SECURITY POLICY

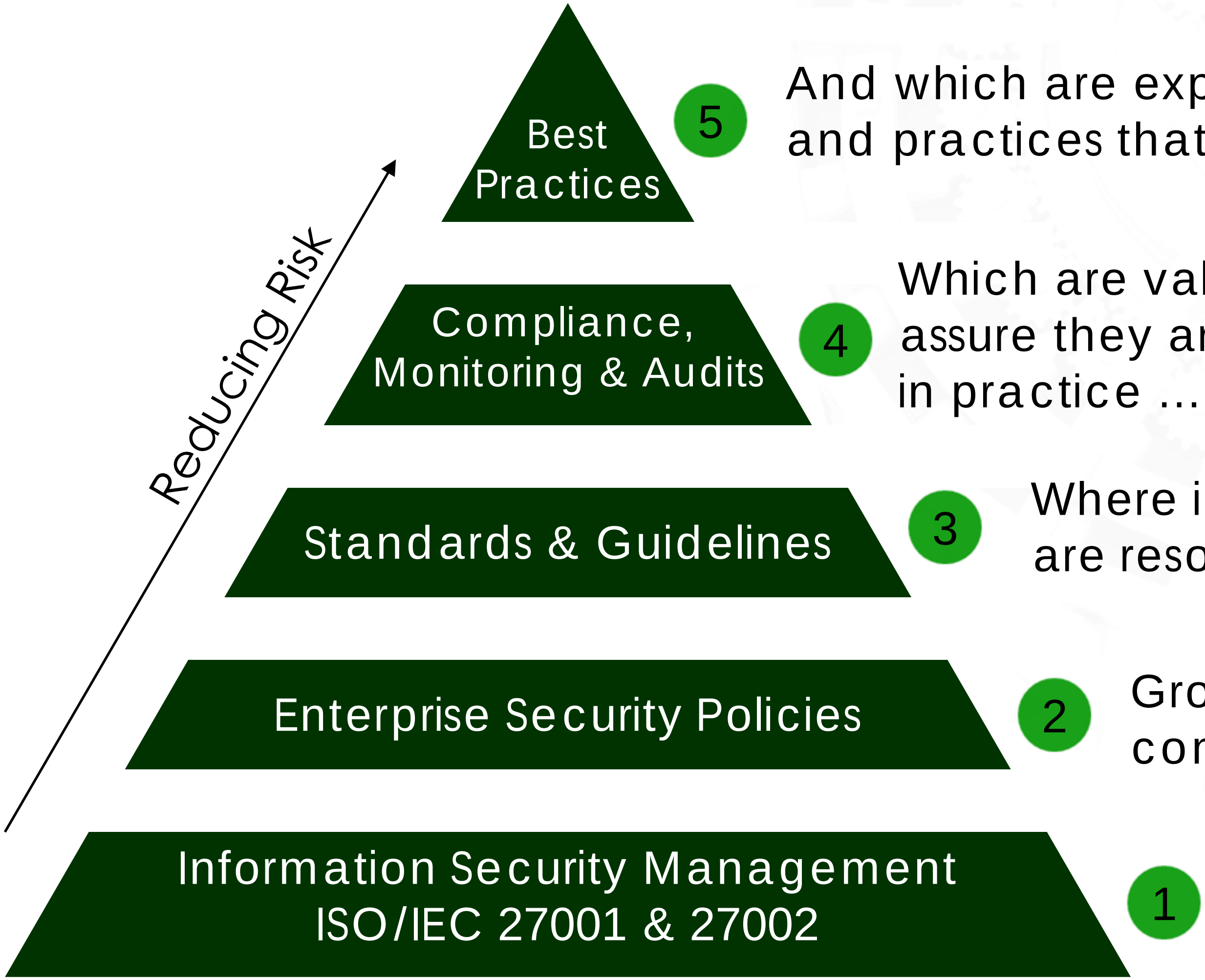
3: POLICY IN CONTEXT

SECURITY ARCHITECTURE

OBJECTIVES

1. Show policy's role within an information security program.
2. Explain the steps in the management of the information security program.

SECURITY MANAGEMENT FRAMEWORK



Reducing Risk

Best Practices

5 And which are expressed as activities and practices that are of high quality …

Compliance, Monitoring & Audits

4 Which are validated and watched to assure they are being implemented in practice …

Standards & Guidelines

3 Where implementation details are resolved by the business …

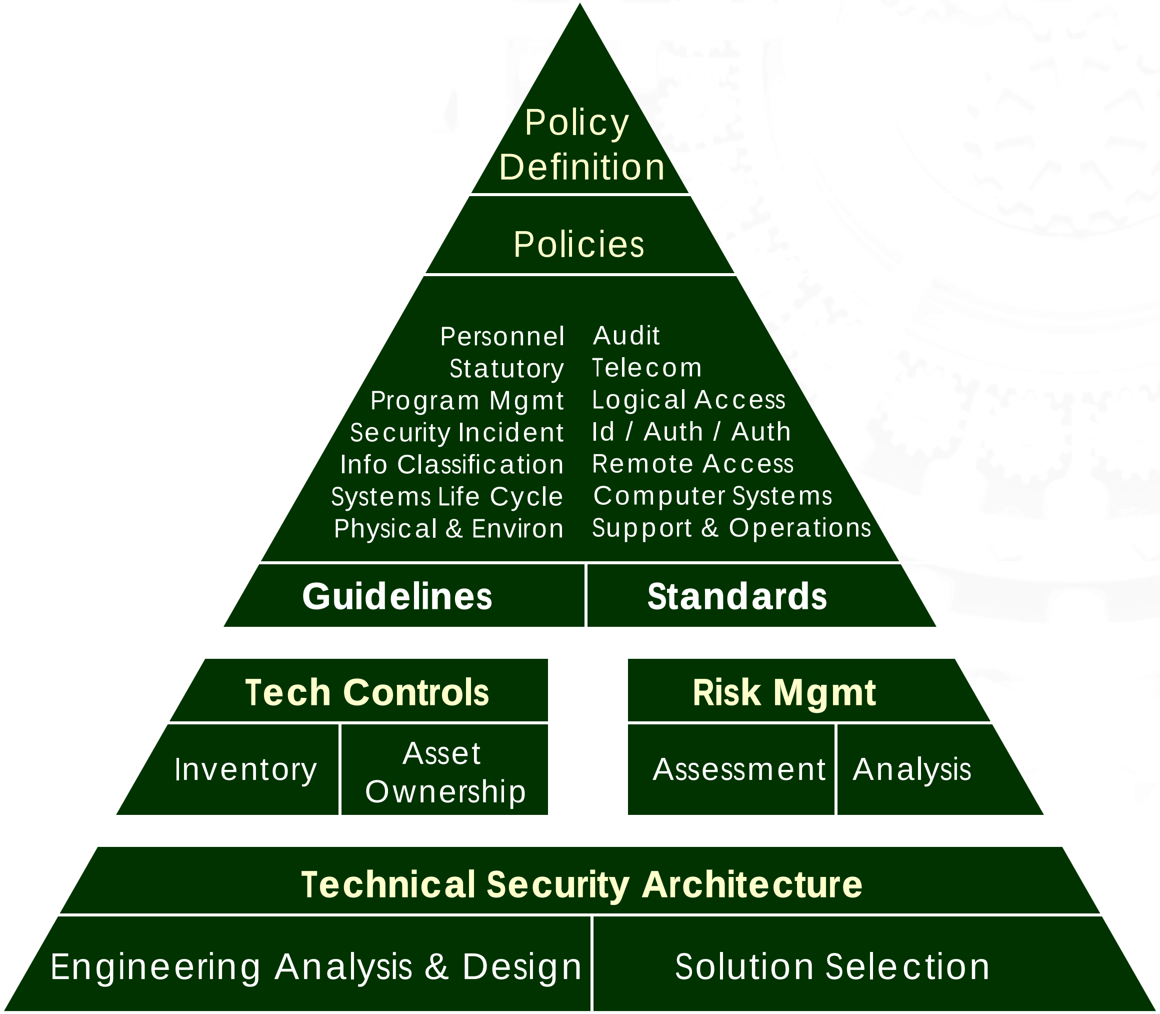
Enterprise Security Policies

2 Grounded in a comprehensive structure …

Information Security Management ISO/IEC 27001 & 27002

1 You need to start with a foundation …

POLICIES & TECHNICAL ARCHITECTURE



Policy Definition

Policies

Personnel
Statutory
Program Mgmt
Security Incident
Info Classification
Systems Life Cycle
Physical & Environ

Audit
Telecom
Logical Access
Id / Auth / Auth
Remote Access
Computer Systems
Support & Operations

Guidelines

Standards

Tech Controls

Inventory

Asset Ownership

Risk Mgmt

Assessment

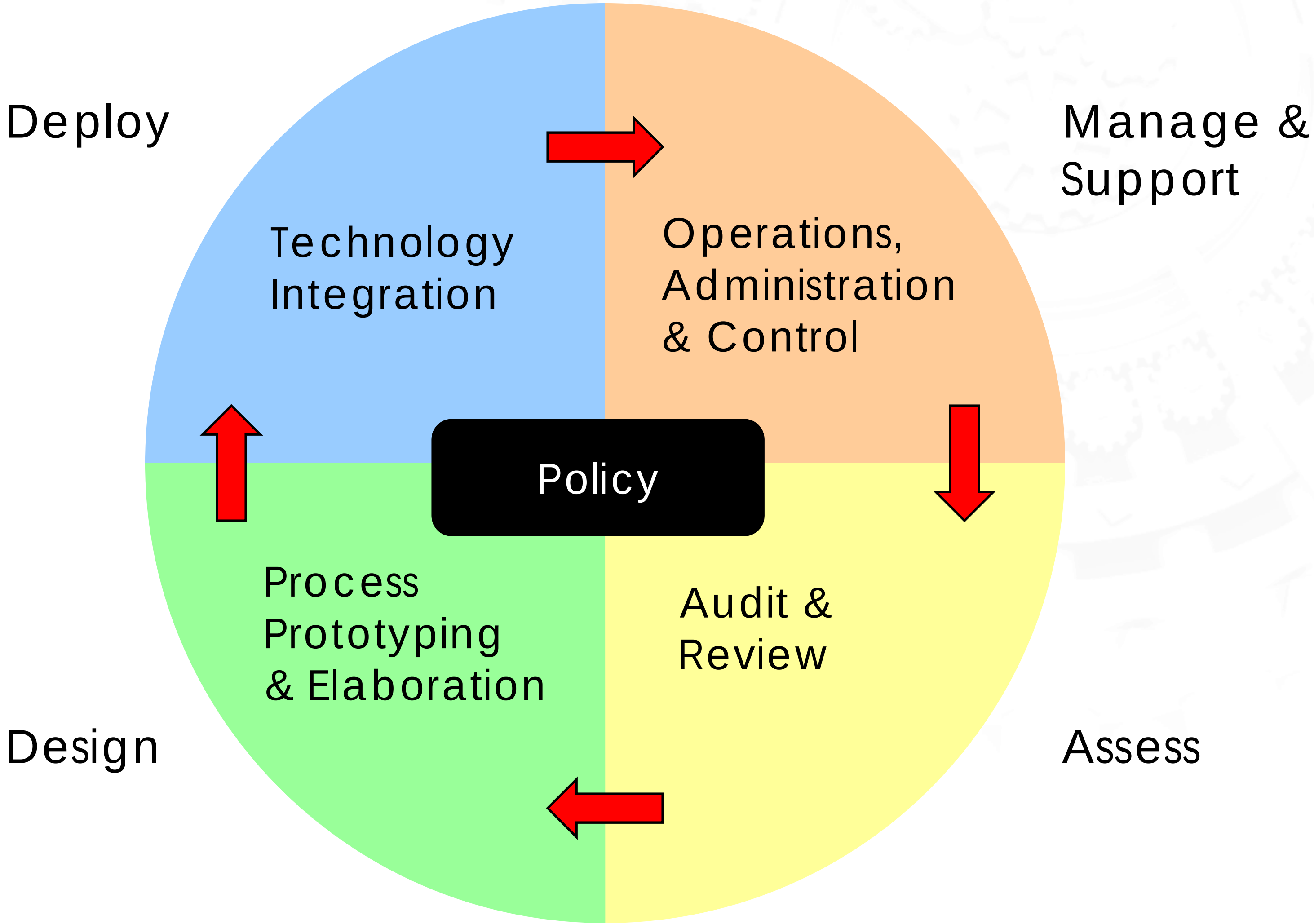
Analysis

Technical Security Architecture

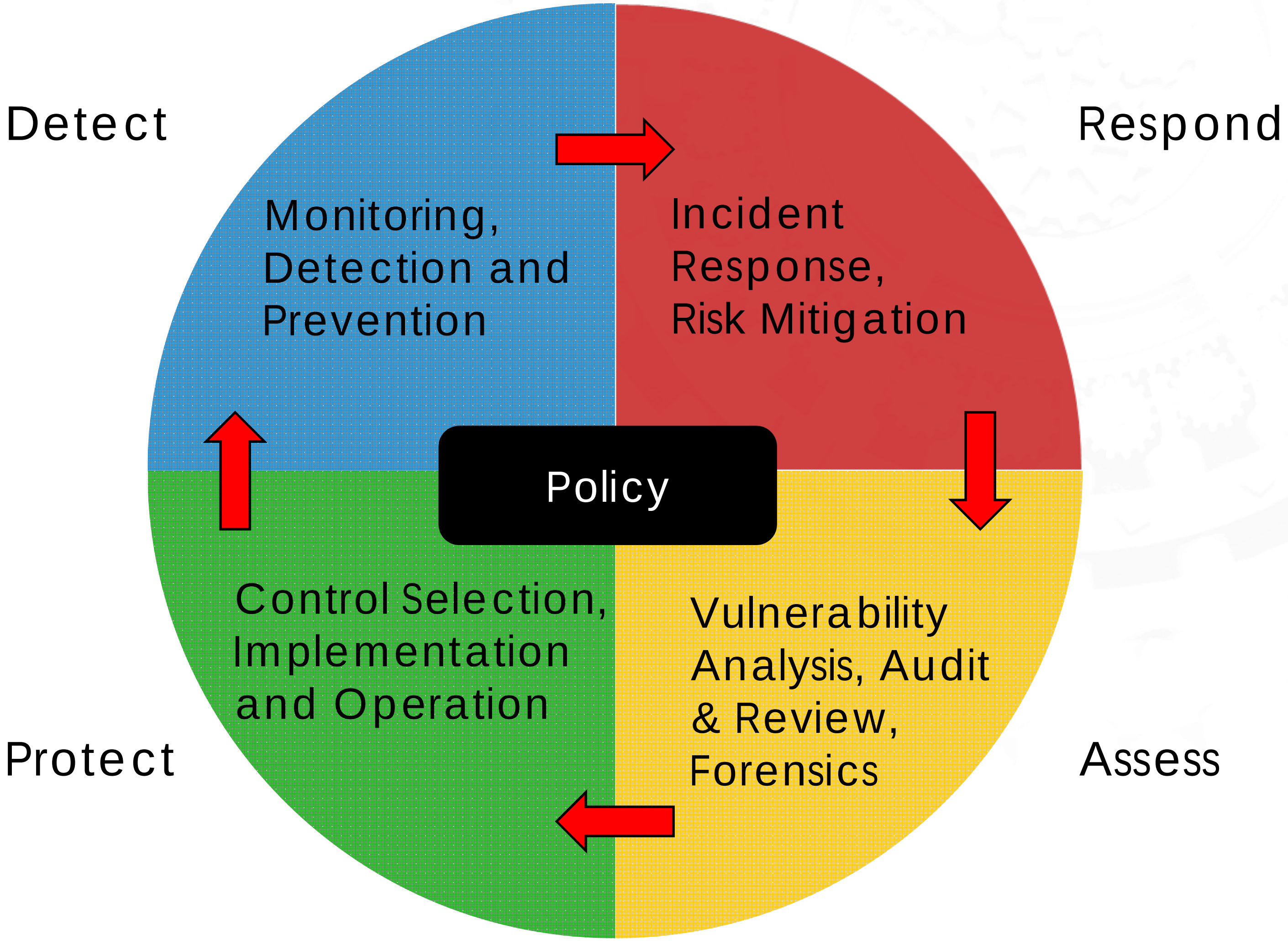
Engineering Analysis & Design

Solution Selection

INFORMATION SECURITY PROGRAM

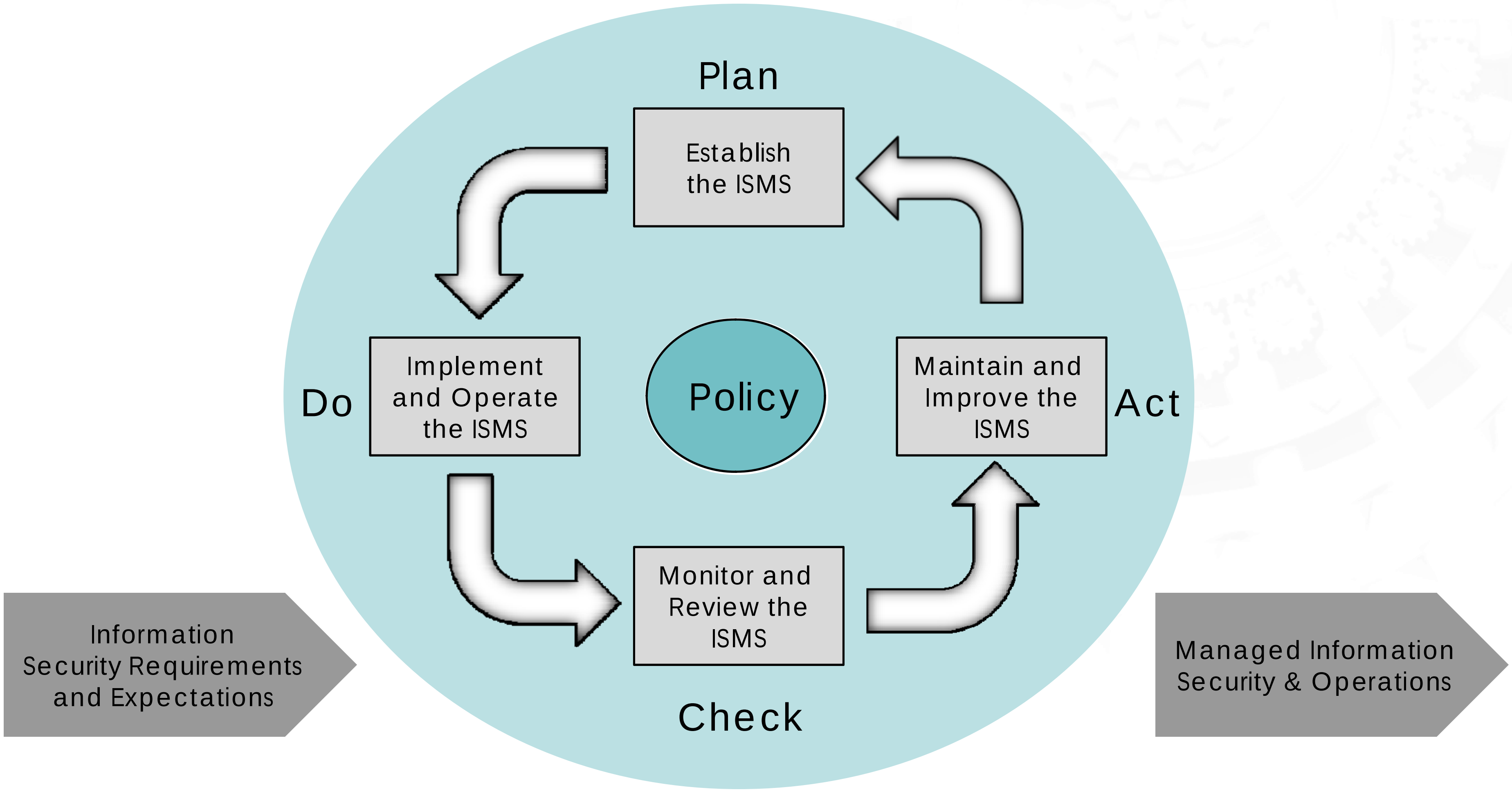


INFORMATION ASSURANCE MODEL



Detect
Monitoring, Detection and Prevention
Respond
Incident Response, Risk Mitigation
Policy
Control Selection, Implementation and Operation
Vulnerability Analysis, Audit & Review, Forensics
Protect
Assess

THE ISMS (ISO 27001) MODEL


Plan
Establish the ISMS
Do
Implement and Operate the ISMS
Policy
Maintain and Improve the ISMS
Act
Monitor and Review the ISMS
Check
Information Security Requirements and Expectations
Managed Information Security & Operations

POLICY

- Policy is the hub of the wheel … its central focus.
- It should be a reference point for actions taken and decisions made.
- Policy should be used when activities “on the wheel” are undertaken.
- Reviews should be conducted to ensure policy reflects business objectives.

AUDIT, ASSESSMENT & REVIEW

Policy is a key component of audit activities:

- Evaluate current security picture
- Compare against policy
- Performed on a regular basis and after a security event or as defined by a regulatory agency
- Results of audit and review process are used in the next phase of the security process

SECURITY STRATEGIC PLANNING

Iterative policy development should be part of strategic planning cycles:

- High level planning
- Use policy as a benchmark and a compass
- New strategic initiatives always impact policy
- Looks at process, not technology
- Uses audit and review findings

TECHNOLOGY INTEGRATION

The way security technologies work together is driven by security policy (remember defense in depth):

- Technical planning and implementation
- Based on policy
- Uses audit and review as well as developed process to determine technological requirements
- Tactical implementation of strategic goals
- The swords and shields of information security

POLICY MANAGEMENT TOOLS

- Apply security policies to systems
- Validate computers and applications connecting to the environment
- Detect policy compromise
- Automatic remediation if out of compliance
- May maintain “white list” of applications

Operation, Administration and Control

Operational actions should be dictated by policy:

- Keeping the processes and technology running
- Responding to security events
- Testing and practicing the right execution
- People play a key role
- Uses technology, process and policy to provide input to the audit and review process