INFORMATION SECURITY POLICY

OBJECTIVES

1. Provide an overview of security policy.
2. Define and show the relationship between policies, standards, guidelines, and procedures.
3. Identify categories and key components of security policies.
4. Introduce security policy processes.

INFORMATION SECURITY POLICY

- Policies, Standards, Guidelines
- Elements of Policies, Standards & Guidelines
- Policy Objectives
- Policy Classifications
- Policy Components
- Information Security Policy Framework
- Policy Support
- Policy Development Lifecycle
- Delivery Methods

INFORMATION SECURITY POLICY

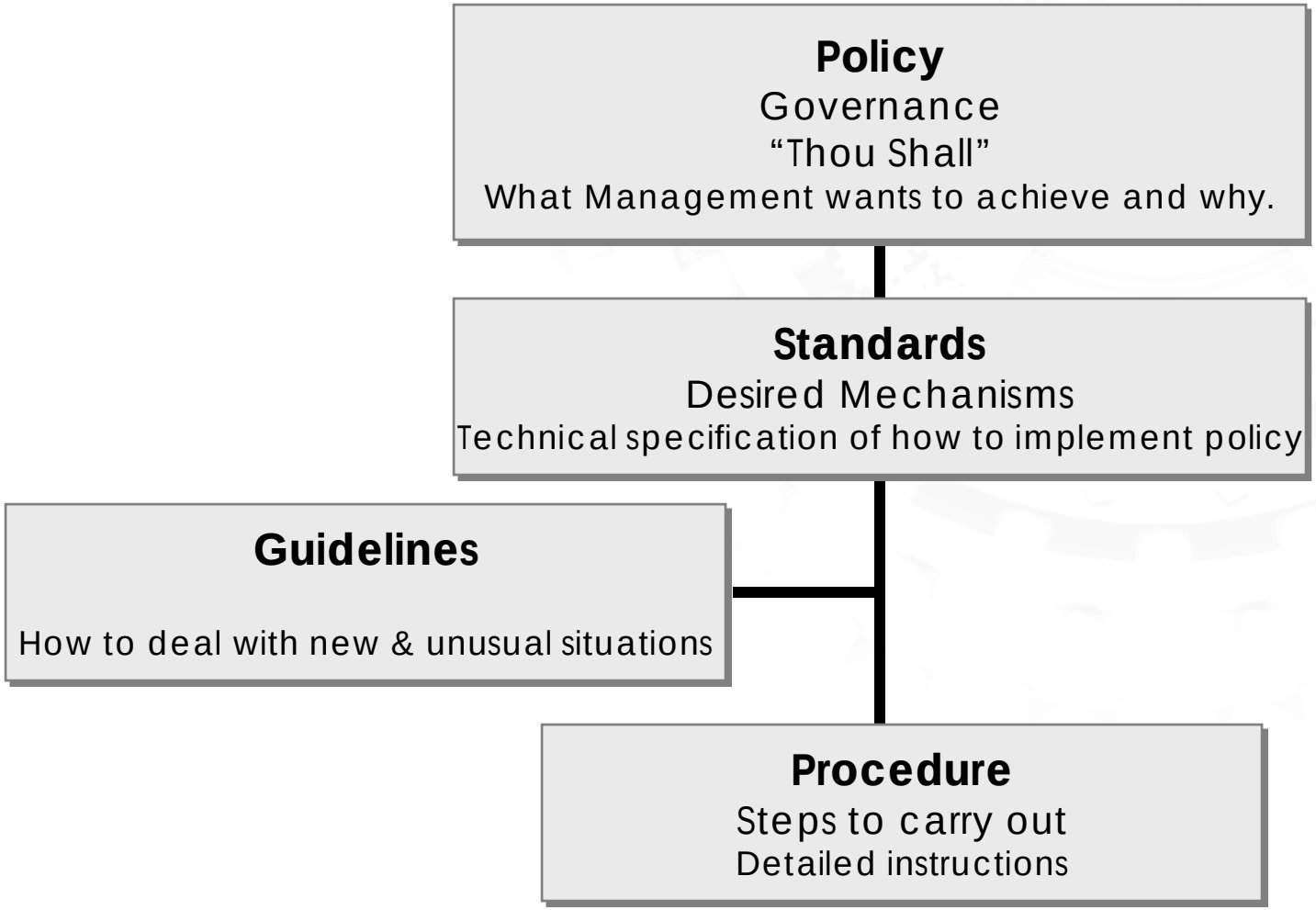
- Without strong management policies, corporate security programs will be less effective and not align with management objectives.
- Policies are the blueprint for the security framework
- Policies, Standards and Guidelines enables the corporation to implement the specific controls processes and awareness programs to raise the level of information security and assurance.

POLICES & STANDARDS

- Policies
  - High Level “umbrellas”
  - Low Level
- Standards
  - Corporate-wide standards
  - Local Guidelines
- Procedures
  - Local repeatable processes

- *User Management Policies*
  - *All system users must be individually identified*
- *OS Authentication*
  - *Unix, Windows users …*
  - *Administrative access vs. general*
- *How-To*
  - *Request an account*
  - *Approve a new system*

HOW THEY RELATE



ELEMENTS OF A POLICY

- Scope – What you are going to protect
- High Level Policy Statement – 30,000 ft overview
- Accountability – personnel
- Non- compliance – a statement pertaining to loss if compromised
- Monitoring – how policies, standards or guidelines will be validated
- Exceptions – in the event that a community of users cannot meet compliance

INFORMATION SECURITY POLICY OBJECTIVES

- Foster information confidentiality
- Outline data integrity responsibilities
- Define assets that require protection
- How resources should be used efficiently and appropriately
- Provide for system availability
- Raise awareness
- Provide a foundation, a roadmap and a compass for information security audit, process, technology and operations

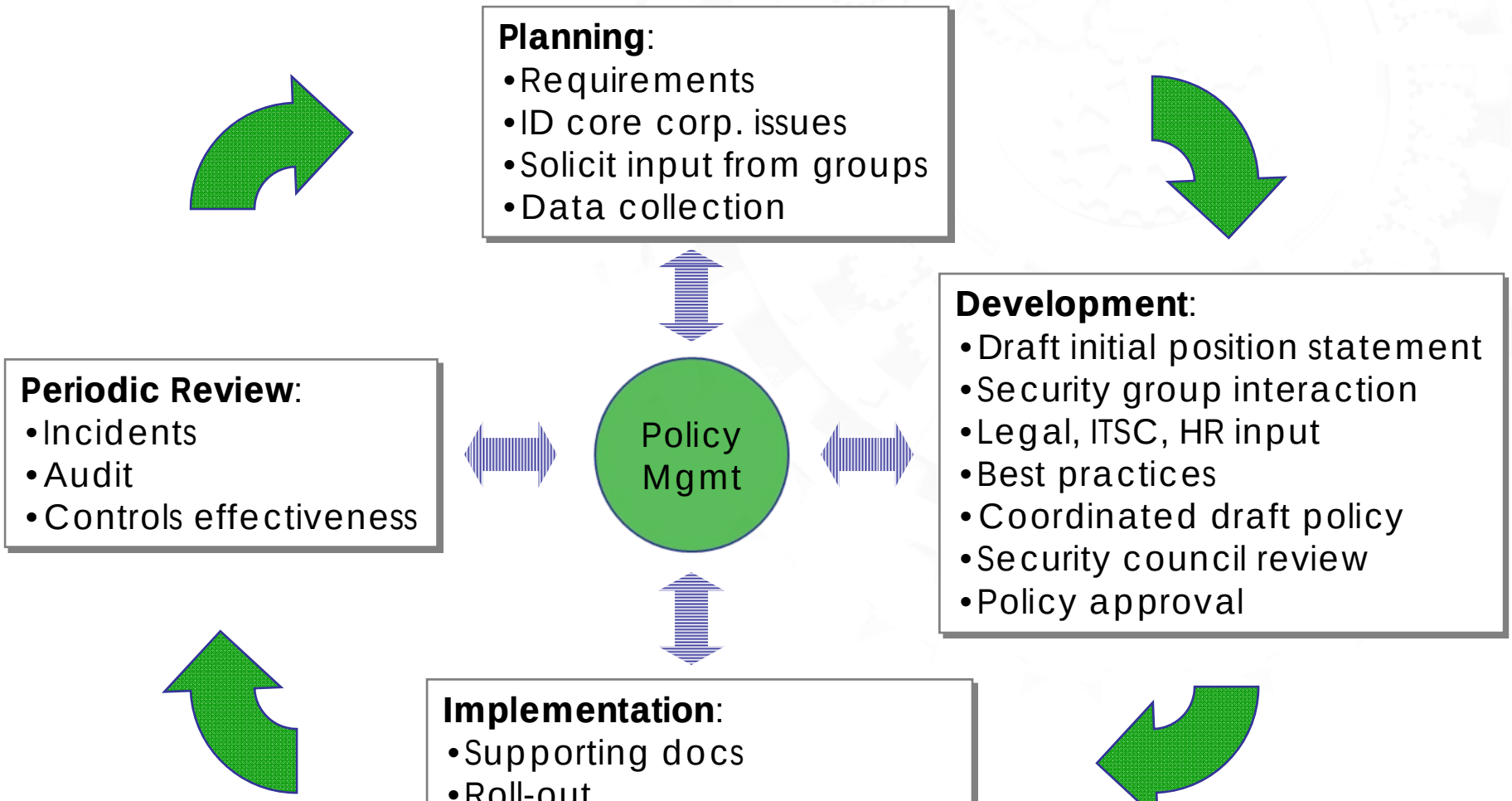
ELEMENTS OF A STANDARD

- Scope – How you are going to protect
- Role & Responsibilities – defining, executing, and supporting standards
- Guidance – references overriding policy statements
- Baseline standards – high level statements for platform and applications
- Technical Standard – product/version specifications and associated descriptions
- Administrative Standard - initial and ongoing administration of platform and applications

ELEMENTS OF A GUIDELINE

- Guidelines should be based on industry best practices (whenever possible)
- Purpose – to efficiently meet the standard and policy requirements
- Intent – description of guideline's objectives
- Roles & Responsibilities – defining, executing and supporting guidelines
- Guideline Statements – step by step process to implement policy elements
- Operational Statements - defines the "how" of day to day operations

POLICY DEVELOPMENT LIFE-CYCLE



POLICY CLASSIFICATIONS

Regulatory	HIPAA, FCRA, GLBA, SOX
Public	Marketing materials
Internal	Trade secrets, proprietary ideas, HR Information
Confidential	Non-public corporate financial reports
Restrictive (Private)	Corporate payroll information, credit card transactions, customer data

POLICY CATEGORIES

- Information Security
  - Computer security policy
  - Program policy
  - Issue-specific policy
  - System-specific policy
- General Business
  - HR policies
  - Travel policy
  - Time and expense policy

COMMON POLICY COMPONENTS

- Intent / Purpose
- Scope and applicability
- Policy authors and sponsors
- Roles and responsibilities
- Effective and review dates
- Compliance measures
- Supplementary information and resources

GENERAL POLICY CONTENT

- Date of effective enforcement
- Statement of intent and audience
- Sponsor / authorizing corporate officer (or committee)
- Policy objectives and expectations
- Exception and change request process
- Breach of policy response process
- Review and expiration dates
- Corporate boundaries outlined in policy
  - Prohibited activities, liability issues, legal requirements, due diligence, etc.
- Local issues resolved by standards, guidelines, and other supporting documents ?