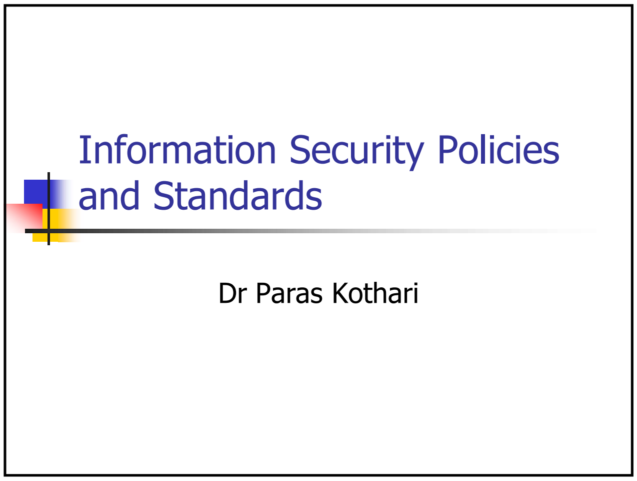
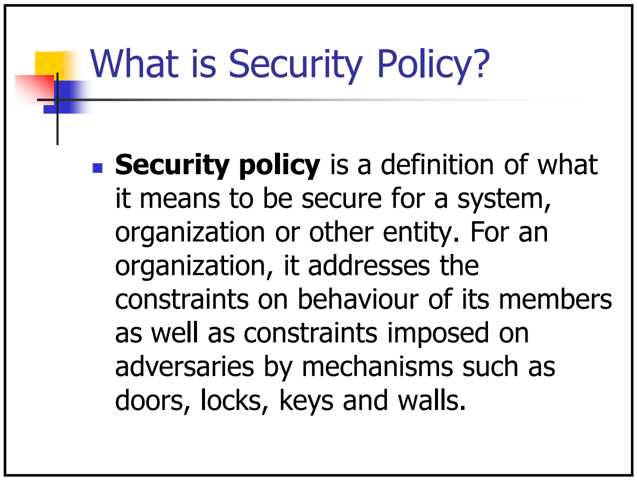


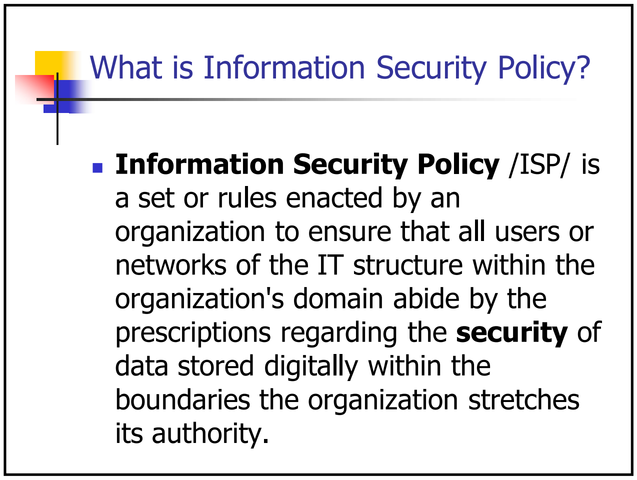
Information Security Policies and Standards

Dr Paras Kothari



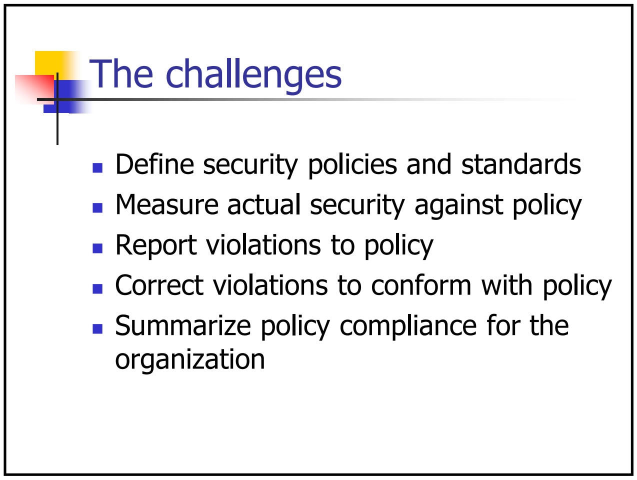
What is Security Policy?

- **Security policy** is a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behaviour of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.



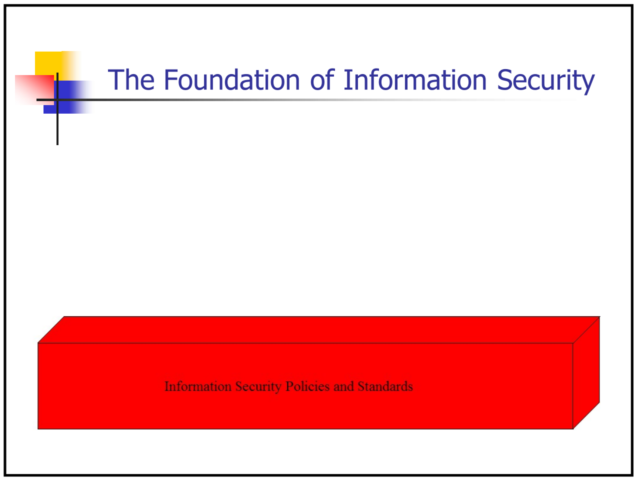
What is Information Security Policy?

- **Information Security Policy** /ISP/ is a set or rules enacted by an organization to ensure that all users or networks of the IT structure within the organization's domain abide by the prescriptions regarding the **security** of data stored digitally within the boundaries the organization stretches its authority.



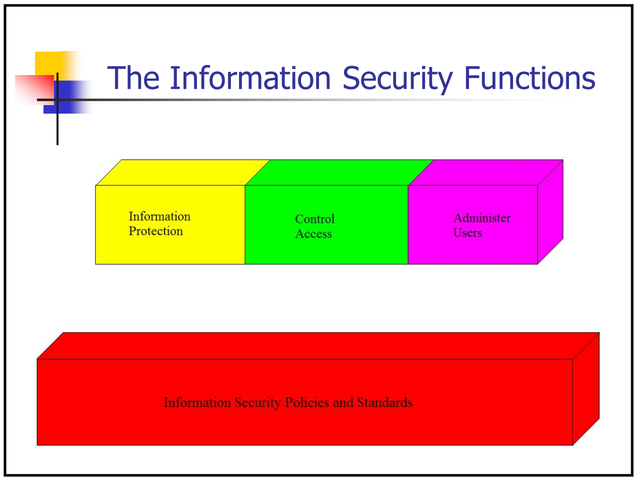
The challenges

- Define security policies and standards
- Measure actual security against policy
- Report violations to policy
- Correct violations to conform with policy
- Summarize policy compliance for the organization



The Foundation of Information Security

Information Security Policies and Standards



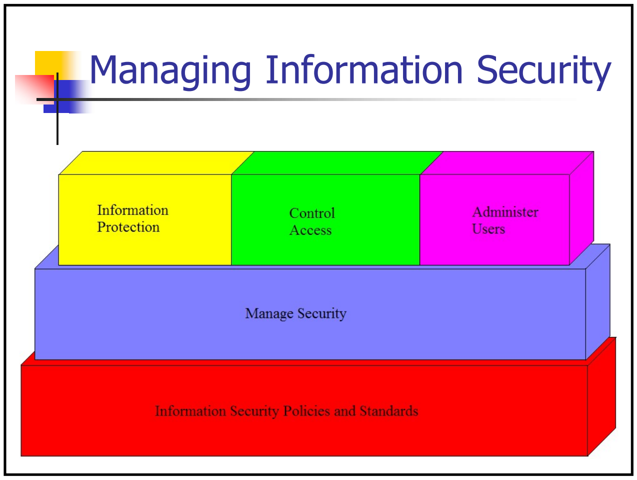
The Information Security Functions

Information Protection

Control Access

Administer Users

Information Security Policies and Standards



Managing Information Security

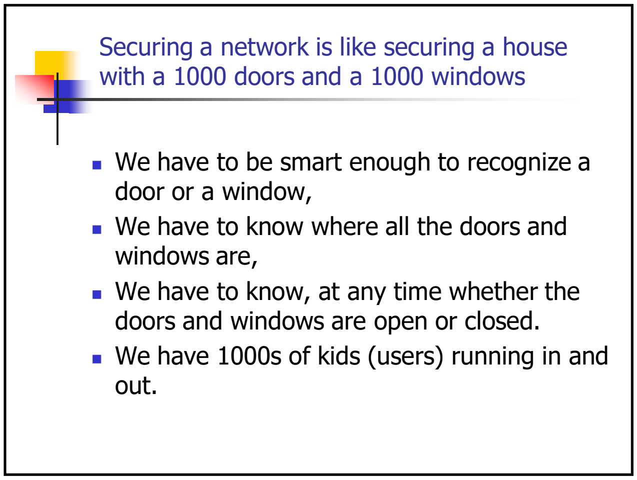
Information Protection

Control Access

Administer Users

Manage Security

Information Security Policies and Standards



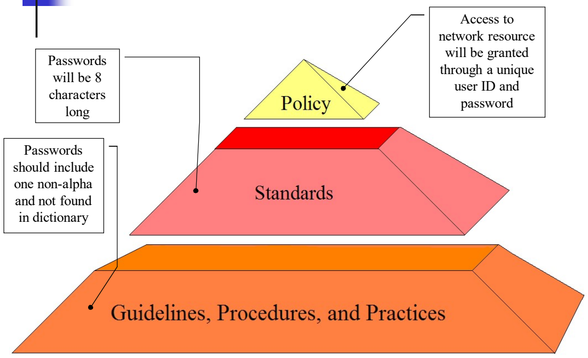
Securing a network is like securing a house with a 1000 doors and a 1000 windows

- We have to be smart enough to recognize a door or a window,
- We have to know where all the doors and windows are,
- We have to know, at any time whether the doors and windows are open or closed.
- We have 1000s of kids (users) running in and out.

Definitions

- Policies
  - High level statements that provide guidance to workers who must make present and future decision
- Standards
  - Requirement statements that provide specific technical specifications
- Guidelines
  - Optional but recommended specifications

Security Policy



Passwords will be 8 characters long

Passwords should include one non-alpha and not found in dictionary

Access to network resource will be granted through a unique user ID and password

Policy

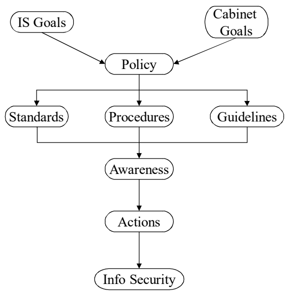
Standards

Guidelines, Procedures, and Practices

Elements of Policies

- Set the tone of Management
- Establish roles and responsibility
- Define asset classifications
- Provide direction for decisions
- Establish the scope of authority
- Provide a basis for guidelines and procedures
- Establish accountability
- Describe appropriate use of assets
- Establish relationships to legal requirements

Policy Lifecycle



IS Goals

Cabinet Goals

Policy

Standards

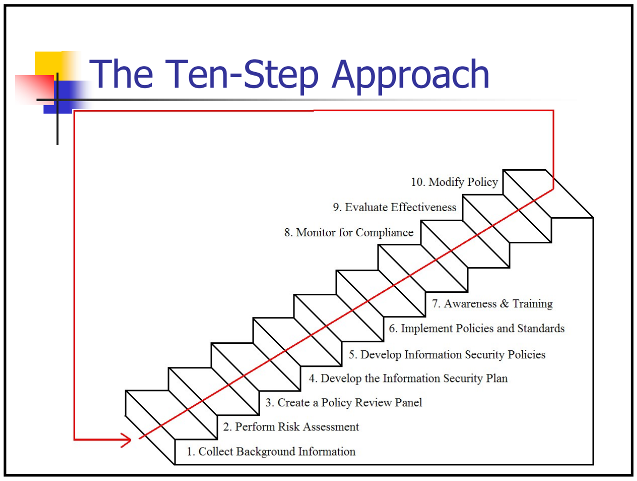
Procedures

Guidelines

Awareness

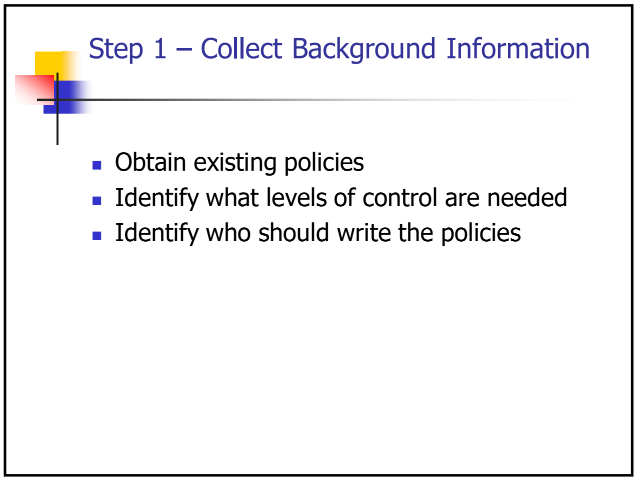
Actions

Info Security



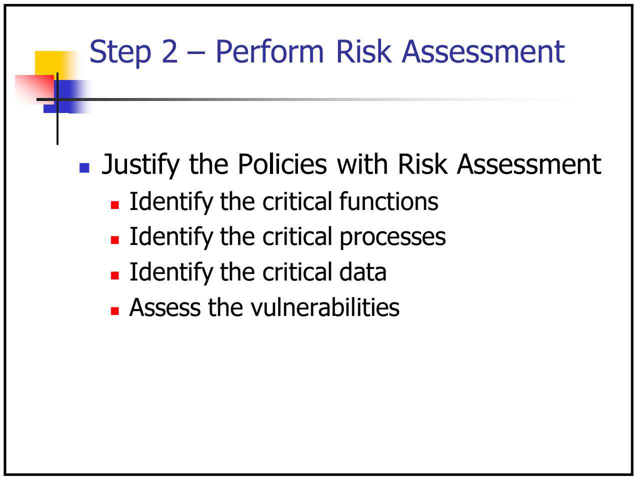
The Ten-Step Approach

10. Modify Policy
9. Evaluate Effectiveness
8. Monitor for Compliance
7. Awareness & Training
6. Implement Policies and Standards
5. Develop Information Security Policies
4. Develop the Information Security Plan
3. Create a Policy Review Panel
2. Perform Risk Assessment
1. Collect Background Information



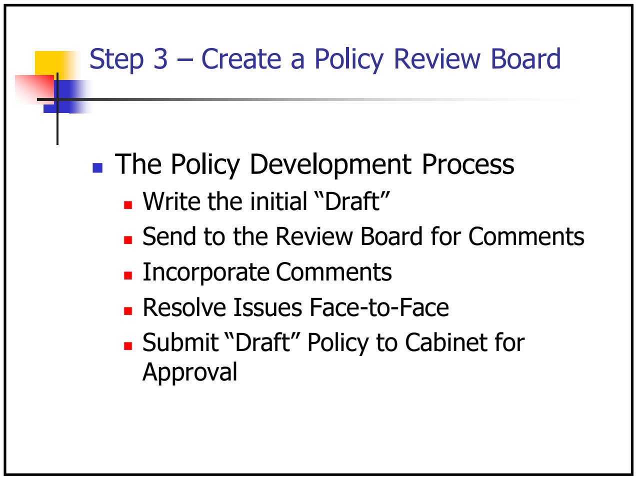
Step 1 – Collect Background Information

- Obtain existing policies
- Identify what levels of control are needed
- Identify who should write the policies



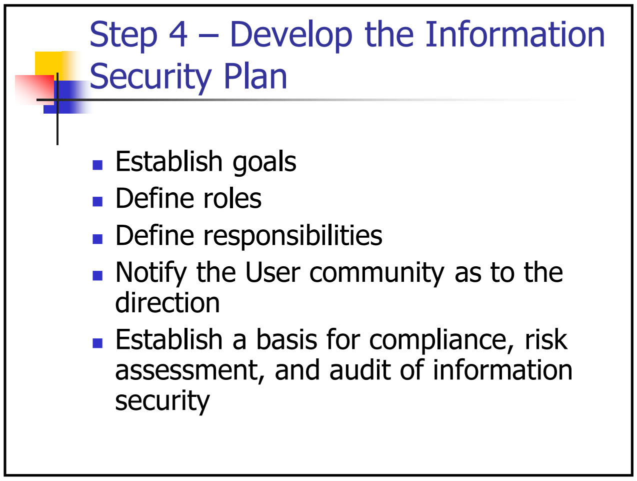
Step 2 – Perform Risk Assessment

- Justify the Policies with Risk Assessment
  - Identify the critical functions
  - Identify the critical processes
  - Identify the critical data
  - Assess the vulnerabilities



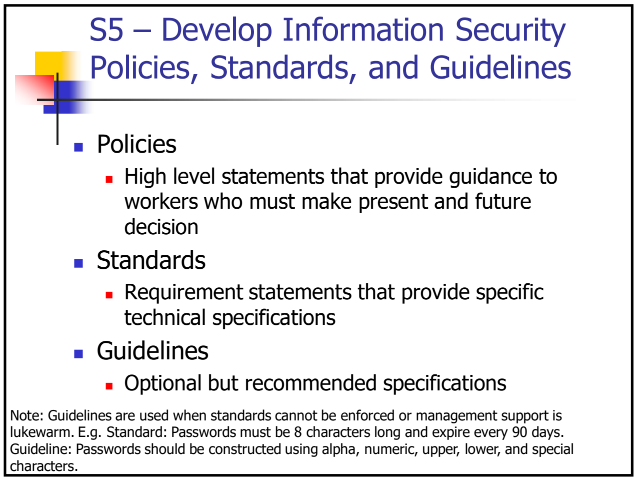
Step 3 – Create a Policy Review Board

- The Policy Development Process
  - Write the initial "Draft"
  - Send to the Review Board for Comments
  - Incorporate Comments
  - Resolve Issues Face-to-Face
  - Submit "Draft" Policy to Cabinet for Approval



Step 4 – Develop the Information Security Plan

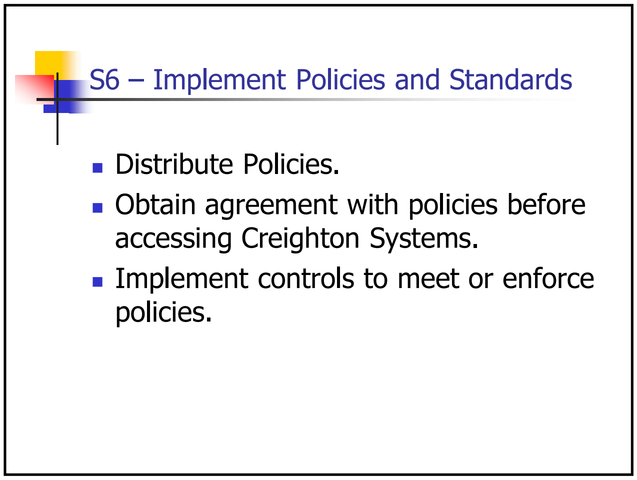
- Establish goals
- Define roles
- Define responsibilities
- Notify the User community as to the direction
- Establish a basis for compliance, risk assessment, and audit of information security



S5 – Develop Information Security Policies, Standards, and Guidelines

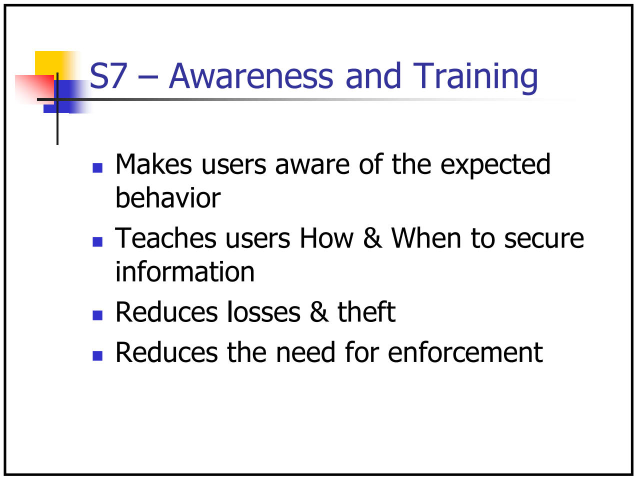
- Policies
  - High level statements that provide guidance to workers who must make present and future decision
- Standards
  - Requirement statements that provide specific technical specifications
- Guidelines
  - Optional but recommended specifications

Note: Guidelines are used when standards cannot be enforced or management support is lukewarm. E.g. Standard: Passwords must be 8 characters long and expire every 90 days. Guideline: Passwords should be constructed using alpha, numeric, upper, lower, and special characters.



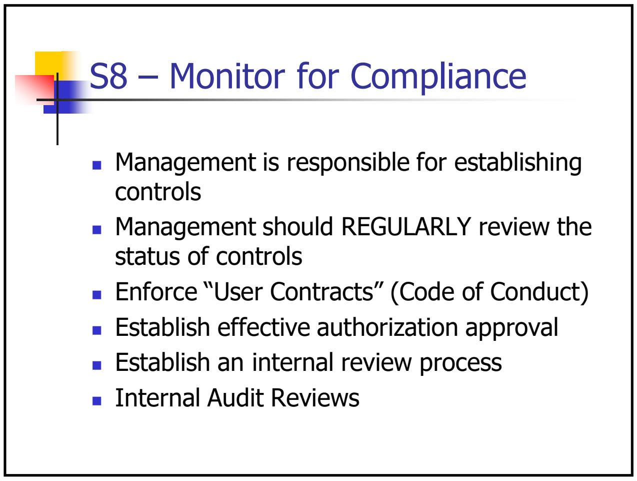
S6 – Implement Policies and Standards

- Distribute Policies.
- Obtain agreement with policies before accessing Creighton Systems.
- Implement controls to meet or enforce policies.



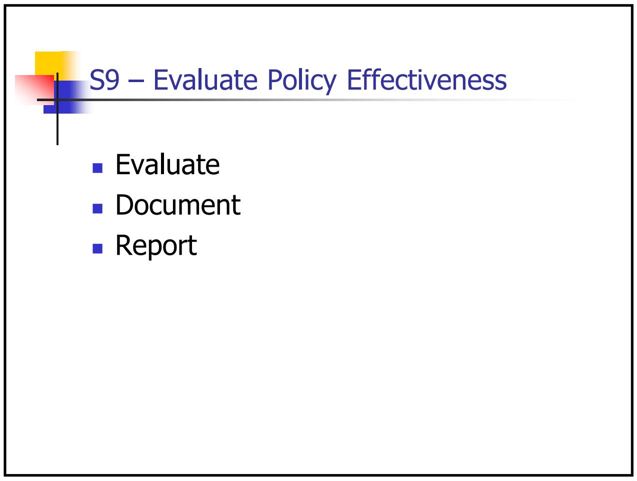
S7 – Awareness and Training

- Makes users aware of the expected behavior
- Teaches users How & When to secure information
- Reduces losses & theft
- Reduces the need for enforcement



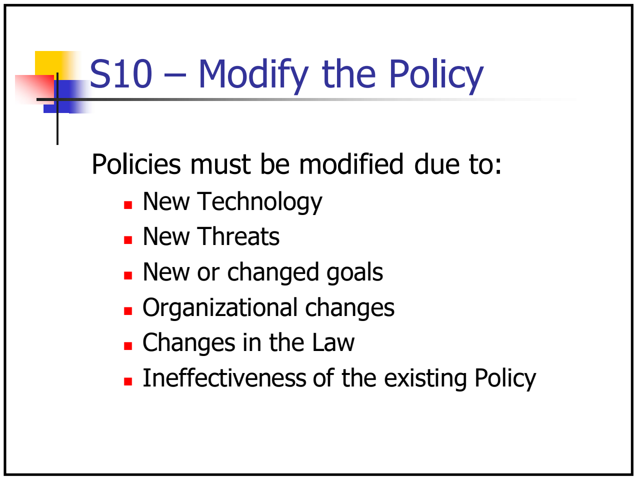
S8 – Monitor for Compliance

- Management is responsible for establishing controls
- Management should REGULARLY review the status of controls
- Enforce "User Contracts" (Code of Conduct)
- Establish effective authorization approval
- Establish an internal review process
- Internal Audit Reviews



S9 – Evaluate Policy Effectiveness

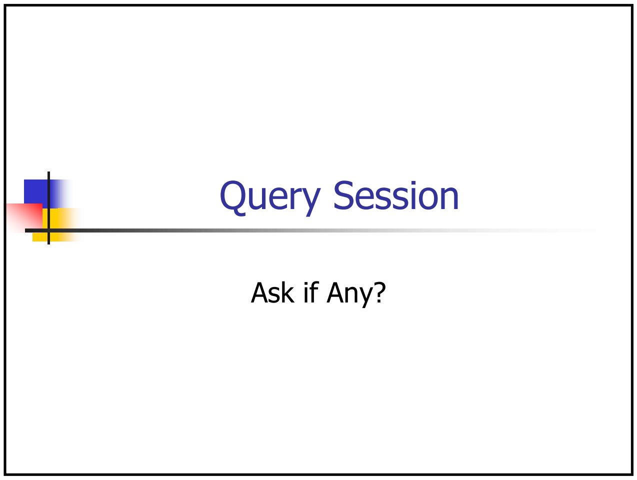
- Evaluate
- Document
- Report



S10 – Modify the Policy

Policies must be modified due to:

- New Technology
- New Threats
- New or changed goals
- Organizational changes
- Changes in the Law
- Ineffectiveness of the existing Policy



Query Session

Ask if Any?