements**
- **COOP**



# COOP

---

- **Oklahoma's Lessons Learned**
- **Plans**
  - **Analyze requirements**
  - **Review / revise documents**
  - **Coordinate**
- **DHS Plan**
  - **Coordinate nationwide COOP exercise**
    - **Spring 04**